Aruba Central
User Guide

a Hewlett Packard
Enterprise company

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Chapter 1
About this Guide

This user guide describes the features supported by Aruba Central and provides detailed instructions to set up and configure devices such as Instant APs, Aruba Switches, and Aruba SD-WAN Gateways.

Intended Audience

This guide is intended for system administrators who configure and monitor their networks using Aruba Central.

Related Documents

In addition to this document, the Aruba Central product documentation includes the following documents:

- *Aruba Central Help Center*
- *Aruba Central Getting Started Guide*
- *Aruba Central Managed Service Provider User Guide*
- *Aruba Central SD Branch Solution Guide*

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts

The following informational icons are used throughout this guide:

Indicates a risk of damage to your hardware or loss of data.

Indicates helpful suggestions, pertinent information, and important things to remember.

Indicates a risk of personal injury or death.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	asp.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Chapter 2
What is Aruba Central?

Aruba Central offers unified network management, AI-based analytics, and IoT device security for wired, wireless, and SD-WAN networks. All of these capabilities are combined into one easy-to-use platform, which includes the following apps:

- **Network Operations**—Provides unified network management by consolidating wired, wireless, and SD-WAN deployment and management tasks, real-time diagnostics, and live monitoring, for simple and fast problem resolution.
- **ClearPass Device Insight**—Provides a single pane of glass for device visibility employing automated device discovery, machine learning (ML) based fingerprinting and identification. For more information, see Aruba ClearPass Device Insight Information Center.

This section includes the following topics:

Key Features

Aruba Central offers the following key features and benefits:

- Streamlined configuration and deployment of devices—Leverages the ZTP capability of Aruba devices to bring up your network in no time. Aruba Central supports group configuration of devices, which allows you to provision and manage multiple devices with similar configuration requirements with less administrative overhead.
- Integrated wired, WAN, and wireless Infrastructure management—Offers a centralized management interface for managing wireless, WAN, and wired networks in distributed environments, and thus help organizations save time and improve efficiency.
- Advanced analytics and assurance—With continuous monitoring, AI-based analytics provide real-time visibility and insight into what's happening in the Wi-Fi network. The insights utilize machine learning that leverage a growing pool of network data and deep domain experience.
- Secure cloud-based platform—Offers a secure cloud platform with HTTPS connection and certificate based authentication.
- Interface for Managed Service Providers—Offers an additional interface for MSPs to provision and manage their respective tenant accounts. Using the MSP mode, service provider organizations can administer network infrastructure for multiple organizations in a single interface.
- SD-Branch Management—Offers a simplified solution for managing and monitoring SD Branch devices such as Branch Gateways, VPN Concentrators, Instant APs, and Aruba Switches. It also provides detailed dashboards showing WAN health and pictorial depictions of the branch setup. The Aruba SD-Branch solution extends the SD-WAN concepts to all elements in a branch setup to deliver a full-stack solution for managing WLAN, LAN and WAN connections. The SD-Branch solution provides a common cloud-management model that simplifies deployment, configuration, and management of all components of a

branch setup. The solution leverages the ZTP and cloud management capabilities of Aruba devices to integrate management and infrastructure for WAN, WLAN, and LAN and provide a holistic solution from access network to edge with end-to-end security. It also addresses all communications in distributed deployments, from micro branches to medium or large branches. For more information, see the Aruba SD-Branch Solution.

- Health and usage monitoring—Provides a comprehensive view of your network, device status and health, and application usage. You can monitor, identify, and address issues by using data-driven dashboards, alerts, reports, and troubleshooting workflows. Aruba Central also utilizes the DPI feature of the devices to monitor, analyze and block traffic based on application categories, application type, web categories and website reputation. Using this data, you can prioritize business critical applications, limit the use of inappropriate content, and enforce access policies on a per user, device or location basis.
- Guest Access—Allows you to manage access for your visitors with a secure guest Wi-Fi experience. You can create guest sponsor roles and social logins for your guest networks. You can also design your guest landing page with custom logos, color, and banner text.
- Presence Analytics—Offers a value added service for Instant AP based networks to get an insight into user presence and loyalty. The Presence Analytics dashboard allows you to view the presence of users at a specific site and the frequency of user visits at a given location or site. Using this data, you can make business decisions to improve customer engagement.

Supported Web Browsers

To view the Aruba Central UI, ensure that JavaScript is enabled on the web browser.

Table 3: *Browser Compatibility Matrix*

Browser Versions	Operating System
Google Chrome 39.0.2171.65 or later	Windows and Mac OS
Mozilla Firefox 34.0.5 or later	Windows and Mac OS
Safari 7 or later	Mac OS
Microsoft Edge version 79 or later	Windows

Operational Modes and Interfaces

Aruba offers the following variants of the Aruba Central web interface:

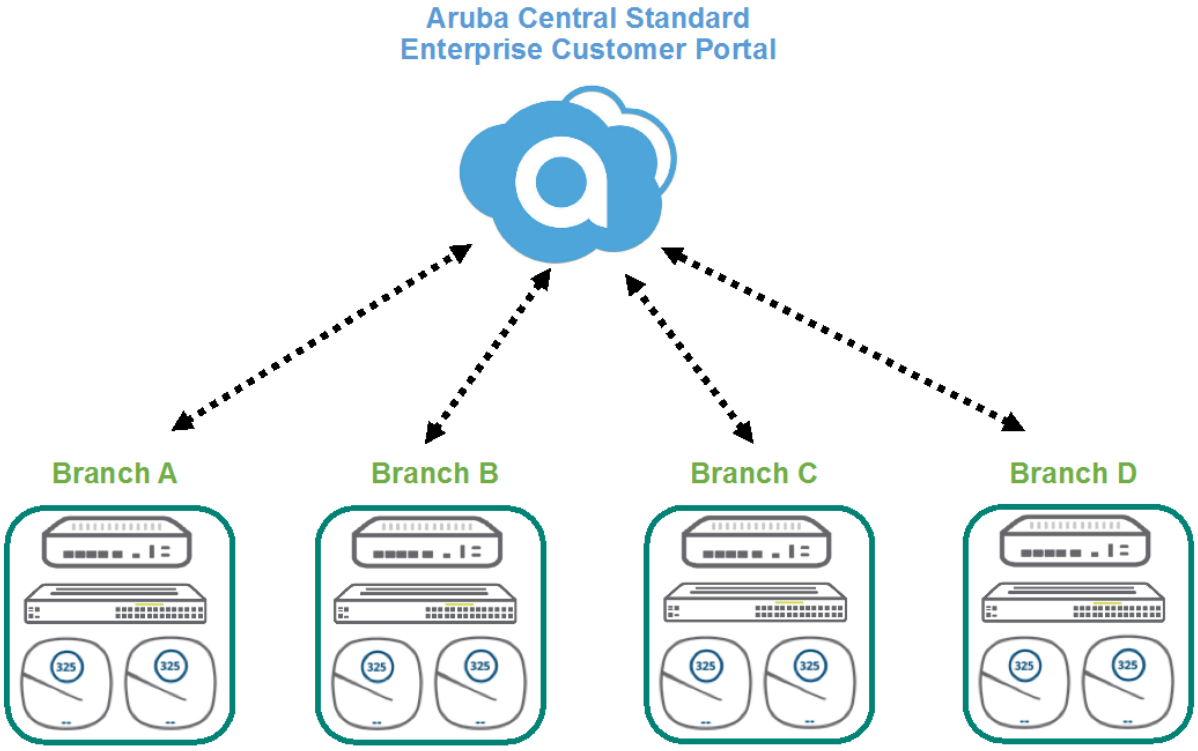
- Standard Enterprise Mode
- Managed Service Provider Mode

Standard Enterprise Mode

The Standard Enterprise interface is intended for users who manage their respective accounts end-to-end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision devices and subscriptions to manage their respective accounts.

The following figure illustrates a typical Standard Enterprise mode deployment.

Figure 1 *Standard Enterprise Mode*

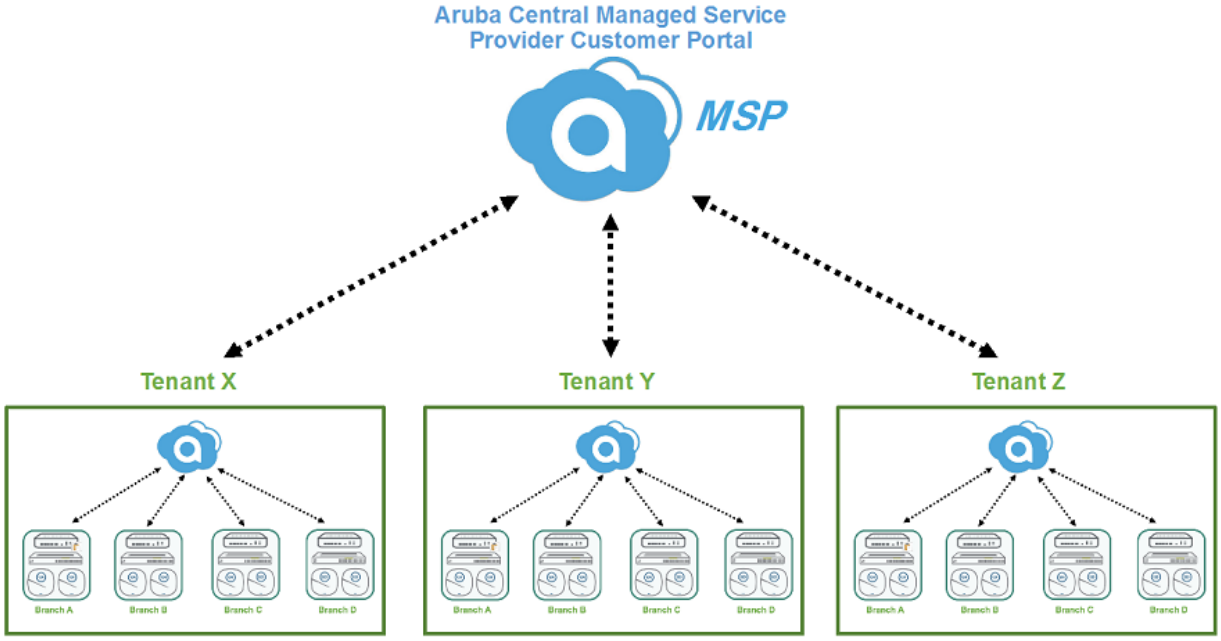


Managed Service Provider Mode

Aruba Central offers the MSP mode for managed service providers who need to manage multiple customer networks. The MSP administrators can provision tenant accounts, allocate devices, assign licenses, and monitor tenant accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. Tenants can access only their respective accounts, and only those features and application services to which they have subscribed.

The following figure illustrates a typical MSP mode deployment.

Figure 2 *Managed Service Provider Mode*



Supported Devices

This section provides the following information:

- Supported Instant APs
- Supported AOS-Switch Platforms
- Supported AOS-CX Platforms
- Supported SD-Branch Components
- Supported 4G Modems for Aruba SD-Branch

Supported Instant APs

The following table lists the Instant AP platforms, the installation mode, the minimum supported Aruba Instant software versions, and the Instant APs supporting power draw:

Table 4: *Supported Instant AP Platforms*

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version	Power Draw Support
AP-567EX	Outdoor	Aruba Instant 8.7.1.0	No
AP-567	Outdoor	Aruba Instant 8.7.1.0	Yes
AP-565EX	Outdoor	Aruba Instant 8.7.1.0	No
AP-565	Outdoor	Aruba Instant 8.7.1.0	Yes
AP-503H	Indoor	Aruba Instant 8.7.1.0	Yes

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version	Power Draw Support
AP 577EX	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-577	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-575EX	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-575	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-574	Outdoor	Aruba Instant 8.7.0.0	Yes
AP 518	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-505H	Indoor	Aruba Instant 8.7.0.0	Yes
AP-505	Indoor	Aruba Instant 8.6.0.0	Yes
AP-504	Indoor	Aruba Instant 8.6.0.0	Yes
AP-555	Indoor	Aruba Instant 8.5.0.0	No
AP-535	Indoor	Aruba Instant 8.5.0.0	No
AP 534	Indoor	Aruba Instant 8.5.0.0	No
AP 515	Indoor	Aruba Instant 8.4.0.0	Yes
AP-514	Indoor	Aruba Instant 8.4.0.0	Yes
AP-387	Outdoor	Aruba Instant 8.4.0.0	Yes
AP-303P	Indoor	Aruba Instant 8.4.0.0	No
AP-377EX	Outdoor	Aruba Instant 8.3.0.0	No
AP-377	Outdoor	Aruba Instant 8.3.0.0	Yes
AP-375EX	Outdoor	Aruba Instant 8.3.0.0	No
AP-375	Outdoor	Aruba Instant 8.3.0.0	Yes
AP-374	Outdoor	Aruba Instant 8.3.0.0	Yes
AP-345	Indoor	Aruba Instant 8.3.0.0	Yes
AP-344	Indoor	Aruba Instant 8.3.0.0	Yes
AP-318	Indoor	Aruba Instant 8.3.0.0	Yes
AP-303	Indoor	Aruba Instant 8.3.0.0	No
AP-203H	Indoor	Aruba Instant 6.5.3.0	No
AP-367	Outdoor	Aruba Instant 6.5.2.0	No

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version	Power Draw Support
AP-365	Outdoor	Aruba Instant 6.5.2.0	No
AP-303HR	Indoor	Aruba Instant 6.5.2.0	No
AP-303H	Indoor	Aruba Instant 6.5.2.0	Yes
AP-203RP	Indoor	Aruba Instant 6.5.2.0	No
AP-203R	Indoor	Aruba Instant 6.5.2.0	No
IAP-305	Indoor	Aruba Instant 6.5.1.0-4.3.1.0	Yes
IAP-304	Indoor	Aruba Instant 6.5.1.0-4.3.1.0	Yes
IAP-207	Indoor	Aruba Instant 6.5.1.0-4.3.1.0	No
IAP-335	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	Yes
IAP-334	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	Yes
IAP-315	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	No
IAP-314	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	Yes
IAP-325	Indoor	Aruba Instant 6.4.4.3-4.2.2.0	No
IAP-324	Indoor	Aruba Instant 6.4.4.3-4.2.2.0	No
IAP-277	Outdoor	Aruba Instant 6.4.3.1-4.2.0.0	No
IAP-228	Indoor	Aruba Instant 6.4.3.1-4.2.0.0	No
IAP-205H	Indoor	Aruba Instant 6.4.3.1-4.2.0.0	No
IAP-215	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-214	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-205	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-204	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-275	Outdoor	Aruba Instant 6.4.0.2-4.1.0.0	No
IAP-274	Outdoor	Aruba Instant 6.4.0.2-4.1.0.0	No
IAP-103	Indoor	Aruba Instant 6.4.0.2-4.1.0.0	No
IAP-225	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No
IAP-224	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No
IAP-115	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version	Power Draw Support
IAP-114	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No
RAP-155P	Indoor	Aruba Instant 6.2.1.0-3.3.0.0	No
RAP-155	Indoor	Aruba Instant 6.2.1.0-3.3.0.0	No
RAP-109	Indoor	Aruba Instant 6.2.0.0-3.2.0.0	No
RAP-108	Indoor	Aruba Instant 6.2.0.0-3.2.0.0	No
RAP-3WN	Indoor	Aruba Instant 6.1.3.1-3.0.0.0	No
RAP-3WNP	Indoor	Aruba Instant 6.1.3.1-3.0.0.0	No

- RAP-155, RAP-155P, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277 IAPs are no longer supported from Aruba Instant 8.7.0.0 onwards.
- IAP-103, RAP-108, RAP-109, IAP-114, IAP-115, IAP-204, IAP-205, and IAP-205H IAPs are no longer supported from Aruba Instant 8.3.0.0 onwards.
- By default, AP-318, AP-374, AP-375, and AP-377 IAPs have Eth1 as the uplink port and Eth0 as the downlink port. Aruba does not recommend you to upgrade these IAPs to Aruba Instant 8.5.0.0 or 8.5.0.1 firmware versions, as the upgrade process changes the uplink port from Eth1 to Eth0 port thereby making the devices unreachable.
- For more information about Aruba's End-of-life policy and the timelines for hardware and software products at the end of their lives, see: https://www.arubanetworks.com/support-services/end-of-life/.
- Data sheets and technical specifications for the supported AP platforms are available at: https://www.arubanetworks.com/products/networking/access-points/.

Supported AOS-Switch Platforms

- Aruba Central uses the SSL certificate by GeoTrust Certificate Authority for device termination and web services. As the SSL certificate is about to expire, Aruba is replacing it with a new certificate from another trusted Certificate Authority. During the certificate upgrade window, all devices managed by Aruba Central will be disconnected. After the upgrade, the devices reconnect to Aruba Central and resume their services with Aruba Central. However, for AOS-Switches to reconnect to Aruba Central after the certificate upgrade, you must ensure that the switches are upgraded to the recommended software version listed in Table 5.
- Aruba Central does not support switch software versions below 16.08 release for firmware upgrade. In addition, only the latest three switch software versions of all major release versions will be available for firmware upgrade from Aruba Central. For example, if the latest switch software version released is 16.10.0011, the following versions will be available for firmware upgrade: 16.10.0009, 16.10.0010 and 16.10.0011.
- Changing AOS-Switches firmware from latest version to earlier major versions is not recommended if the switches are managed in UI groups. For features that are not supported or not managed in Aruba Central on earlier AOS-Switch versions, changing firmware to earlier major versions might result in loss of configuration.

The following tables list the switch platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 5: *Supported AOS-Switch Series, Software Versions, and Switch Stacking*

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2530 Switch Series	YA/YB.16.05.0008 or later	YA/YB.16.10.0013	N/A	N/A	N/A
Aruba 2540 Switch Series	YC.16.03.0004 or later	YC.16.10.0013	N/A	N/A	N/A
Aruba 2920 Switch Series	WB.16.03.0004 or later	WB.16.10.0013	Yes **Switch Software Dependency**: WB.16.04.0008 or later	BPS	UI and Template
Aruba 2930F Switch Series	WC.16.03.0004 or later	WC.16.10.0014	Yes	VSF	UI and Template

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
			Switch Software Dependency: WC.16.07.0002 or later		
Aruba 2930M Switch Series	WC.16.04.0008 or later	WC.16.10.0014	Yes **Switch Software Dependency**: WC.16.06.0006 or later	BPS	UI and Template
Aruba 3810 Switch Series	KB.16.03.0004 or later	KB.16.10.0014	Yes **Switch Software Dependency**: KB.16.07.0002 or later	BPS	UI and Template
Aruba 5400R Switch Series	KB.16.04.0008 or later	KB.16.10.0014	Yes **Switch Software Dependency**: KB.16.06.0008 or later	VSF	Template only

Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central.

Table 6: *Supported Aruba Mobility Access Switch Series and Software Versions*

Mobility Access Switch Series	Supported Software Versions
■ S1500-12P ■ S1500-24P ■ S2500-24P ■ S3500-24T	ArubaOS 7.3.2.6 ArubaOS 7.4.0.3 ArubaOS 7.4.0.4 ArubaOS 7.4.0.5 ArubaOS 7.4.0.6

Data sheets and technical specifications for the supported switch platforms are available at: https://www.arubanetworks.com/products/networking/switches/

Supported AOS-CX Platforms

To manage your AOS-CX switches using Aruba Central, ensure that the switch software is upgraded to 10.05.0021 or a later version. AOS-CX switches with version 10.05.0021 or earlier might not connect to Aruba Central after ten days of operation. You must upgrade the AOS-CX switch to a recommended software version to connect to Aruba Central.

The following table lists the AOS-CX platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 7: *Supported AOS-CX Switch Series, Software Versions, and Switch Stacking*

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type	Maximum Number of Stack Members	Supported Configuration Group Type (UI / Template)
AOS-CX 6100 Switch Series	10.06.0110 or later	10.06.0110	-N/A-	-N/A-	-N/A-	Template only
AOS-CX 6200 Switch Series	10.05.0021	10.06.0101	Yes **Switch Software Dependency**: 10.05.0021	VSF	8	UI and Template
AOS-CX 6300 Switch Series	10.05.0021	10.06.0101	Yes **Switch Software Dependency**: 10.05.0021	VSF	10	UI and Template
AOS-CX 6300 Switch Series [JL762A] Back 2 Front Power Supply SKU only	10.06.0001 or later	10.06.0101	Yes **Switch Software Dependency**: 10.05.0021	VSF	10	UI and Template
AOS-CX 6405 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	Template only
AOS-CX 6410 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	Template only

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type	Maximum Number of Stack Members	Supported Configuration Group Type (UI / Template)
AOS-CX 8320 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8325 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8360 Switch Series	10.06.0001 or later	10.06.0101	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8400 Switch Series	10.06.0001 or later	10.06.0101	-N/A-	-N/A-	-N/A-	Template only

Provisioning and configuring of AOS-CX 6405, 6410, and 8400 switch series and switch stacks is supported only through configuration templates.

Data sheets and technical specifications for the supported switch platforms are available at: https://www.arubanetworks.com/products/networking/switches/.

Supported SD-Branch Components

The Aruba SD-WAN Gateway portfolio includes Aruba Gateways that function as Branch Gateways and VPNCs.

The following table lists the Aruba Gateway platforms and ArubaOS software versions that function as Branch Gateways:

Table 8: *Supported Aruba Gateways*

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 9004-LTE	ArubaOS 8.5.0.0-2.1.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.1.0.0
Aruba 9012	ArubaOS 8.5.0.0-2.0.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.0.0.4
Aruba 9004	ArubaOS 8.5.0.0-1.0.7.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.0.0.4
Aruba 7210, 7220, and 7240XM	ArubaOS 8.5.0.0-2.0.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.0.0.4

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 7030	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7024	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7010	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7008	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7005	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4

The following table lists the Aruba Gateway platforms and ArubaOS software versions that function as VPNCs:

Table 9: *Supported Aruba VPNCs*

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 9004	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0
Aruba 9012	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0
Aruba 7280	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7240XM	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7220	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7210	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
vGW-4G	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
vGW-2G	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
vGW-500M	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7030	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4

Table 9: *Supported Aruba VPNCs*

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 7024	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7010	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4

Aruba Virtual Gateways also function as VPNCs. The minimum supported software version for Virtual Gateways is ArubaOS 8.1.0.0-1.0.4.1.

Aruba 9012 Gateway supports traffic inspection while deployed as a VPNC.

Data sheets and technical specifications for the supported Gateways are available at:
https://www.arubanetworks.com/products/networking/gateways-and-controllers/

Supported 4G Modems for Aruba SD-Branch

The following table lists the 4G modems that are supported on the Aruba Branch Gateways:

Table 10: *Supported 4G Modems for Aruba SD-Branch*

USB 4G Modem Model	Carrier Support
Inseego Skyus SC4V	Verizon
Inseego Skyus SC4A	AT&T
Digisol DG-BA4305	ROW
ZTE MF861	AT&T
Franklin Wireless U772	Sprint
Huawei E3372h-320	ROW
Huawei E3372s-153/ E3372h-153	ROW
Huawei E3372h-607	ROW
Huawei E8372h-153	ROW
Huawei E8372h-608	ROW
Huawei E8372h-511	T-Mobile
Huawei E8372h-517	T-Mobile
Huawei E3276-500	ROW
Huawei K5160	ROW
ZTE MF79S	ROW

USB 4G Modem Model	Carrier Support
ZTE MF825C	ROW
ZTE MF831	ROW
ZTE MF832S	ROW
ZTE MF832U	ROW
ZTE MF823	ROW
Huawei E3276-150	ROW
Novatel (Inseego) U620L	Verizon

ROW (Rest of the World) indicates that the modem can be used outside of the United States region. However, the list of supported carriers and supported countries for the modem may vary. To select a modem for a specific country and carrier, refer to the modem documentation.

Thank you for choosing Aruba Central as your network management solution!

Before you get started with Aruba Central, we recommend that you review the Key capabilities of Aruba Central and the list of Aruba devices supported in Aruba Central.

Key Terms and Concepts

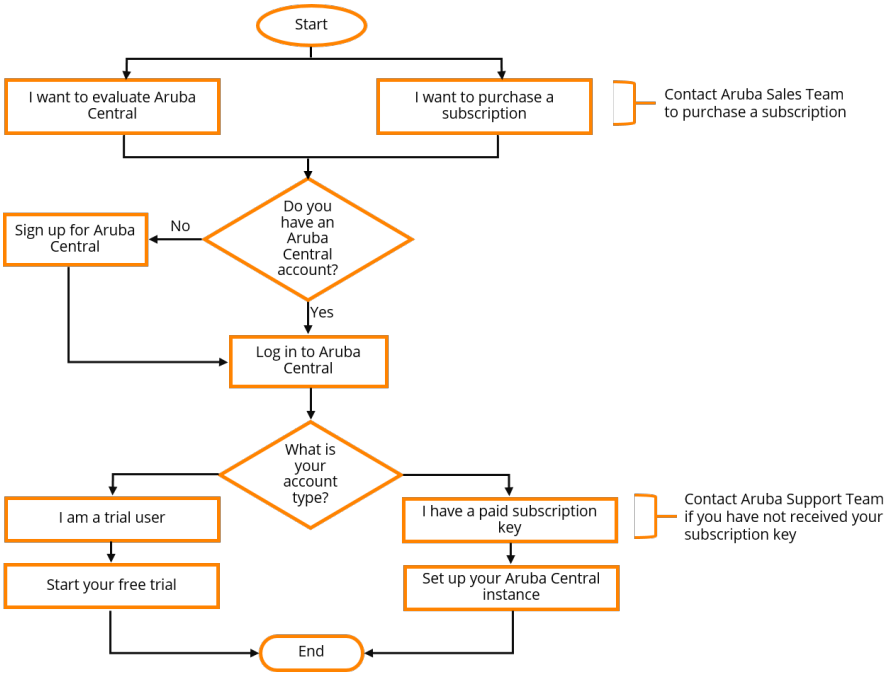
Take a few minutes to familiarize yourself with the key terms and concepts used in the help topics.

Cluster Zone	Refers to an Aruba Central deployment area within a specific region. In other words, cluster zones are regional grouping of one or more container instances on which Aruba Central is deployed. Cluster zones allow your deployments to restrict customer data to a specific region and plan time zone specific maintenance windows. Each cluster zone has separate URLs for signing up for Aruba Central, accessing Aruba Central portal, and for allowing devices to communicate with Aruba Central. To view the zone in Aruba Central UI, click the **User Settings** menu at the bottom of the left navigation pane.
Enterprise Mode	Refers to the Aruba Central solution deployment mode in which the customers provision, manage, and maintain their networks end-to-end for their respective organizations or businesses.
Managed Services Mode	Refers to the Aruba Central deployment mode in which the service providers, resellers, administrators, and retailers to centrally manage and monitor multiple tenant or end-customer accounts from a single management interface.
Subscription	Refers to the license granted to a customer for using a product or service.
Evaluation Account	Refers to the Aruba Central account created for evaluating Aruba Central solution and its services.
Paid Subscriber	Refers to the customers who have purchased a subscription to obtain access to Aruba Central and its services.
Subscription Key	Refers to the license key. A subscription key is a 14-character alphanumeric string; for example, PQREWD6ADWERAS.
Customer ID Subscriber ID	Refers to the identity number of your Aruba Central account. To view your subscriber ID, click the **User Settings** menu at the bottom of the left navigation pane in the Aruba Central UI.
Zero Touch Provisioning	Refers to one of the following: ▪ Zero Touch Provisioning of Aruba Central accounts— When you purchase a subscription key and add this subscription key in Aruba Central, Aruba Central queries the Aruba Activate database to retrieve the devices mapped to your purchase order and add these devices to the inventory. This process is referred to as zero touch provisioning in Aruba Central. ▪ Zero Touch Provisioning of Devices—Most Aruba devices support self-provisioning; that is, when you connect a device to a provisioning network, it can automatically download provisioning parameters from the Activate server and connect to their management entity.

Onboarding	Refers to the process of importing devices to Aruba Central's device inventory, activating subscriptions, and making devices available for management from Aruba Central.
Device Sync	Refers to the process of synchronizing devices from the Activate database. The device sync operation allows Aruba Central to retrieve devices from Activate and automatically add these devices to the device inventory in Aruba Central.
Provisioning	Refers to the process of setting up a device for deploying networks as per the configuration requirements of your organization.
Group	Refers to the device configuration container in Aruba Central. You can combine devices with common configuration requirements into a single group and apply the same configuration to all the devices in that group.
Site	Refers to the physical locations where devices are installed. Organizing devices per sites allows you to filter your dashboard view per site.
Label	Refers to the tags used for logically grouping devices based on various parameters such as ownership, specific areas within a site, departments, and so on.

Workflow Summary

The following illustration summarizes the steps required for getting started with Aruba Central:



Navigate through the following topics to know more about the onboarding and provisioning procedures:

- Creating an Aruba Central Account
- Accessing Aruba Central Portal
- Starting Your Free Trial
- Setting up Your Aruba Central Instance

Creating an Aruba Central Account

To start using Aruba Central, you need to register and create an Aruba Central account. Both evaluating and paid subscribers require an account to start using Aruba Central.

Zones and Sign-Up URLs

Aruba Central instances are available on multiple regional clusters. These regional clusters are referred to as zones. When you register for an Aruba Central account, Aruba creates an account for you in the zone that is mapped to the country you selected during registration.

To create an Aruba Central account in the zone that is mapped to your country, use the following zone-specific sign-up URLs.

Table 11: *Sign-Up URLs & Apps*

Regional Cluster	Sign-Up URL	Available Apps
US-1	https://portal.central.arubanetworks.com/signup	**Network Operations**
US-2	https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/	▪ **Network Operations** ▪ **ClearPass Device Insight**
Canada-1	https://portal-ca.central.arubanetworks.com/signup	**Network Operations**
China-1	https://portal.central.arubanetworks.com.cn/signup	**Network Operations**
EU-1	https://portal-eu.central.arubanetworks.com/signup	▪ **Network Operations** ▪ **ClearPass Device Insight**
APAC-1	https://portal-apac.central.arubanetworks.com/signup	**Network Operations**
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/signup	**Network Operations**
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com/signup	**Network Operations**

Signing up for an Aruba Central Account

You can choose one of the following ways to start your Aruba Central account trail:

1. Open the following page in a supported browser window:http://www.arubanetworks.com/products/sme/eval/.
   a. Click **Start the Central Demo**. The Aruba Central Demo page is displayed.
   b. Fill the form to start a product demo, and click **Start Demo**.
   c. The Aruba Central Account Home page is displayed.
2. Use the sign-up URL for your region from Sign-Up URLs & Apps and complete the following steps:
   a. Enter your email address. Based on the email address you entered, the **Registration** page guides you to the subsequent steps:

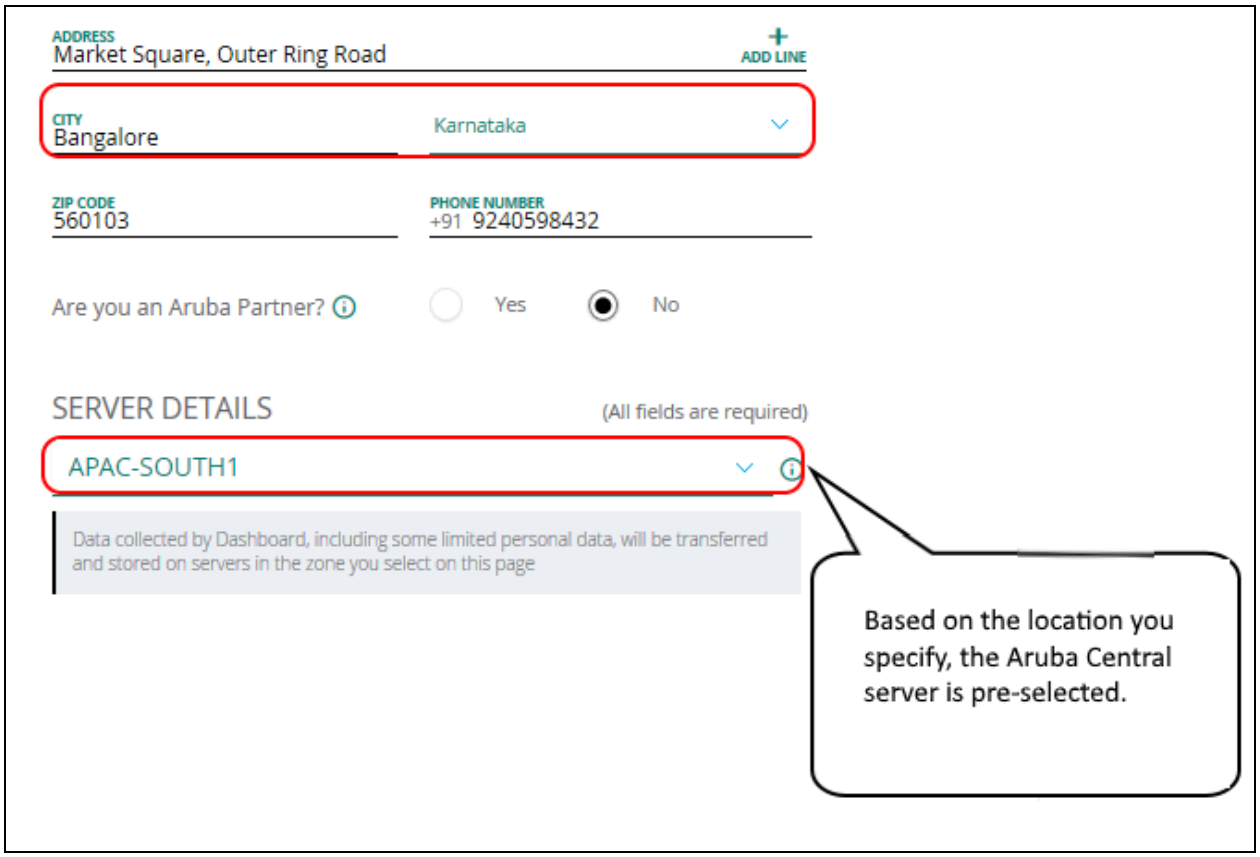
Table 12: *Registration Workflow*

If...	Then...
If you are a new user:	The **Registration** page prompts you to create a password. To continue with the registration, enter a password in the **Password** and **Confirm Password** fields.
If you are an existing Aruba customer, but you do not have an Aruba Central account: If your email account is already registered with Aruba, but you do not have an Aruba Central account:	The **Registration** page displays the following message: **Email already exists. Please enter the password below**. To continue with registration, validate your account: 1. Enter the password. 2. Click **Validate Account**. **NOTE:** If you do not remember the password, click **Forgot Password** to reset the password.
If you are invited to join as a user in an existing Aruba Central customer account:	The **Registration** page displays the following message: **An invitation email has already been sent to your email ID. Resend**. To continue with the registration: 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the **Registration** page and click **Resend**. A registration invitation will be sent your account. 3. Click the registration link. The user account is validated. 4. Complete the registration on the **Sign Up** page to sign in to Aruba Central.
If you are a registered user of Aruba Central and have not verified your email yet:	The **Registration** page displays the following message: **You are an existing Aruba Central user. Please verify your account. Resend Verification email**. To continue: 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the **Registration** page and click **Resend Verification email**. A registration invitation will be sent your account. 3. Click the account activation link. 4. After the email verification is completed successfully, click **Log in** to access Aruba Central.
If you are already a registered user of Aruba Central and have verified your email:	The **Registration** page displays the following message: **User has been registered and verified. Sign in to Central**. Click **Sign in to Central** to skip the registration process and access the Aruba Central portal.

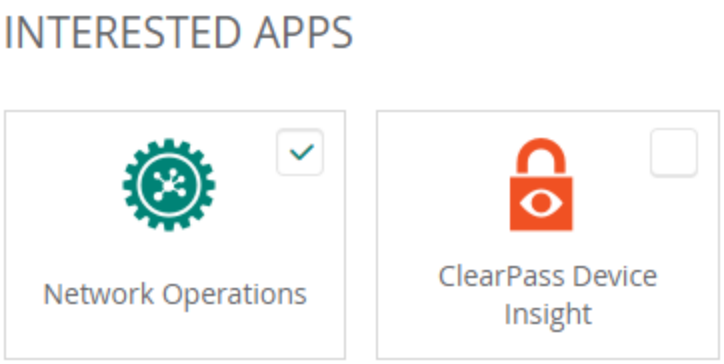
Table 12: *Registration Workflow*

If...	Then...
If your email address is in the **arubanetworks.com** or **hpe.com** domain:	The **Single Sign-On** option is enabled. You can use your respective Aruba or HP Enterprise credentials to log in to your Aruba Central account after the registration.

b. To continue with registration, enter your first name, last name, company name, address, country, state, ZIP code, and phone details.
c. Specify if you are an Aruba partner.
d. Ensure that you select an appropriate zone. The **Registration** page displays a list of zones in which the Aruba Central servers are available for account creation. Based on the country you select, the Aruba Central server is automatically selected. If you want your account and Aruba Central data to reside on a server from another zone, you can select an Aruba Central server from the list of available servers.



e. From the **Interested Apps** section, select the app(s) that you want to pre-provision. You must select at least one app to continue:
   - **Network Operations**
   - **ClearPass Device Insight**

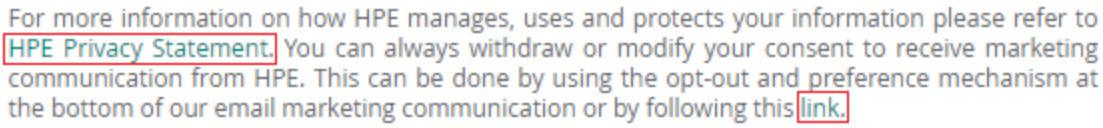


See Table 11 for the app(s) available in the zone in which you are signing up.

NOTE

If you are interested in evaluating the Aruba Central MSP solution, select only the **Network Operations** app.

f. Select the **I agree to the Terms and Conditions** check box.
g. Set a preferred mode of communication for receiving notifications about Aruba products and services.
h. Optionally, to read about the privacy statement, click the **HPE Privacy Statement** link. To opt out of marketing communication, you can either click the unsubscribe link available at the bottom of the email or click the link as shown in the following figure:



i. Click **Sign Up**. Your new account is created in the zone you selected and an email invitation is sent to your email address for account activation.
j. Access your email account and click the **Activate Your Account** link. After you verify your email, you can log in to Aruba Central.

Accessing Aruba Central Portal

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central.

If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created.

Login URLs

When you try to access Aruba Central portal, you are redirected to the Aruba Central URL that is mapped to your cluster zone.

Table 13: *Cluster Zone— Portal URLs*

Regional Cluster	Login URL
US-1	https://portal.central.arubanetworks.com/platform/login/user

Regional Cluster	Login URL
US-2	https://portal-prod2.central.arubanetworks.com/platform/login/user
Canada-1	https://portal-ca.central.arubanetworks.com/platform/login/user
China-1	https://portal.central.arubanetworks.com.cnath/platform/login/user
EU-1	https://portal-eu.central.arubanetworks.com/platform/login/user
APAC-1	https://portal-apac.central.arubanetworks.com/platform/login/user
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/platform/login/user
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com/platform/login/user

Logging in to Aruba Central

To log in to Aruba Central:

1. Access the Aruba Central login URL for your zone.
2. Notice that the zone is automatically selected based on your geographical location.
3. Enter the email address and click **Continue**.
4. Log in using your credentials.

If your user credentials are stored in your organization's Identity Management server and SAML SSO authentication is enabled for your IdP on Aruba Central, complete the SSO authentication workflow.

5. Enter the password.

If you have forgotten password, you can click the **Forgot Password** and reset your password. The Forgot Password link resets only your Aruba Central account; hence, it is not available to SSO users.

6. Click **Continue**. The **Initial Setup** wizard opens.
   - If you have a paid subscription, click **Get Started** and set up your account.
   - If you are a trial user, click **Evaluate Now** and start your trial.

Changing Your Password

To change your Aruba Central account:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **Change Password**.
3. Enter a new password.
4. Log in to Aruba Central using the new password.

The **Change Password** menu option is not available for federated users who sign in to Aruba Central using their SSO credentials.

Logging Out of Aruba Central

To log out of Aruba Central:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **Logout**.

Accessing Aruba Central Mobile Application

Aruba Central mobile application lets you manage, monitor, and optimize your Central account. You can log in to your Aruba Central account using your credentials from the mobile application. To download the Aruba Central application, visit the App Store on iOS devices running iOS 9.0 or later and Google Play Store on Android devices running android 5.0 Lollipop or later.

About the Network Operations App User Interface

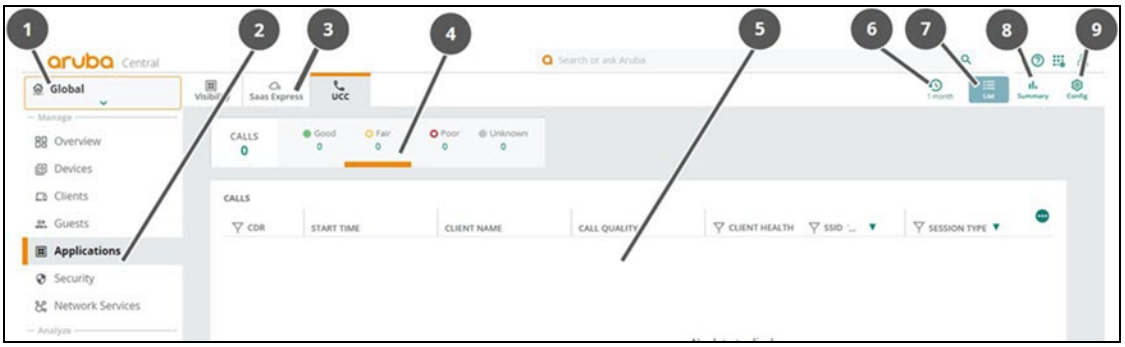
The **Network Operations** app is one of the apps in Aruba Central that helps to manage, monitor, and analyze your network.

Aruba offers the following variants of the **Network Operations** app user interface:

- **Standard Enterprise mode**— This mode is intended for customers who manage their respective accounts end-to- end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision and manage their respective accounts.
- **Managed Service Provider (MSP) mode**— This mode is for managed service providers who need to manage multiple customer networks. With MSP mode enabled, the MSP administrators can provision customer accounts, allocate devices, assign licenses, and monitor customer accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. The tenants can access only their respective accounts, and only those features and application services to which they have subscribed.

The following image displays the navigational elements of the **Network Operations** app in the Standard Enterprise mode. However, the navigational elements also apply to the MSP mode.

Figure 3 *Navigation Elements of the Network Operations App*



Callout Number	Description
1	Filter to select an option under **Groups**, **Labels**, **Sites**. For all devices, select **Global**. A corresponding dashboard is displayed.
2	Item under the left navigation contextual menu. The menu is dependent on the filter selection.
3	First-level tab on the dashboard.
4	Second-level tab on the dashboard.
5	Dashboard content for the selected view and filter. For example, the current dashboard in the image displays the **UCC** tab under **Manage** > **Applications** in the **List** view for the **Global** filter.
6	Time range filter. This is displayed for selected dashboards only.
7	**List** view to display tabular data for the selected filter. This is displayed for selected dashboards only.
8	**Summary** view to display charts for the selected filter. This is displayed for selected dashboards only.
9	**Config** view to enable configuration options for the selected filter. This is displayed for selected dashboards only.

Types of Dashboards in the Network Operations App

The **Network Operations** app uses a filter to set the dashboard context for the app. The menu for the left navigation pane changes according to the selected filter value. Selecting any item on the left navigation pane displays a corresponding dashboard. Accordingly, for different values of the filter, the content displayed for the left navigation menu and the dashboard context differs.

The dashboard for any item on the left navigation menu can have a combination of the following views:

- **Summary** view— Click the Summary **Summary** icon to display the summary dashboard. The summary dashboard displays a number of charts. For example, for the global dashboard, under **Manage**, the **Overview** > **Network Health** tab in **Summary** view displays a map of the available sites and their corresponding health. If available, use the time range filter to change the time-lines for the charts.
- **List** view— Click the List **List** icon to display tabular data for a selected dashboard. For example, for the global dashboard under **Manage**, the **Overview** > **Network Health** tab in **List** view displays a list of the available sites managed by Aruba Central. If available, use the time range filter to change the time-lines for the tabular data.
- **Config** view— Click the Config **Config** icon to enable the configuration options for a specific dashboard. For example, for the global dashboard under **Manage**, the **Applications** > **UCC** tab in **Config** view displays various configuration options for UCC.

Navigating to the Switch, Access Point, or Gateway Dashboard

In the **Network Operations** app, you can navigate to a device dashboard for a switch, access point, or gateway. The device dashboard enables you to monitor, troubleshoot, or configure a single device. In order

to do this, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, select one of the following options:
   - To view an access point dashboard, click the **Access Points** tab.
   - To view a switch dashboard, click the **Switches** tab.
   - To view a gateway dashboard, click the **Gateways** tab.

     The list of devices is displayed in **List** view.
3. Click a device listed under **Device Name**.

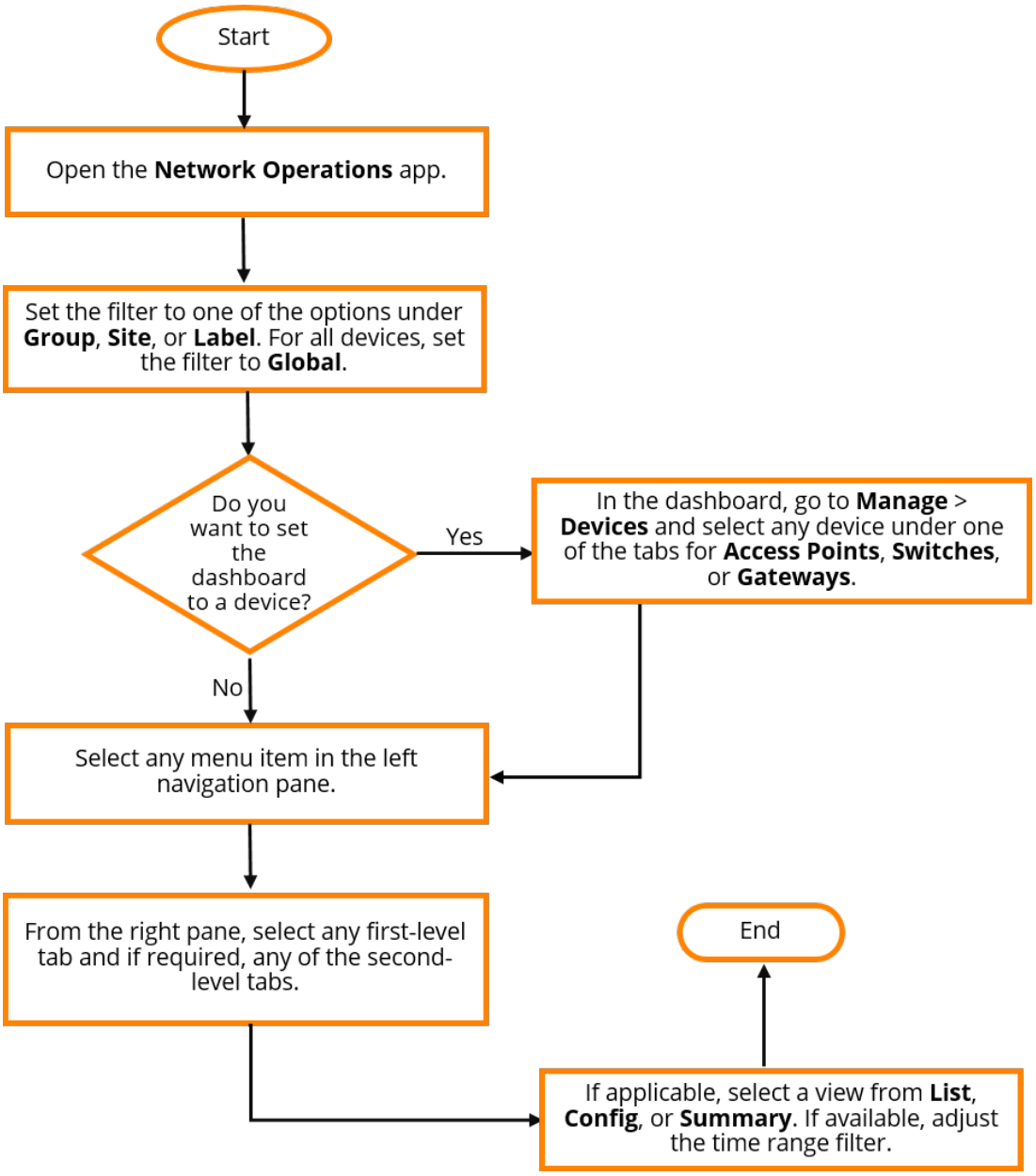
   The dashboard context for the specific device is displayed.

   To exit the device dashboard, click the back arrow on the filter.

Workflow to Configure, Monitor, or Troubleshoot in the Network Operations App

The following image displays a flowchart to help you navigate the **Network Operations** app to complete any task.

Figure 4 *Navigation Workflow for Network Operations App*



The Standard Enterprise Mode

This section discusses the user interface for the Standard Enterprise mode for the **Network Operations** app. This mode is intended for customers who manage their respective accounts end-to- end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision and manage their respective accounts.

The following topics are discussed in this section:

- Launching the Network Operations App
- Parts of the Network Operations App User Interface
- Search Bar
- Help Icon
- Account Home Icon

- User Icon
- Filter
- Time Range Filter
- Left Navigation Pane

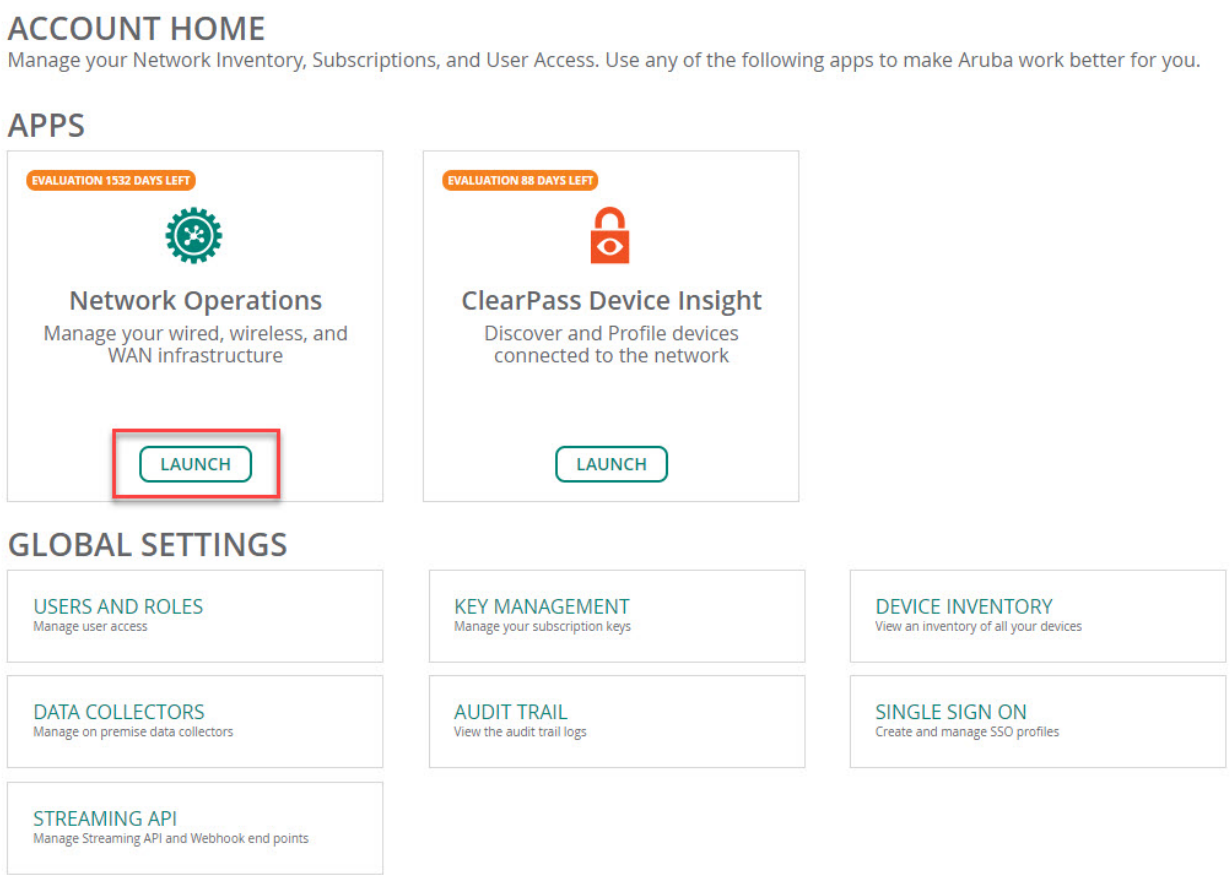
Launching the Network Operations App

If the **Network Operations** app is the only app provisioned, the **Network Operations** app is displayed at each user login. If there are a number of apps provisioned such as **Network Operations**, **ClearPass Device Insight** and so on, the **Account Home** page is displayed at each user login. From the **Account Home** page, you can manage network inventory, subscriptions, and user access.

In the event of multiple apps provisioned, perform the following steps to launch the **Network Operations** app:

1. Log in to the **Account Home** page.
   The **Account Home** page displays the apps and **Global Settings**
   For more information, see Accessing Aruba Central Portal.
2. Click **Launch** on the **Network Operations** tile.
   The **Network Operations** app is launched.

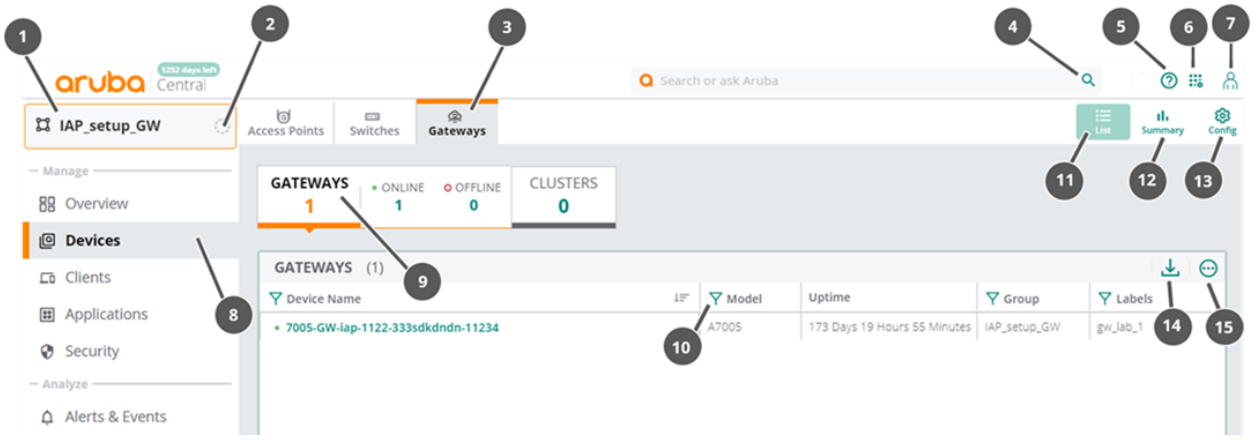
Figure 5 *Launching the **Network Operations** App*



Parts of the Network Operations App User Interface

After you launch the **Network Operations** app, the Standard Enterprise view is displayed.

Figure 6 *Parts of the Network Operations App*



Callout Number	Description
1	Filter to select an option under **Groups**, **Labels**, or **Sites**. For all devices, select **Global**. To select a specific device, see Navigating to the Switch, Access Point, or Gateway Dashboard. The example in the image shows the filter set to a group called "IAP_setup_GW". For more information, see Filter.
2	Health Bar for the selected filter. For more information, see The Health Bar.
3	First-level tab for the selected dashboard, corresponding to the selected item in the left navigation pane. The example in the image shows the first-level tab selection as **Gateways** under **Manage** > **Devices** for the group dashboard.
4	Search bar. For more information, see Search Bar.
5	Help icon. For more information, see Help Icon.
6	Account Home icon For more information, see Account Home Icon.
7	User settings icon. For more information, see User Icon.
8	Menu item under left navigation contextual menu. Menu is dependent on the filter selection. For more information, see Types of Dashboards in the Network Operations App.
9	Second-level tab for the dashboard, corresponding to the selected first-level tab. The example in the image shows the second-level tab selection as **Gateways** under **Manage** > **Devices** > **Gateways** for the group dashboard.

Callout Number	Description
10	Icon is for filtering the data of the selected column.
11	**List** icon. Click the **List** icon to view a tabular representation of the data. This icon is not available for all pages.
12	**Summary** icon. Click the **Summary** icon to view a graphical representation of the data. This icon is not available for all pages.
13	**Config** icon. Click the **Config** icon to enable configuration mode. This icon is not available for all pages.
14	Icon is for downloading the data of the selected page in CSV format.
15	Icon is for selecting or resetting the column headers for the selected page.

Search Bar

The search bar enables users to look for help information.

Help Icon

The help icon contains the following options:

- **Tutorials**—Displays the Aruba Central product learning center.
- **Feedback**—Allows you to provide feedback on the Aruba Central. You can choose the rating from the range of 1 to 10, where 1 being extremely unlikely and 10 being extremely likely and type your comment into the box and click **Submit** to submit the feedback.
- **Documentation Center**—Directs you to the online help documentation.
- **Get help on this page**—Selecting this option changes the appearance of some of the text on the UI to green italics. On the UI, when you point to the text in green italics, a dialog box displays the help information for that text. To disable this option, click **Done**.
- **Airheads Community**—Directs you to the Aruba support forum at https://community.arubanetworks.com/t5/Cloud-Managed-Networks/bd-p/CloudManagedNetworks.
- **View / Update Case**—Enables you to view or edit an existing support ticket in the Aruba Support Portal at https://asp.arubanetworks.com. You must log in to this portal.
- **Open New Case**—Enables you to create a new support ticket in the Aruba Support Portal at https://asp.arubanetworks.com. You must log in to this portal.

Account Home Icon

The Account Home icon enables you to go to the **Account Home** page and switch to another app if you have one subscribed. Most of the apps require service subscriptions to be enabled on the devices. Contact your administrator or the Aruba Central Support team to obtain access to an application service.

User Icon

The user icon enables you to view user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:

- **Switch Customer**—Enables you to switch to another account. This is especially required during troubleshooting scenarios.
- **Change Password**—Enables you to change the password of the account.
- **User Settings**
  - **Time Zone**—Displays the zone, date, time, and time zone of the region.
  - **Language**—Administrators can set a language preference. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
  - **Idle Timeout**—Administrators can set a timeout value for inactive user sessions in the Idle Timeout field. The value is in minutes.
  - **Get system maintenance notifications**—Administrators can select the check box to receive system maintenance notification on their registered email ID. Email notifications are sent before any scheduled maintenance activity or unplanned outage.
  - **Get software update notifications**—Administrators can select the check box to receive software update notification on their registered email ID.
- **Enable MSP**—Enables MSP mode and switches the user interface to the MSP mode. This option changes to Disable MSP when the MSP mode is enabled. You can select **Disable MSP** to switch to the Standard Enterprise interface. The MSP mode can be disabled only if there is no tenant data. The option is grayed out if there are any active tenant accounts.
- **Terms of Service**—Displays the terms and conditions for using Aruba Central services.
- **Logout**—Enables you to log out of from your account.

Filter

The filter enables you to set the dashboard context to a value under one of the following options:

- **Groups**—Sets the dashboard context to a group of devices.
- **Sites**—Sets the dashboard context to all a site.
- **Labels**—Sets the dashboard context to a label.

If no filter is applied, by default the filter is set to **Global** for all devices.

Use the search box in the filter to enter an available group, site, or label name and then select the option to set the filter.

Hovering over **Groups**, **Labels**, or **Sites** displays the associated config icon. Clicking on the config icon redirects you to **Maintain** > **Organization** in the global dashboard.

Time Range Filter

The time range filter enables you to set a time duration for showing monitoring and reports data. The option is displayed for selected dashboards only. You can set the filter to any of the following time ranges:

- 3 hours
- 1 day
- 1 week

- 1 month
- 3 months

Left Navigation Pane

The left navigation pane is a *contextual* menu that displays a number of configuration, monitoring, and troubleshooting options depending on filter value.

NOTE

This topic discusses the Network Operations app in MSP mode. To know more about the Account Home page, see the online Aruba Central documentation.

The MSP mode is intended for the managed service providers who manage multiple distinct tenant accounts. The MSP mode allows service providers to provision and manage tenant accounts, assign devices to tenant accounts, manage subscription keys and other functions such as configuring network profiles and viewing alerts.

Launching the Network Operations App for MSP

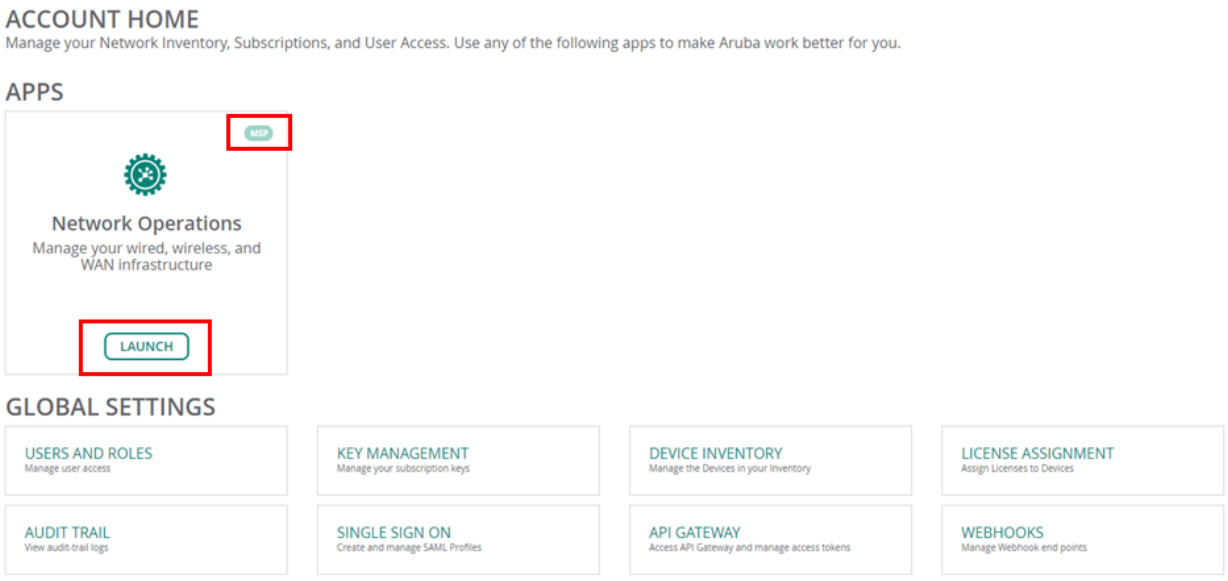
Aruba Central in MSP mode consists of the **Network Operations** app and the **Account Home** page.

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central. If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created. The Network Operations app is displayed at each user login to Aruba Central.

From the **Network Operations** app, you can navigate to the **Account Home** page by clicking the **Account Home** icon .

From the **Account Home** page, you can navigate to the **Network Operations** app by clicking the **Launch** button for the **Network Operations** tile.

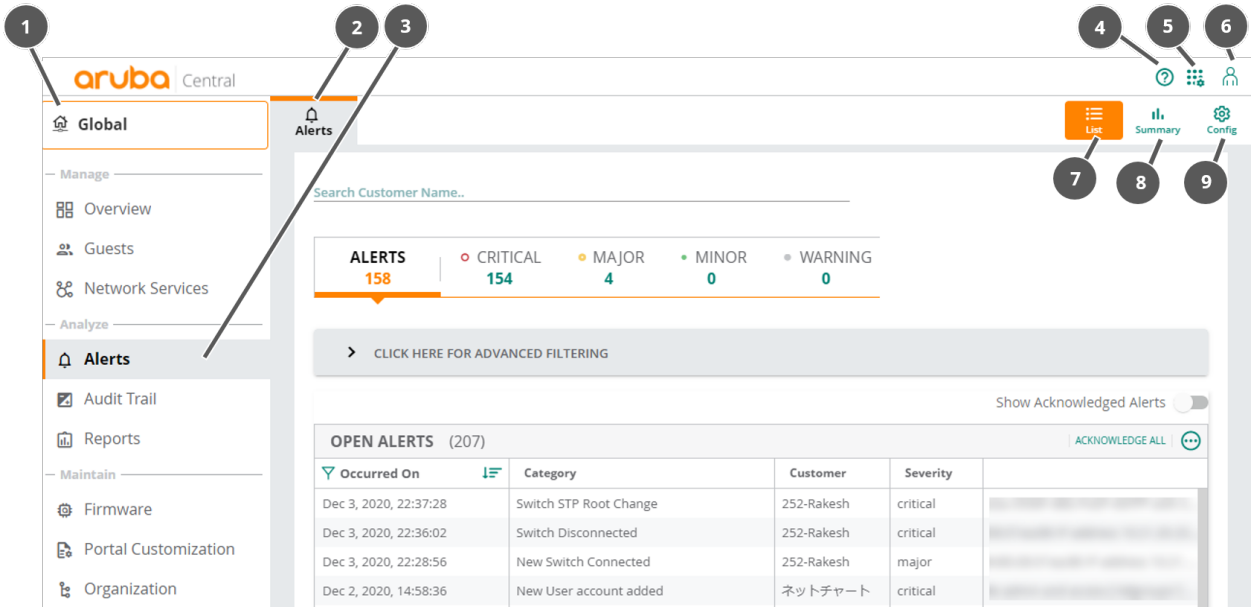
Figure 7 *Launching the Network Operations App for MSP from Account Home*



Parts of the Network Operations App for MSP

After you launch the **Network Operations** app, the MSP view opens.

Figure 8 *Parts of the Aruba Central User Interface for MSP*



Callout Number	Description
1	Filter to select a group or all groups. For more information, see Filter. Here, the global dashboard is displayed as the filter is set to **All Groups**.
2	First-level tab on dashboard. The dashboard may also have second and third-level tabs dependent on the filter selection.
3	Menu item under left navigation contextual menu. Menu is dependent on the filter selection.
4	Help icon. For more information, see Help Icon.
5	Account Home icon.
6	User Settings icon. For more information, see User Icon.
7	List view. Click the **List** icon to view a tabular representation of the data. Only applicable for the global dashboard.
8	Summary view. Click the **Summary** icon to view a graphical representation of the data. Only applicable for the global dashboard.
9	Config view. Click the **Config** icon to enable configuration mode.

Help Icon

The help icon contains the following options:

- **Get help on this page**— Selecting this option changes the appearance of some of the text on the UI to green italics. On the UI, when you point to the text in green italics, a dialog box displays the help information for that text. To disable this option, click **Done**.
- **Tutorials**— Displays the Aruba Central product learning center.
- **Feedback**— Allows you to provide feedback on the Aruba Central. You can choose the rating from the range of 1 to 10, where 1 being extremely unlikely and 10 being extremely likely and type your comment into the box and click **Submit** to submit the feedback.
- **Documentation Center**— Directs you to the online help documentation.
- **Airheads Community**— Directs you to the Aruba support forum.
- **View / Update Case**—Enables you to view or edit an existing support ticket in the Aruba Support Portal at https://asp.arubanetworks.com. You must log in to this portal.
- **Open New Case**— Enables you to create a new support ticket in the Aruba Support Portal at https://asp.arubanetworks.com. You must log in to this portal.

Account Home Icon

The Account Home icon enables you to go to the **Account Home** page.

User Icon

The user icon enables you to view user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:

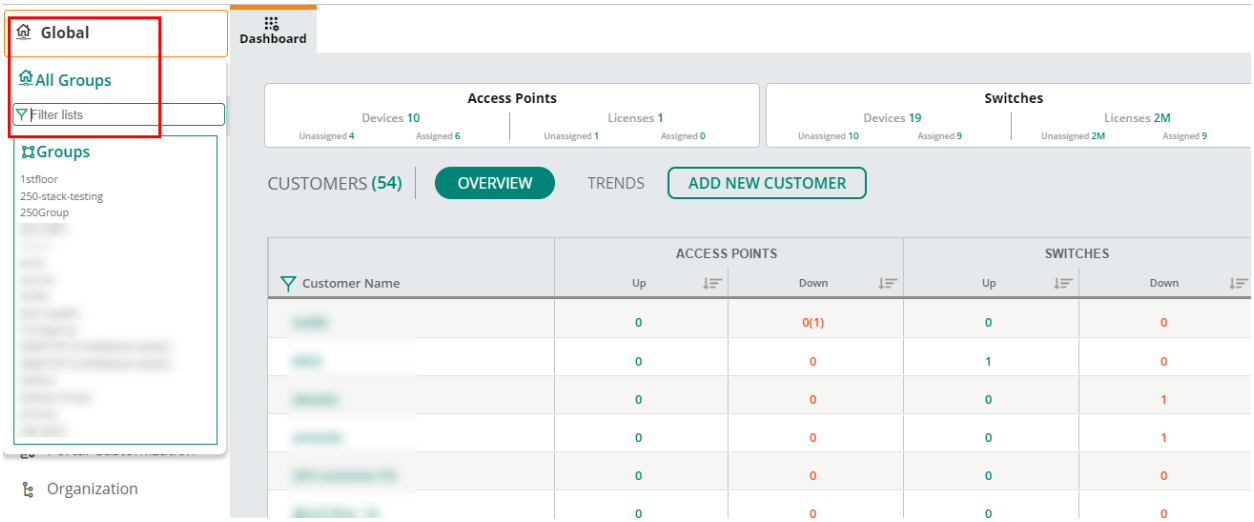
- **Switch Customer**— Enables you to switch to another account. This is especially required during troubleshooting scenarios.
- **Change Password**— Enables you to change the password of the account.
- **User Settings**
  - **Time Zone**— Displays the zone, date, time, and time zone of the region.
  - **Language**— Administrators can set a language preference. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
  - **Idle Timeout**— Administrators can set a timeout value for inactive user sessions in the Idle Timeout field. The value is in minutes.
  - **Get system maintenance notification**— Administrators can select the check box to get system maintenance notification.
  - **Get software update notifications**— Administrators can select the check box to get software update notification.
- **Disable MSP**— Disables MSP mode and switches the user interface to the standard enterprise mode. This option changes to **Enable MSP** when the MSP mode is disabled. You can select **Enable MSP** to switch to the MSP mode. The MSP mode can be disabled only if there is no tenant data. The option is grayed out if there are any active tenant accounts.
- **Terms of Service**— Displays the terms and conditions for using Aruba Central services.
- **Logout**— Enables you to log out of from your account.

Filter

The filter enables you to select a group or **All Groups** for performing specific configuration and monitoring tasks. If no filter is applied, by default the filter is set to **All Groups**. When you set the filter to

All Groups, the global dashboard is displayed and when you set the filter to a group, the group dashboard is displayed. You can type a group name to start your search for a filter value.

Figure 9 *MSP Filter set to Global on Selecting All Groups*



Time Range Filter

The time range filter enables you to set a time duration for showing monitoring and reports data. This time filter is not displayed when you view the configuration or device details. It is displayed only when you view monitoring data. You can set the filter to any of the following time ranges:

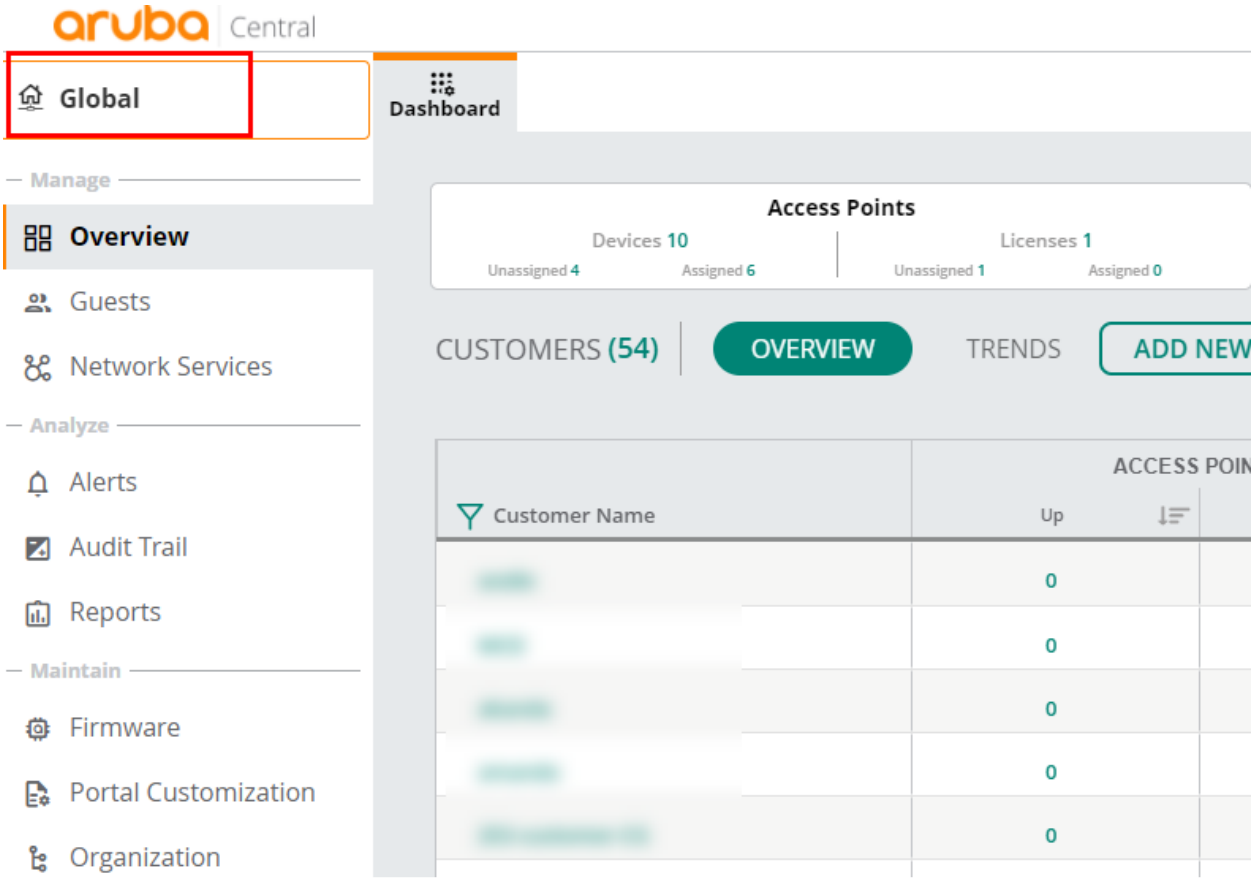
- 3 hours
- 1 day
- 1 week
- 1 month
- 3 months

The Global Dashboard in MSP Mode

In the **Network Operations** app in MSP mode, use the filter to select **All Groups**. The global dashboard is displayed.

In the global dashboard under the left navigation pane, you can see a number of menu items divided under the following categories: **Manage**, **Analyze**, and **Maintain**.

Figure 10 *Launching the Global Dashboard for MSP*



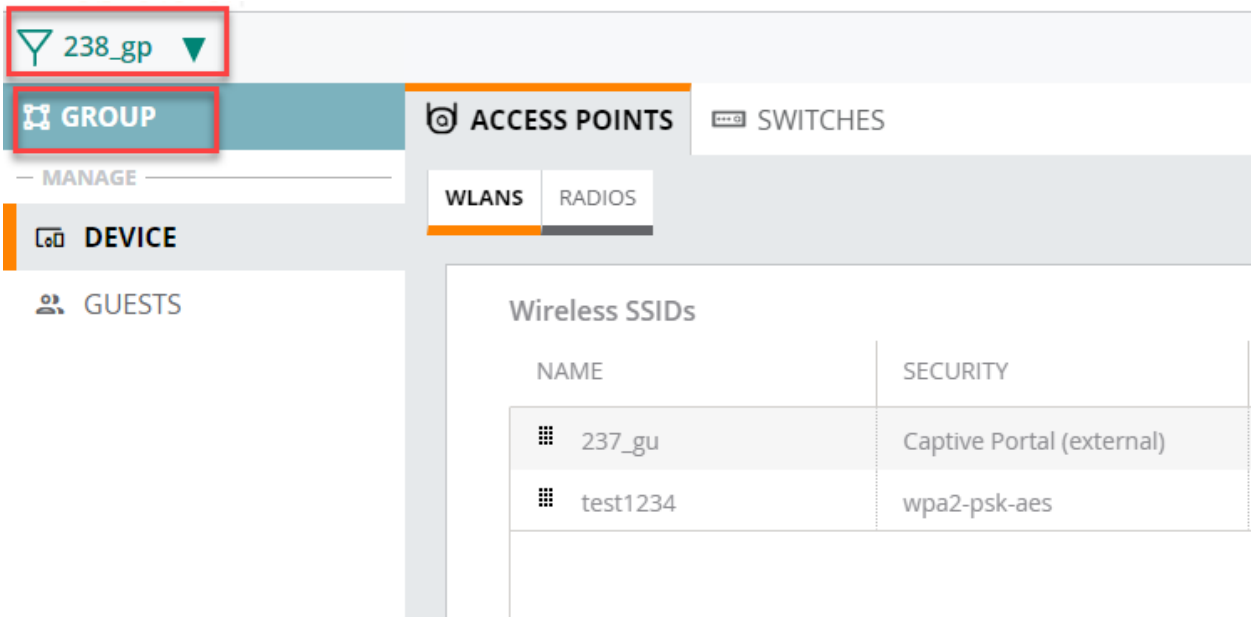
Selecting each menu item in the left navigation pane displays a corresponding dashboard with tabs. Each tab may support all or some of the following functions:

- **Summary** — Click the icon Summary to view a graphical representation of the data. Only applicable for the global dashboard.
- **List**— Click the icon List to view a tabular representation of the data. Only applicable for the global dashboard.
- **Config**— Click the icon Config to enable configuration mode.

The Group Dashboard in MSP Mode

In the **Network Operations** app in MSP mode, use the filter to select a group. The group dashboard is displayed.

Figure 11 *Launching the Group Dashboard for MSP*



NOTE

Some tabs or options may not be seen in your dashboard view if you are not an administrator for the Aruba Central account.

In the group dashboard under the left navigation pane, you can see the **Device** and **Guest** options under **Manage**.

Selecting an option in the left navigation pane displays a corresponding dashboard with tabs. Each tab supports the **Config** view that enables the configuration mode. The next sections discuss the left navigation menu items in the group dashboard.

The Health Bar

The Health Bar provides a snapshot of the overall health of the devices configured as part of the specific dashboard. The applicable dashboards include global, group, site, client, and device dashboards.

The topic discusses the following:

- Health Bar for the Global Dashboard
- Health Bar for the Group Dashboard
- Health Bar for the Site Dashboard
- Health Bar for the AP Dashboard
- Health Bar for the Switch Dashboard
- Health Bar Dashboard for the Gateway Dashboard
- Health Bar for the Wireless Client Dashboard
- Health Bar for the Wired Client Dashboard
- Health Bar for the Remote Client Dashboard

Viewing the Health Bar Dashboard

To view the Health Bar, perform the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
   - To select a client:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Clients**.

        A list of clients is displayed in the **List** view.
     c. Click a client listed under **Client Name**.

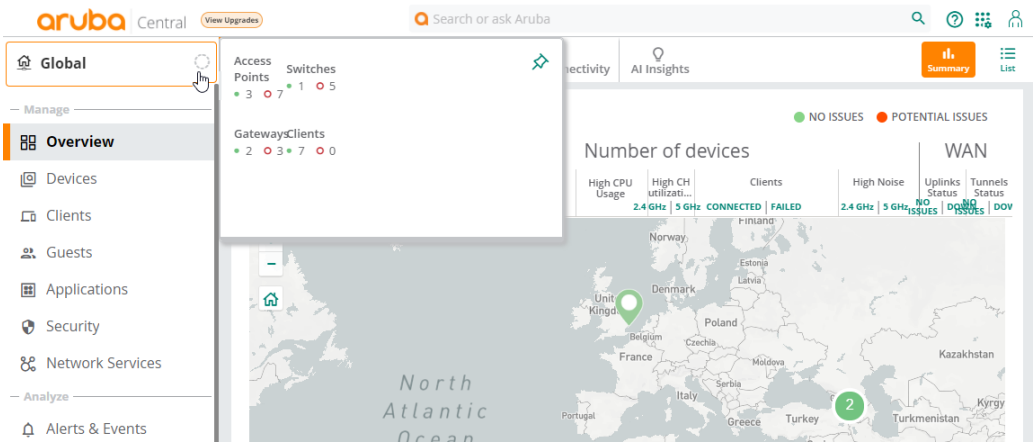
        The dashboard context for the client is displayed.

     The Health Bar icon displays the overall health of the network of the selected filter as either online or offline.
2. In the selected filter, click the Health Bar icon to expand the Health Bar dashboard.
3. Use the pin icon to pin the Health Bar dashboard to the **Network Operations** app display.

Health Bar for the Global Dashboard

The following image shows the Health Bar for the global dashboard.

Figure 12 *Expanded but Unpinned Health Bar in the Global Dashboard*



Health Bar Icons

Icon Type	Description
	This icon is specific to **Site**, **Device**, and **Client** dashboard. It indicates that there are no issues in the connection.
	This icon is specific to **Site**, **Device**, and **Client** dashboard. It indicates that there is an issue in the connection.
	This icon is specific to the **Global** and **Group** dashboards, and the health is not calculated at these levels.

Device and Clients Status Icons

Icon Type	Description
	■ For devices, indicates the number of devices that are online. ■ For clients, indicates the number of clients that are connected.
	■ For devices, indicates the number of devices that are offline. ■ For clients, indicates the number of failed clients. ■ For AI Insights, indicates the number of insights that are of high priority.
	For AI Insights, indicates the number of insights that are of medium priority.
	For AI Insights, indicates the number of insights that are of low priority.

The following table includes information on the various parameters of the Health Bar displayed for a global dashboard. The Health Bar in a global dashboard is in the context of all devices.

Parameter	Description
Access Points	■ Displays the number of access points that are online and the number of access points that are offline. ■ The number in green indicates the number of access points that are online. ■ Clicking the number in green redirects you to **Manage** > **Devices** > **Access Points** > **Online** in **List** view. ■ The number in red indicates the number of access points that are offline. ■ Clicking the number in red redirects you to **Manage** > **Devices** > **Access Points** > **Offline** in **List** view.
Switches	■ Displays the number of switches that are online and the number of switches that are offline. ■ The number in green indicates the number of switches that are online. ■ Clicking the number in green redirects you to **Manage** > **Devices** > **Switches** > **Online** in **List** view. ■ The number in red indicates the number of switches that are offline. ■ Clicking the number in red redirects you to **Manage** > **Devices** > **Switches** > **Offline** in **List** view.

Parameter	Description
Gateways	▪ Displays the number of gateways that are online and the number of gateways that are offline. ▪ The number in green indicates the number of gateways that are online. ▪ Clicking the number in green redirects you to **Manage** > **Devices** > **Gateways > Online** in **List** view. ▪ The number in red indicates the number of gateways that are offline. ▪ Clicking the number in red redirects you to **Manage** > **Devices** > **Gateways > Offline** in **List** view.
Clients	▪ Displays the number of clients that are connected and the number of clients that are failed. ▪ The number in green indicates the number of clients that are connected. ▪ The number in red indicates the number of clients that are failed. ▪ Clicking the numbers redirects you to **Manage** > **Clients** > **Clients** in **List** view.

Health Bar for the Group Dashboard

The following table includes information on the various parameters of the Health Bar displayed for a group dashboard. The Health Bar in a group dashboard is in the context of all devices configured as part of that group.

Parameter	Description
Access Points	▪ Displays the number of access points that are online and the number of access points that are offline. ▪ The number in green indicates the number of access points that are online. ▪ Clicking the number in green redirects you to **Manage** > **Devices** > **Access Points > Online** in **List** view. ▪ The number in red indicates the number of access points that are offline. ▪ Clicking the number in red redirects you to **Manage** > **Devices** > **Access Points > Offline** in **List** view.
Switches	▪ Displays the number of switches that are online and the number of switches that are offline. ▪ The number in green indicates the number of switches that are online. ▪ Clicking the number in green redirects you to **Manage** > **Devices** > **Switches > Online** in **List** view. ▪ The number in red indicates the number of switches that are offline. ▪ Clicking the number in red redirects you to **Manage** > **Devices** > **Switches > Offline** in **List** view.
Gateways	▪ Displays the number of gateways that are online and the number of gateways that are offline. ▪ The number in green indicates the number of gateways that are online. ▪ Clicking the number in green redirects you to **Manage** > **Devices** > **Gateways > Online** in **List** view. ▪ The number in red indicates the number of gateways that are offline. ▪ Clicking the number in red redirects you to **Manage** > **Devices** > **Gateways > Offline** in **List** view.

Parameter	Description
Clients	▪ Displays the number of clients that are connected and the number of clients that are failed. ▪ The number in green indicates the number of clients that are connected. ▪ The number in red indicates the number of clients that are failed. ▪ Clicking the numbers redirects you to **Manage** > **Clients** > **Clients** in **List** view.

Health Bar for the Site Dashboard

The following table includes information on the various parameters of the Health Bar displayed for a site dashboard. The Health Bar in a site dashboard is in the context of all devices configured as part of that site. The values are refreshed every minute.

The Health Bar icon indicating the site status changes to red when the value for one of the following parameters in the **List** view is greater than zero for the **Down** status:

- **Number of devices**
  - **Status**
  - **High Mem Usage**
  - **High CPU Usage**
  - **High CH Utilization**
  - **High Noise**
- **Uplink Status**
- **Tunnels Status**

Parameter	Description
Access Points	▪ Displays the number of access points that are online and the number of access points that are offline. ▪ The number in green indicates the number of access points that are online. ▪ Clicking the number in green redirects you to **Manage** > **Devices** > **Access Points > Online** in **List** view. ▪ The number in red indicates the number of access points that are offline. ▪ Clicking the number in red redirects you to **Manage** > **Devices** > **Access Points > Offline** in **List** view.
Switches	▪ Displays the number of switches that are online and the number of switches that are offline. ▪ The number in green indicates the number of switches that are online. ▪ Clicking the number in green redirects you to **Manage** > **Devices** > **Switches > Online** in **List** view. ▪ The number in red indicates the number of switches that are offline. ▪ Clicking the number in red redirects you to **Manage** > **Devices** > **Switches > Offline** in **List** view.
Gateways	▪ Displays the number of gateways that are online and the number of gateways that are offline. ▪ The number in green indicates the number of gateways that are online.

Parameter	Description
	■ Clicking the number in green redirects you to **Manage** > **Devices** > **Gateways > Online** in **List** view. ■ The number in red indicates the number of gateways that are offline. ■ Clicking the number in red redirects you to **Manage** > **Devices** > **Gateways > Offline** in **List** view.
Clients	■ Displays the number of clients that are connected and the number of clients that are failed for the last three hours. ■ The number in green indicates the number of clients that are connected. ■ The number in red indicates the number of clients that are failed. ■ Clicking the numbers redirects you to **Manage** > **Clients** > **Clients** in **List** view.
AI Insights	■ Displays the number of insights categorized by status. ■ The number in red indicates the insights are of high priority. ■ The number in orange indicates the insights are of medium priority. ■ The number in yellow indicates the insights are of low priority. ■ Clicking the numbers redirects you to **Manage** > **Overview** > **AI Insights** at the site context.

Health Bar for the AP Dashboard

The following table includes information on the various parameters of the Health Bar displayed for an AP. If the AP is not online and running, not all of the following data is available.

Parameter	Description
AP Status	■ Value can be **Online Since**, **Offline**, or **Operating under Thermal Management**. ■ If the value is **Online Since**, it also displays the time period, in the format of days-hours-minutes, for which the AP has been online and running. ■ When an AP operates under thermal management, the device health is displayed as **Poor** and the radios are in disabled mode. For more information, see Thermal Shutdown Support in IAP.
Device Health	■ Displays the performance of the AP in terms of the CPU and memory usage. ■ For example, the device health is **Good** when the CPU usage is less than or equal to 70% and the memory usage is less than or equal to 90%. If the value of the CPU and/or memory usage falls below the threshold, the device health is displayed as **Poor**. If the AP is down, the value is **Offline**. If the scenario is not applicable, a "-" sign is displayed. ■ Hover over the **Device Health** status to get the exact percentage value of the memory and CPU usage.
Radio 2.4 GHz	■ Displays the performance of the AP in terms of the channel utilization and noise floor in the 2.4 GHz channel. ■ For example, the device health is **Good** when the channel utilization is less than or equal to 70% and the noise floor is less than or equal to -80 dBm. If the value of the channel utilization and noise floor falls below the threshold, the device health is displayed as **Poor**. If the AP is online, but the radio is down, the value displayed is **Disabled**. If the scenario is not applicable, a "-" sign is displayed. ■ Hover over the **Radio 2.4 GHz** status to get the exact value of the channel utilization and

Parameter	Description
	noise floor.
Radio 5 GHz	▪ Displays the performance of the AP in terms of the channel utilization and noise floor in the 5 GHz channel. ▪ For example, the device health is **Good** when the channel utilization is less than or equal to 70% and the noise floor is less than or equal to -80 dBm. If the value of the channel utilization and noise floor falls below the threshold, the device health is displayed as **Poor** If the AP is online, but the radio is down, the value displayed is **Disabled**. If the scenario is not applicable, a "-" sign is displayed. ▪ Hover over the **Radio 5 GHz** status to get the exact value of the channel utilization and noise floor.
Radio 5 GHz (Secondary)	▪ Displays the performance of the AP in terms of the channel utilization and noise floor in the 5 GHz (Secondary) channel. ▪ For example, the device health is **Good** when the channel utilization is less than or equal to 70% and the noise floor is less than or equal to -80 dBm. If the value of the channel utilization and noise floor falls below the threshold, the device health is displayed as **Poor**. If the AP is online, but the radio is down, the value displayed is **Disabled**. If the scenario is not applicable, a "-" sign is displayed. ▪ Hover over the **Radio 5 GHz (Secondary)** status to get the exact value of the channel utilization and noise floor. **NOTE:** In the Health Bar dashboard, the **Radio 5 GHz (Secondary)** data is available only for AP-555 and only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.
Virtual Controller	Indicates if the AP is connected to a virtual controller. If the AP is connected, clicking on the virtual controller name redirects you to the **Manage** > **Overview** > **Summary** page for the virtual controller.

Health Bar for the Switch Dashboard

The following table includes information on the various parameters of the Health Bar displayed for a switch. If the switch is not online and running, not all of the following data is available.

Parameter	Description
Switch Status	Displays the time period for which the switch has been online and running or its offline status.
Device Health	▪ Displays the performance of the switch in terms of the CPU and memory usage. ▪ For example, the device health is **Good** when the CPU usage is less than or equal to 70% and the memory usage is less than or equal to 70%. If the value of the CPU and/or memory usage falls below the threshold, the device health is displayed as **Poor**. ▪ Hover over the **Device Health** status to get the exact percentage value of the memory and CPU usage.
Port - Status	▪ Displays the number of ports on the switch that are online and the number of ports that are offline. ▪ The number in green indicates the number of switch ports that are online.

Parameter	Description
	▪ The number in red indicates the number of switch ports that are offline.
Port - Alerts	▪ Displays the total number of open alerts.

Health Bar Dashboard for the Gateway Dashboard

The following table includes information on the various parameters of the Health Bar displayed for a gateway. If the gateway is not online and running, not all of the following data is available.

Parameter	Description
Gateway Status	Displays the time period, in the format of days-hours-minutes, for which the gateway has been running or its offline status.
WAN	▪ Displays the number of WAN ports as online or offline. ▪ The number in green indicates the number of WAN ports that are online. ▪ The number in red indicates the number of WAN ports that are offline. ▪ Clicking the numbers redirects you to **Manage** > **WAN** > **Summary**.
LAN	▪ Displays the number of LAN ports as online or offline. ▪ The number in green indicates the number of LAN ports that are online. ▪ The number in red indicates the number of LAN ports that are offline. ▪ Clicking the numbers redirects you to **Manage** > **LAN** > **Summary**.
Tunnels	▪ Displays the number of VPN tunnels as online or offline. ▪ The number in green indicates the number of VPN tunnels that are online. ▪ The number in red indicates the number of VPN tunnels that are offline. ▪ Clicking the numbers redirects you to **Manage** > **WAN** > **Tunnels**.
Path Steering	▪ Displays the number of path steering policies that are compliant of the total number of policies. ▪ Clicking the numbers redirects you to **Manage** > **WAN** > **Path Steering**.
Alerts	▪ Displays the total number of open alerts. ▪ Clicking the number redirects you to **Analyze** > **Alerts & Events** in **List** view.

Health Bar for the Wireless Client Dashboard

The following table includes information on the various parameters of the Health Bar displayed for a wireless client.

Parameter	Description
Client Status	Displays the connection status of the client.
Device Health	Displays the device health of the client.

Parameter	Description
Signal Quality	Displays the signal quality in dB.
Tx | Rx Rate	Displays the transmit and receive rate in Mbps.
Connected To	▪ Displays the device to which the wired client is connected. ▪ Clicking on the device redirects you to the **Manage** > **Overview** > **Summary** page for that device.
Refresh icon	Refreshes the data on the Health Bar for the client.

Health Bar for the Wired Client Dashboard

The following table includes information on the various parameters of the Health Bar displayed for a wired client.

Parameter	Description
Client Status	Displays the connection status of the client.
Connected Port	Displays the port to which the client is connected.
Connected To	▪ Displays the device to which the wired client is connected. ▪ Clicking on the device redirects you to the **Manage** > **Overview** > **Summary** page for that device.
Refresh icon	Refreshes the data on the Health Bar for the client.

Health Bar for the Remote Client Dashboard

The following table includes information on the various parameters of the Health Bar displayed for a remote client.

Parameter	Description
Client Status	Displays the connection status of the client.
Connected To	▪ Displays the name of the gateway to which the remote client is connected. ▪ Clicking on the device redirects you to the **Manage** > **Overview** > **Summary** page for that device.
Refresh icon	Refreshes the data on the Health Bar for the client.

The Global Dashboard

In the **Network Operations** app, the global dashboard is displayed when the filter is set to **Global**. The global dashboard displays information related to all devices registered to that account in Aruba Central.

Some tabs may not be seen in your dashboard view if you are not an administrator for the Aruba Central account.

Table 14: *Contents of the Global Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > **Overview**	**Network Health**	Displays information of the networks sorted by site, including information on network devices and WAN connectivity of individual sites. For more information, see Network Health Dashboard.
	WAN Health	Displays detailed information of the network health status and usage for the sites in which Branch Gateways and VPN Concentrators are configured in your setup. For more information, see WAN Health—Global.
	Summary	Displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range Filter. For more information, see Global—Summary
	Wi-Fi Connectivity	Displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase. The connection phases include Association, Authentication, DHCP, and DNS. For more information, see Wi-Fi Connectivity.
	AI Insights	Displays a report of network events that may affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level observed in the network for the selected time range. Each insight report provides specific details on the occurrences of these events for ease in debugging. For more information, see The AI Insights Dashboard.
Manage > **Devices**	**Access Points**	Displays the access points information in the following views: ■ **Summary** view: Monitoring APs in Summary View ■ **List** view: Monitoring APs in List View
	Switches	Displays the switches information in the following views: ■ **Summary** view: Monitoring Switches in Summary View ■ **List** view: Monitoring Switches in List View
	Gateways	Displays the gateways information in the following views: ■ **Summary** view: Monitoring Gateways in Summary View ■ **List** view: Monitoring Gateways in List View
Manage > **Clients**	**Clients**	Displays information about all the clients connected to the devices configured for the group. For more information, see All Clients.

Left Navigation Menu	First-Level Tabs	Description
Manage > **Guests**	**Guest Access**	Enables guest users to connect to the network and at the same time, allows the administrator to control guest user access to the network. For more information, see Guest Access.
	Presence Analytics	Enables businesses to collect real-time data on user footprints within the wireless network range of Aruba Instant APs that are managed using Aruba Central. For more information, see Presence Analytics.
Manage > **Applications**	**Visibility**	Provides a summary of client traffic and their data usage to and from applications and websites. Also, analyzes the client traffic flow using the graphs displayed. For more information, see Application Visibility.
	SAAS Express	Enables the following to provide an improved user experience: discovering SaaS application servers, monitoring application performance, and steering traffic to the best available servers.. For more information, see SaaS Application Traffic Management with SaaS Express.
Manage > **Security**	**RAPIDs**	Helps to identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. For more information, see Rapids.
	Gateway IDS/IDPS	Enables traffic inspection, threat detection, and threat prevention on the Aruba Branch Gateways. For more information, see Overview of Aruba IDPS.
	Firewall	Monitors traffic coming into and going out of the Aruba Central-managed network and acts as an investigative resource for users to track blocked sessions within the network. For more information, see Firewall.
Manage > **Network Services**	**SD-WAN Overlay**	Configured IPsec tunnels between the Branch Gateways and VPN Concentrators provisioned in an Aruba Central account. For more information, see SD-WAN Overlay Tunnel and Route Orchestration .
	Virtual Gateways	Helps deploy a virtualized instance of a headend gateway in the customer's public cloud infrastructure. The virtualized instance of Aruba Gateway is referred to as Virtual Gateway. For more information, see Deploying Aruba Virtual Gateways.
	Cloud Connect	Helps integrate SD-Branch with Zscaler and allows to set up and maintain a secure tunnels between Aruba Branch Gateways and Zscaler Public Service Edges. For more information, see Aruba SD-Branch Integration with Zscaler through Cloud Connect Service.
	Cloud Security (Legacy)	Helps integrate SD-Branch with Zscaler and allows to set up tunnels automatically or manually between Aruba Branch Gateways and Zscaler Public Service Edges. For more information, see Aruba SD-Branch Integration with Zscaler Cloud Security Service.

Left Navigation Menu	First-Level Tabs	Description
Analyze > **Alerts and Events**	**Alerts & Events**	Displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. For more information, see Alerts & Events.
Analyze > **Audit Trail**	**Audit Trail**	Shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. For more information, see Viewing Audit Trail.
Analyze > **Tools**	▪ **Network Check** ▪ **Device Check** ▪ **Commands** ▪ **Health Checks**	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools.
Analyze > **Reports**	**Reports**	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports.
Maintain > **Firmware**	▪ **Access Points** ▪ **Switch-MAS** ▪ **Switches** ▪ **Gateways**	Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information, see Managing Software Upgrades.
Maintain >Organization	**Groups**	A group in Aruba Central is the primary configuration element that functions as a container for device management, monitoring, and maintenance. Groups enable administrators to manage devices efficiently by using either a UI-based configuration workflow or CLI-based configuration template. For more information, see Groups for Device Configuration and Management.
	Sites and Labels	A site refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Labels are tags attached to a device provisioned in the network. Labels determine the ownership, departments, and functions of the devices. For more information, see Sites and Labels.
	Certificates	Enables administrators to upload a valid certificate signed by a root CA so that devices are validated and authorized to use Aruba Central. For more information, see Groups for Device Configuration and Management.
	Install Manager	Simplifies and automates site deployments, and helps IT administrators manage site installations with ease. For more information, see Installation Management.

The Label Dashboard

In the **Network Operations** app, the label dashboard is displayed when the filter is set to any of the options under **Labels**. The site dashboard displays information related to all devices configured for that site in Aruba Central.

Table 15: *Contents of the Label Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > **Devices**	**All Devices**	Displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range filter. For more information, see Global—Summary
	Access Points	Displays the access points information in the following views: ▪ **Summary** view: Monitoring APs in Summary View ▪ **List** view: Monitoring APs in List View
	Switches	Displays the switches information in the following views: **Summary** view: Monitoring Switches in Summary View ▪ **List** view: Monitoring Switches in List View
	Gateways	Displays the gateways information in the following views: ▪ **Summary** view: Monitoring Gateways in Summary View ▪ **List** view: Monitoring Gateways in List View
Manage > **Clients**	**Clients**	Displays information about all the clients connected to the devices configured for the group. For more information, see All Clients.
Manage > **Security**	**RAPIDs**	Identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central sends alerts to the network administrators about the possible threat and provides essential information needed to locate and manage the threat. For more information, see Rapids.
Analyze > **Alerts and Events**	**Alerts & Events**	Displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. For more information, see Alerts & Events.
Analyze > **Tools**	▪ **Network Check** ▪ **Device Check** ▪ **Commands**	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools.
Analyze > **Reports**	**Reports**	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports.

The Site Dashboard

In the **Network Operations** app, the site dashboard is displayed when the filter is set to any of the options under **Sites**. The site dashboard displays information related to all devices configured for that site in Aruba Central.

Table 16: *Contents of the Site Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > **Overview**	**Site Health**	Displays details of wired and wireless devices deployed on the site. This page includes information on client connectivity statistics, change logs, health of devices, and RF health of the site. For more information, see Site Health Dashboard.
	Summary	Displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range filter. For more information, see Global—Summary
	Wi-Fi Connectivity	Displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase. The connection phases include Association, Authentication, DHCP, and DNS. For more information, see Wi-Fi Connectivity.
	WAN Health	Displays details for the wired, wireless, and gateway devices deployed on the site. For more information, see WAN Health—Site.
	AI Insights	Displays a report of network events that may affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level in the network for the selected time range. Each insight report provides specific details on the occurrences of these events for ease in debugging. For more information, see The AI Insights Dashboard.
	Topology	Provides a graphical representation of the site including the network layout, details of the devices deployed, and the health of the WAN uplinks and tunnels. For more information, see Monitoring Sites in the Topology Tab.
	Floor Plans	Provides information regarding the current location of the Instant AP. For more information, see Access Point > Overview > Floor Plan.
Manage > **Devices**	**Access Points**	Displays the access points information in the following views: ▪ **Summary** view: Monitoring APs in Summary View ▪ **List** view: Monitoring APs in List View
	Switches	Displays the switches information in the following views: ▪ **Summary** view: Monitoring Switches in Summary View ▪ **List** view: Monitoring Switches in List View
	Gateways	Displays the gateways information in the following views: ▪ **Summary** view: Monitoring Gateways in Summary View

Left Navigation Menu	First-Level Tabs	Description
		▪ **List** view: Monitoring Gateways in List View
Manage > **Clients**	**Clients**	Displays information about all the clients connected to the devices configured for the group. For more information, see All Clients.
Manage > **Applications**	**Visibility**	Provides a summary of client traffic and their data usage to and from applications and websites. Also, analyzes the client traffic flow using the graphs displayed. For more information, see Application Visibility.
Manage > **Security**	**RAPIDS**	Identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central sends alerts to the network administrators about the possible threat and provides essential information needed to locate and manage the threat. For more information, see Rapids.
Manage > **Guests**	**Presence Analytics**	Enables businesses to collect real-time data on user footprints within the wireless network range of Aruba Instant APs that are managed using Aruba Central. For more information, see Presence Analytics.
Analyze > **Alerts and Events**	**Alerts & Events**	Displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. For more information, see Alerts & Events.
Analyze > **Live Events**	**Live Events**	Enables you to troubleshoot issues related to a wireless client connected to an access point or a wired client connected to a switch. For more information, see Client Live Troubleshooting.
Analyze > **Tools**	▪ **Network Check** ▪ **Commands**	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools.
Analyze > **Reports**	**Reports**	Enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports.

The Access Point Dashboard

In the **Network Operations** app, the access point dashboard is displayed when the filter is set to an access point. To navigate to an access point dashboard, see Navigating to the Switch, Access Point, or Gateway Dashboard.

The following table lists all the available menu items in the **Network Operations** app for the access point dashboard.

Table 17: *Contents of the Access Point Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > **Overview**	**Summary**	Displays the AP device details, network information, radio details including the topology of clients connected to each radio, and the health status of the AP in the network. See Access Point > Overview > Summary.
	AI Insights	Displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization. See Access Point > Overview > AI Insights
	Floor Plan	Displays information regarding the current location of the Instant AP. See Access Point > Overview > Floor Plan.
	Performance	Displays the size of data transmitted through the AP. See Access Point > Overview > Performance.
	RF	Displays details corresponding to 2.4 GHz, 5 GHz, and 5 GHz Secondary radios of the AP. See Access Point > Overview > RF.
	Spectrum	Displays details for all Wi-Fi and non-Wi-Fi devices associated to each radio. See Access Point > Overview > Spectrum
Manage > **Device**	**Access Point** Configuration using UI groups	Enables AP configuration in the **Config** view. See Deploying a Wireless Network Using Instant APs. Configuration using UI groups contains the following second-level tabs: ▪ **WLANs**—Configure wireless network profiles on Instant APs. See Configuring Wireless Network Profiles on Instant APs. ▪ **Access Points**—Configure device parameters on Instant APs. See Configuring Device Parameters . ▪ **Radios**—Configure ARM and RF parameters on Instant APs. See Configuring ARM and RF Parameters on Instant APs. ▪ **Interfaces**—Configuring interfaces parameters on Instant APs. See Configuring Uplink Interfaces on Instant APs. ▪ **Security**—Configure authentication and security profiles on Instant APs. See Configuring Authentication and Security Profiles on Instant APs. ▪ **VPN**—Configure VPN host settings on an Instant AP to enable communication with a controller in a remote location. See Configuring Instant APs for VPN Tunnel Creation. ▪ **Services**—Configure AirGroup, location services, Lawful Intercept, OpenDNS, and Firewall services on Instant APs. See Configuring Services. ▪ **System**—Configure system parameters on Instant APs. See Configuring Systems. ▪ **Configuration Audit**—View configuration sync errors and overrides. See Viewing Configuration Status.

Left Navigation Menu	First-Level Tabs	Description
	Access Point Configuration using template groups	Configuration using template groups contains the following second-level tabs: ▪ **Templates**—Configure Access Points using template groups. See Configuring APs Using Templates. ▪ **Variables**—Modify, download, or upload variables associated with devices that you can use in template configuration. See Managing Variable Files. ▪ **Configuration Audit**—View configuration sync errors and overrides. See Viewing Configuration Status.
Manage > **Clients**	**Clients**	Displays details of all the clients connected to a specific AP. See Access Point > Clients > Clients.
Manage > **Security**	**VPN**	Displays information on VPN connections associated with the virtual controller along with information on the tunnels and the data usage through each of the tunnels. See Access Point > Security > VPN
Analyze > **Alerts & Events**	**Alerts & Events**	The **Alerts & Events** tab displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. See Access Point > Alerts & Events > Alerts & Events.
Analyze > **Audit Trail**	**Audit Trail**	The **Audit Trail** tab displays the logs for all the device management, configuration, and user management events triggered in Aruba Central. See Viewing Audit Trail in the Standard Enterprise Mode and MSP Mode.
Analyze > **Tools**	**Commands**	The **Commands** tab allows network administrators and user with troubleshooting permission to identify, diagnose, and debug issues on Aruba Instant APs at an advanced level using commands. See Using Troubleshooting Tools.
Maintain > **Firmware**	**Access Points**	The **Access Points** tab allows the user to view the firmware details and upgrade the devices provisioned in Aruba Central. See Viewing Firmware Details.

The Switch Dashboard

In the **Network Operations** app, the switch dashboard is displayed when the filter is set to a switch. To navigate to a switch dashboard, see Navigating to the Switch, Access Point, or Gateway Dashboard.

The following table lists all the available menu items in the **Network Operations** app for the switch dashboard.

- Some tabs may not be seen in your dashboard view if you are not an administrator for the Aruba Central account. Also, some tabs or some fields inside tabs are only applicable either for AOS-Switch or AOS-CX switches.
- AOS-CX switches can be configured using templates only.

Table 18: *Contents of the Switch Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > Overview	**Summary**	Displays details about a specific switch, including device information, network summary, and port and hardware status. It also displays uplink and usage details. Use the time range filter to change the time period for the displayed information. See Switch > Overview > Summary.
	Hardware	Displays switch hardware details, including status of power supplies and fans, CPU and memory utilization, and device temperature. See Switch > Overview > Hardware.
	Routing	Displays routing information for the switch, such as, type of route, number of static and connected routes, and distance of the route. See Switch > Overview > Routing. **NOTE:** The **Routing** tab is displayed only for AOS-Switches.
	AI Insights	Displays information on switch performance issues, such as, PoE issues, port errors, port flaps, airtime utilization, and memory utilization. See Switch > Overview > AI Insights.
Manage > Clients	**Clients**	Displays details about the wired clients that are connected to the switch. See Switch > Clients > Clients.
	Neighbours	Displays details about the devices neighboring the switch. See Switch > Clients > Neighbours.
Manage > LAN	**Ports**	Displays details about ports and the LAGs configured in the switch. See Switch > LAN > Ports.
	PoE	Displays details about PoE status, PoE ports, and the power consumption from these ports. See Switch > LAN > PoE.
	VLAN	Displays VLAN information configured on the switch and details about tagged and untagged ports. See Switch > LAN > VLAN.
Manage > VSX	**VSX**	Displays VSX configuration details between AOS-CX switches and the status of the inter-switch link (ISL). See Switch > VSX. **NOTE:** The **VSX** tab is displayed only for AOS-CX switch series.
Manage > Device	**AOS-Switch—** Configuration using UI groups	Enables AOS-Switch configuration in the **AOS-S Config** view. See Configuring or Viewing AOS-Switch Properties in UI Groups. Configuration using UI groups contains the following second-level tabs: ▪ **Switches**—Configure and view general switch properties, such as, hostname, IP address, and netmask. See Configuring or Viewing Switch Properties. ▪ **Stacks**—Create stacks, add members, or view stacking details, such as, stack type, stack id, and topology. See Configuring AOS-Switch Stacks Using

Left Navigation Menu	First-Level Tabs	Description
		UI Groups. ■ **Interface:** ◦ **Ports**—Assign or view port properties, such as, PoE, access policies, and trunk groups. See Configuring Switch Ports on AOS-Switches. ◦ **PoE**—Configure or view PoE settings for each port. See Configuring PoE Settings on AOS-Switch Ports. ◦ **Trunk Groups**—Configure or view trunk groups and their associated properties, such as, members of the trunk group, and type of trunk group. See Configuring Trunk Groups on AOS-Switches in UI Groups. ◦ **VLANs**—Configure or view VLAN details and the associated ports and access policies. See Configuring VLANs on AOS-Switches. ◦ **Spanning Tree**—Configure or view spanning tree protocol and its associated properties. See Enabling Spanning Tree Protocol on AOS-Switches. ◦ **Loop Protection**—Configure or view loop protection and its associated properties. See Configuring Loop Protection on AOS-Switch Ports. ■ **Security:** ◦ **Access Policies**—Add or view access policies. See Configuring Access Policies on AOS-Switches. ◦ **DHCP Snooping**—Configure or view DHCP snooping, authorized DHCP servers IP addresses, and their associated properties. See Configuring DHCP Snooping on AOS-Switches. ◦ **Port Rate Limit**—View or specify bandwidth to be used for inbound or outbound traffic for each port. See Configuring Port Rate Limit on AOS-Switches. ◦ **RADIUS**—Configure RADIUS (Remote Authentication Dial-In User Service) server settings on AOS-Switches. See Configuring RADIUS Server Settings on AOS-Switches. ◦ **Downloadable User Role**—Enable DUR and configure ClearPass settings to download user roles, policy, and class from the ClearPass Policy Manager server. See Configuring Downloadable User Role on AOS-Switches. ◦ **Tunneled Node Server**—Configure user-based tunnel or port-based tunnel on switches. See Configuring Tunnel Node Server on AOS-Switches. ◦ **Authentication**—Configure and enable 802.1X and MAC authentication on switches. You can also configure authentication order and priority for authentication methods. Configuring Authentication for AOS-Switches. ■ **System:** ◦ **Access/DNS**—Configure or view the administrator and operator logins. See Configuring System Parameters for AOS-Switches. ◦ **Time**—Configure time synchronization in switches. See Configuring Time Synchronization on AOS-Switches. ◦ **SNMP**—Add or view SNMP v2c and v3 community and its trap destination. See Configuring SNMP on AOS-Switches. ◦ **CDP**—Configure CDP and its associated properties. See Configuring

Left Navigation Menu	First-Level Tabs	Description
		CDP on AOS-Switches. ◦ **DHCP**—Add or view a DHCP pool and its associated properties. See Configuring DHCP on AOS-Switches. ■ **Routing**—Configure or view a specific routing path to a gateway. See Configuring Routing on AOS-Switches. ■ **IGMP**—Configure IGMP and its associated properties. See Configuring IGMP on AOS-Switches. ■ **QoS**—Configure QoS traffic policies on switches to classify and prioritize traffic throughout a network. See Configuring QoS Settings on AOS-Switches. ■ **Device Profile**—Configure device profile on switches to dynamically detect devices based on certain parameters. See Configuring Device Profile. ■ **Configuration Audit**—View configuration sync errors and overrides. See Viewing Configuration Status.
	AOS-Switch— Configuration using templates	See Using Configuration Templates for AOS-Switch Management. Configuration of AOS-Switches using template groups contains the following second-level tabs: ■ **Templates**—Configure switch using template groups. See Creating a Configuration Template. ■ **Variables**—Modify, download, or upload variables associated with devices that you can use in template configuration. See Managing Variable Files. ■ **Configuration Audit**—View configuration sync errors and overrides. See Viewing Configuration Status.
	AOS-Switch Stack— Configuration using templates	Configuration of AOS-Switch stacks using template groups contains the following second-level tabs: ■ **Templates**—Configure switch stack using template groups. See Configuring AOS-Switch Stacks using Template Groups. ■ **Variables**—Modify, download, or upload variables associated with devices that you can use in template configuration. See Managing Variable Files. ■ **Configuration Audit**—View configuration sync errors and overrides. See Viewing Configuration Status.
	AOS-CX— Configuration using UI groups	Enables AOS-CX configuration in the **AOS-CX Config** view. See Configuring AOS-CX Switches in UI Groups. Configuration using UI groups allows you to configure the following features: ■ **System**: ◦ **Properties**—Edit system property settings such as contact, location, time zone, and administrator password. You can also select the VRF to be used and add the DNS and NTP servers. See Configuring System Properties on AOS-CX. ◦ **SNMP**—Add, edit, or delete SNMP v2 communities, v3 users, and trap notifications. See Configuring SNMP on AOS-CX. ◦ **Logging**—Add, edit, or delete logging servers to view event logs from the AOS-CX switches. Configure FQDN or IP address, log severity level, and the VRF to be used for each of the logging servers. Also configure

Left Navigation Menu	First-Level Tabs	Description
		the global level debug log severity. See Configuring Logging Servers for AOS-CX. ◦ **Administrator**—Add, edit, or delete server groups to be used for authentication, authorization, and accounting. You must also configure the protocol required to enable connection to these server groups. See Configuring AAA for AOS-CX. ▪ **Routing**: ◦ **Static Routing**—Add, edit, or delete static routes manually and configure destination IP addresses and next hop values, VRF, and the administrative distance. You can add different static routes for different VRFs on the switch. See Configuring Static Routing on AOS-CX. ▪ **Interfaces**: ◦ **Ports & Link Aggregations**—View and edit port settings such as description, VLAN mode, speed duplex, routing, and the operational status of the port. Add, edit, or delete LAGs by combining different ports and configuring the speed duplex, VLAN mode, aggregation mode, and the operational status of the LAG. See Configuring Ports and LAGs on AOS-CX. ▪ **Security**: ◦ **Authentication Servers**—Add, edit, or view the RADIUS and TACACS servers for authentication. Add settings such as FQDN or IP address of the servers, authentication port number, response timeout, retry count, and the VRF to be used when communicating with the servers. See Configuring Authentication Servers on AOS-CX. ◦ **Authentication**—View or edit details about 802.1X and MAC authentication methods. Configure the precedence order and other parameters such as reauthentication timeout, cached reauthentication timeout, and quiet period. See Configuring Authentication on AOS-CX. ◦ **Access Control**—View or add access policies and rules to permit or deny passage of traffic. See Configuring Access Control on AOS-CX. ▪ **Bridging**: ◦ **VLANs**—Add, edit, delete, or view VLANs, and associated parameters such as type of IP assignment, operational status, IP address of the DHCP relay. See Configuring VLANs on AOS-CX. ◦ **Loop Prevention**—Enable or disable loop protection and spanning tree protocol, and associated parameters such as the mode and priority. Enable or disable various MSTP mode-related settings such as BPDU filter, BPDU protection, admin edge, and root guard. See Configuring Loop Prevention on AOS-CX.
	AOS-CX— Configuration using **MultiEdit** mode	Enables AOS-CX configuration using the **MultiEdit** mode in the **AOS-CX Config** view. View and edit configuration on the AOS-CX switches using the CLI syntax. You can also apply predefined set of configuration settings such as NAE to the switches. See Using MultiEdit View for AOS-CX. Configuration using the **MultiEdit** mode contains the following options: ▪ **View Config**—View configuration of AOS-CX switches and find differences

Left Navigation Menu	First-Level Tabs	Description
		in the configuration across switches. See Viewing Configuration on AOS-CX. ■ **Edit Config**—Edit configuration for one or more AOS-CX switches in the MultiEdit mode. Edit the entire configuration in a familiar looking CLI with syntax checking, colorization, and command completion. See Editing Configuration on AOS-CX. ■ **Express Config**—Apply predefined set of configuration settings such as NAE scripts and device profile to a single or multiple switches. See Express Configuration on AOS-CX.
	AOS-CX— Configuration using templates	Enables AOS-CX switch configuration in the **AOS-CX** view. See Using Configuration Templates for AOS-CX Switch Management. Configuration of AOS-Switches using template groups contains the following second-level tabs: ■ **Templates**—Configure switch using template groups. See Creating a Configuration Template. ■ **Configuration Audit**—View configuration sync errors and overrides. See Viewing Configuration Status. ■ **Configuration Status**—View configuration status of AOS-CX switches that are managed through UI groups in Aruba Central. See Using Configuration Status on AOS-CX.
	AOS-CX VSF Stack— Configuration	Enables AOS-CX switch stack configuration in the **AOS-CX** view. See AOS-CX VSF Stack.
Analyze > Alerts & Events	**Alerts & Events**	The **Alerts & Events** tab displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. See Alerts & Events. You can also configure and enable certain categories of switch alerts. See Switch Alerts.
Analyze > Audit Trail	**Audit Trail**	Displays the details of logs generated for all device management, configuration, and user management events triggered in Aruba Central. See Viewing Audit Trail.
Analyze > Tools	**Network Check**	The **Network Check** tab allows administrators and users with troubleshooting permission to diagnose issues related to wired network connections. See Troubleshooting Switch Connectivity Issues.
	Device Check	The **Device Check** tab allows network administrators and users with troubleshooting permission to identify, diagnose, and debug issues on AOS-Switch and AOS-CX switches using predefined tests. See Troubleshooting Device Issues.
	Commands	The **Commands** tab allows network administrators and user with troubleshooting permission to identify, diagnose, and debug issues on AOS-Switch and AOS-CX switches at an advanced level using commands. See Troubleshooting Switches.

Left Navigation Menu	First-Level Tabs	Description
Analyze > Reports	**Reports**	The **Reports** tab allows you to create, manage, and view various reports. You can create recurrent reports, generate reports on demand, or schedule reports to run at a later time. See Reports.
Maintain > Firmware	**Switches**	The **Switches** tab allows the user to view the firmware details and upgrade the devices provisioned in Aruba Central. See Managing Software Upgrades.

The Gateway Dashboard

In the **Network Operations** app, the gateway dashboard is displayed when the filter is set to a gateway. To navigate to a gateway dashboard, see Navigating to the Switch, Access Point, or Gateway Dashboard.

The following table lists all the available menu items in the **Network Operations** app for the gateway dashboard.

Some tabs may not be seen in your dashboard view if you are not an administrator for the Aruba Central account.

Table 19: *Contents of the Gateway Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Manage > **Overview**	**Summary**	Displays details about a specific gateway, including device information, WAN summary, and health status. Use the time range filter to change the time period for the displayed information. See Gateway > Overview > Summary.
	IDPS	Displays the graphs related to IDPS. This feature is only applicable to IDPS gateways. Use the time range filter to change the time period for the displayed information. See Gateways > Overview > IDPS.
	Routing	Displays routing information for the following second-level tabs in **List** view. ■ BGP— See Gateway > Overview > Routing > BGP. ■ OSPF—See Gateway > Overview > Routing > OSPF. ■ Overlay—See Gateway > Overview > Routing > Overlay ■ RIP—See Gateway > Overview > Routing > RIP ■ Route Table—See Gateway > Overview > Routing > Route Table Use the time range filter to change the time period for the displayed information.
	Sessions	Displays information for the running sessions. See Gateway > Overview > Sessions.
	AI Insights	Displays information on gateway performance issues such as tunnel up, tunnel down, airtime utilization, and memory utilization. See Gateway > Overview > AI Insights.

Left Navigation Menu	First-Level Tabs	Description
Manage > **WAN**	**Summary**	Displays status information about WAN ports and WAN interfaces. See Gateway > WAN > Summary.
	Tunnels	Display status information for VPN tunnels. See Gateway > WAN > Tunnels
	Path Steering	Displays information about dynamic path steering policies configured on a Branch Gateway. See Gateway > WAN > Path Steering.
Manage > **LAN**	**Summary**	Displays information about LAN port and LAN status. See Gateway > LAN > Summary.
Manage > **Device**	**Gateway**	Enables gateway configuration in **Config** view for the basic mode, advanced mode, and guided setup. See Provisioning Aruba Gateways in Aruba Central.
Manage > **Clients**	**Clients**	Displays a list of clients connected to a gateway. See All Clients.
Manage > **Applications**	**Visibility**	Displays charts showing client traffic trends to application, application categories, website categories, and websites of a specific security reputation score. ▪ Applications— See Applications ▪ Websites— See Websites
	SAAS Express	Displays charts with QoE scores for all of the SaaS applications that you have configured. See Monitoring SaaS Express .
Manage > **Security**	**Firewall**	Displays graphical and tabular representations of all the session activities belonging to gateways managed by Aruba Central. See Firewall.
Analyze > **Alerts and Events**	**Alerts & Events**	Displays alerts for SD-WAN and gateway-related events. See Gateway Alerts. **NOTE:** You can configure alerts in the global dashboard only.
Analyze > **Audit Trail**	**Audit Trail**	Displays the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. See Viewing Audit Trail.
Analyze > **Tools**	**Network Check**	Enables network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. See Troubleshooting Gateway Connectivity Issues.
	Logs	Enables network administrators and users with permission to download and upload TAR logs and crash logs related to gateways. See Enabling Gateway Logs.
	Commands	See Troubleshooting Gateways.
Analyze > **Reports**	**Reports**	Enables network administrators to create various types of reports. You can create recurrent reports or configure the reports to run on demand. For more information, see Reports.
Maintain > **Firmware**	**Firmware**	Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information, see Managing Software Upgrades.

The Client Dashboard

In the **Network Operations** app, the clients dashboard is displayed when the filter is set to one of the options under **Groups**, **Labels**, **Sites**, or **Global**.

The following table lists all the available menu items in the **Network Operations** app for the clients dashboard.

Table 20: *Contents of the Clients Dashboard*

Left Navigation Menu	First-Level Tabs	Description
Wireless Clients		
Manage > **Overview**	**Summary**	Displays the client details about the type of data path that the client uses, the network and connectivity details, and basic client details such as IP address of the client, type of encryption etc. See Summary .
	AI Insights	Displays the information about client performance and connectivity issues such as, excessive 2.4 GHz dwell and low SNR links. See The AI Insights Dashboard.
	Location	Displays the current physical location of the client device on the floor map. See Location.
	Sessions	Displays the firewall session details for the client connected to an AP or a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. See Sessions.
Manage > **Applications**		Displays the client details for passive motoring of the client connected to a wireless network. The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. See Application Visibility.
Analyze > **Live Events**		Allows troubleshooting issues related to a client or a site in real time for detailed analysis. See Live Events.
Analyze > **Events**		Displays the details of events generated by the AP and client association. See Alerts & Events
Analyze > **Tools**		Enables network administrators to perform checks on the client and debug client connectivity issues. See Using Troubleshooting Tools
Wired Clients		
Manage > **Overview**	**Summary**	Displays the information about the type of data path that the client uses, the network details, and basic client details such as IP address of the client, type of encryption etc. See Summary .
	AI Insights	Displays information about client performance and connectivity issues such as, excessive 2.4 GHz dwell and low SNR links.

Left Navigation Menu	First-Level Tabs	Description
		See The AI Insights Dashboard.
	Sessions	Displays the firewall session details for the client connected to a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. See Sessions .
Manage > **Applications**		Displays the client details for passive motoring of the client connected to a wired network. The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. See Application Visibility.
Analyze > **Live Events**		Allows troubleshooting issues related to a wired client connected to a switch in real time for detailed analysis. See Live Events.
Analyze > **Events**		Displays the details of events generated by the AP and client association. See Alerts & Events.
Analyze > **Tools**		Enables network administrators to perform checks on the client and debug client connectivity issues. See Using Troubleshooting Tools.
Remote Clients		
Manage > **Overview**	**Summary**	Displays the information about the type of data path that the client uses, the network details, and basic client details such as IP address of the client, type of encryption, and so on. See Summary.
	AI Insights	Displays information about client performance and connectivity issues such as, excessive 2.4 GHz dwell and low SNR links. See The AI Insights Dashboard.
	Location	Displays the current physical location of the client device on the floor map. See Location.
	Sessions	Displays the firewall session details for the client connected to a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. See Sessions.
Manage > **Applications**		Displays the client details for passive motoring of the client connected to a wired network. The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. See Applications.
Analyze > **Security**		Displays the authentication and accounting details of the remote client. See Security.
Analyze > **Tools**		Enables network administrators to perform checks on the client and debug client connectivity issues. See Tools.

Overview of Aruba Central Foundation and Advanced Licenses

As part of the shift to an Edge-to-Cloud Platform-as-a-Service organization, Aruba has introduced the Aruba Central Foundation and Advanced Licenses (Aruba Central Licenses). This is a uniform software subscription licensing model that will be extended to all products under the Aruba Central-managed portfolio. The new 1, 3, 5, 7, and 10-year fixed-term licenses offer you the flexibility to choose services and device operations that are most meaningful to the type of business that you own.

This licensing model provides different licenses for APs, switches, and gateways.

The licenses for APs, switches, and gateways cannot be used interchangeably. For example, you cannot use an AP Foundation License on a gateway. Similarly, if you have an Aruba 25xx Switch but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch.

The features that are available in both the Foundation and Advanced Licenses have different monitoring and configuration options depending on the licensing tier. For more information, see Supported Features.

This licensing model provides the following types of licenses depending on the devices:

- Switches:
  - **Foundation**—This license provides all the features included in the legacy Device Management tokens.

- Aruba Central does not provide Switch Advanced Licenses.
- Mobility Access Switch (MAS) license will get converted to Switch Foundation 61xx/25xx license and continue to work.

- Access Points (APs):
  - **Foundation**—This license provides all the features included in the legacy Device Management tokens and some additional features that were available as value-added services for APs and switches in the earlier licensing model.
  - **Advanced**—This license provides all the features included in the Foundation License, with additional features related to AI Insights and WLAN services.
- SD-Branch Gateways:
  - **Foundation**—This license provides all features required for SD-Branch functionality in branch or headend deployments.
  - **Foundation Base**—This license provides all the features included in a Foundation License, but can support only up to 75 client devices per branch site.
  - **Foundation** with **Security**—This license provides all features required for SD-WAN functionality in branch or headend deployments and some additional security features.
  - **Foundation Base** with **Security**—This license provides all the features included in a Foundation with Security License, but can support only up to 75 client devices per branch.
  - **Advanced**—This license provides all the features included in a Foundation License, with additional features related to SaaS Express and AI Insights.
  - **Advanced** with **Security**—This license provides all the features of an Advanced License, with additional security features related to IPS and IDS, security dashboard, and anti-malware.

- **Virtual Gateway (VGW) License**—This license is available for AWS, Azure, and ESXi platforms and is licensed based on the bandwidth required. The license types available for VGW are, VGW-500M, VGW-2G, and VGW-4G.

For more information, see SD-WAN Ordering Guide.

The Foundation and Advanced Licenses for APs, switches, and SD-Branch gateways are different and cannot be used interchangeably.

For a detailed list of the features supported in each type of license, see Supported Features.

For more information about evaluation licenses, see Starting Your Free Trial.

Changes to the Legacy Licensing Model

For existing Aruba Central customers, please note that the previous Device Management and Service Token model is changed to the new licensing model, which provides a uniform licensing structure for all types of devices such as APs, switches, and gateways.

The following list provides information about important aspects of the legacy licensing model:

- **Device Management Token**—This is a mandatory token which allows you to manage and monitor your APs and switches from Aruba Central.
- **Service Token**—This token allows you to enable value-added services for APs managed from Aruba Central. These services include UCC, AirGroup, Wi-Fi Connectivity Dashboard (formerly, Clarity), Cloud Guest, WebCC, and Presence Analytics.
- **Subscription Key**—A valid subscription key allows you to manage, profile, and analyze your devices using Aruba Central. A subscription key is a 14-character alphanumeric string provided for either a device management or service token.

The new Aruba Central Licenses simplify the existing subscription-based licensing model. With the introduction of this licensing model, the existing Device Management tokens for APs and switches are no longer available. Similarly, the Service tokens for value-added services on the APs are unavailable. Instead, APs and switches have adopted the current Gateway Foundation and Advanced licensing model.

Supported Devices

The Aruba Central Licenses are supported for APs, switches, and gateways. For more information on the individual device models supported, refer to the next sections. The pricing structure for Foundation and Advanced Licenses for the hardware devices may differ based on the types of models.

APs and IAPs

All AP and IAP models that are currently being shipped are supported. See Supported Instant APs.

Switches

Aruba Central supports AOS-Switch and AOS-CX switches.

AOS-Switches

The following AOS-Switches are supported:

- Aruba 2530 Switch Series
- Aruba 2540 Switch Series

- Aruba 2920 Switch Series
- Aruba 2930F Switch Series
- Aruba 2930M Switch Series
- Aruba 3810 Switch Series
- Aruba 5400R Switch Series

For more information, see Supported AOS-Switch Platforms.

AOS-CX Switches

The following AOS-CX switches are supported:

- AOS-CX 6200 Switch Series
- AOS-CX 6300 Switch Series
- AOS-CX 6400 Switch Series
- AOS-CX 8320 Switch Series
- AOS-CX 8325 Switch Series
- AOS-CX 8360 Switch Series
- AOS-CX 8400 Switch Series

For more information, see Supported AOS-CX Platforms.

Gateways

Aruba Central supports SD-Branch Gateways based on the license type.

For more information, see Supported SD-Branch Components.

Gateway Foundation and Advanced License

The Gateway Foundation and Advanced License can be assigned to the following gateways:

- Aruba 70xx Series
- Aruba 72xx Series
- Aruba 90xx Series

This license does not have a capacity limit for client devices.

Gateway Foundation Base License

The Gateway Foundation Base License can be assigned to the following gateways:

- Aruba 7005, 7008, 9004, 9004-LTE, 9012

This license includes all the features available in the Gateway Foundation License. However, this license can support only up to 75 client devices per branch.

When the client capacity reaches the threshold, Aruba Central triggers an alert to indicate the Gateway Base License capacity limit has exceeded. If the notification option for the license capacity limit exceeded alert is configured, Aruba Central sends an email notification with a list of Aruba gateways that exceed the client-capacity threshold. You can also configure alerts to trigger an incident using Webhook. For more information, see Gateway Alerts.

Gateway Foundation, Foundation Base, and Advanced with Security License

The Gateway Foundation with Security License can be assigned to the following gateways:

- Aruba 9004 Gateway
- Aruba 9004-LTE Gateway
- Aruba 9012 Gateway

Virtual Gateway (VGW) License (VPNC only)

The Virtual Gateway License is available on AWS, Azure, and ESXi platforms and are licensed based on bandwidth required: 500 Mbps, 2 Gbps, or 4 Gbps.

Aruba Virtual Gateway is a virtual instance of the headend gateway for ArubaSD-Branch. Aruba Central supports licenses based on the bandwidth capacity for virtual gateways. All license assignments are undertaken by the virtual gateway orchestration app.

The following are the options available for Virtual Gateway Licenses:

- License duration—1 year, 3 years, and 5 years
- Available bandwidths—500 Mbps, 2 Gbps, and 4 Gbps
- Available Aruba Virtual Gateways based on the bandwidth—VGW-500M for 500 Mbps, VGW-2G for 2 Gbps, and VGW-4G for 4Gbps

Aruba Central maintains a pool of Virtual Gateway Licenses. When a Virtual Gateway License expires and there are no available Virtual Gateway Licenses, the expired license is unassigned from the Aruba Central account. The availability of SKUs is dependent on the installation consuming the license. If a Virtual Gateway License expires and there is a similar new license available, the new license is assigned to the Virtual Gateway, provided that the **Auto-Assign Licenses** option is enabled.

For more information about the **Auto-Assign Licenses** option, see Enabling the Auto-Assign Licenses Option.

For an Aruba Central evaluation account, four licenses of each base SKU are assigned to the account. These evaluation licenses are valid for 90 days.

You can track licenses on the **Key Management** page or the **License Assignment** page available from the **Account Home** page.

The list of licenses available against consumed licenses is also displayed during the deployment of a Virtual Gateway.

When the client capacity reaches the threshold, Aruba Central triggers an alert to indicate the Gateway Base License capacity limit has exceeded. If the notification option for the license capacity limit exceeded alert is configured, Aruba Central sends an email notification with a list of Aruba gateways that exceed the client-capacity threshold. You can also configure alerts to trigger an incident using Webhook. For more information, see Gateway Alerts.

For more information, see SD-WAN Ordering Guide.

Supported Features

This section includes detailed information about the different configuration and monitoring options available for Aruba Central features tied to Foundation and Advanced Licenses.

AP Foundation and Advanced License

The AP Foundation and Advanced License for Aruba Central includes the following features:

Feature Category	Foundation License Features	Advanced License Features
Configuration	■ UI- and template-based group configuration ◦ SSID (Bridge Mode) ◦ IAP VPN ■ Auto-commit ■ Configuration audit	All the features in Foundation
Monitoring and Reporting	■ Network Health, Summary, Wi-Fi Connectivity Dashboards ■ Network Topology View ■ Visual RF Floorplans ■ Client List and Details ■ AP List and Details ■ Go Live mode for Client, AP ■ Application Visibility ■ WebCC Firewall rules, visualization by reputation and category ■ Access to all monitoring data for up to 30 days ■ Access to reporting data for up to 90 days ■ Access to historical Client Summary Report data for up to one year ■ Audit Trail ■ Alerts and Events ■ Access, Spectrum, Monitor mode of radio operations ■ UXI Sensor Integration	■ All the features in Foundation ■ AirSlice ◦ Visibility and Prioritization of applications **NOTE:** AirSlice is supported in this release as Early-Access features. Contact your Aruba SE or Account Manager to enable these in your Aruba Central account.
AI Operations	■ AI Search ■ AI Insights ◦ Connectivity—Wi-Fi ◦ Wireless Quality ◦ Availability—Access Points ◦ Class and Company Baselines ■ AI Assist ◦ Dynamic logs **NOTE:** Dynamic Logs is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.	■ All the features in Foundation ■ AI Insights—Wireless Quality ◦ Outdoor clients impacting Wi-Fi performance ◦ Coverage Hole Detection ◦ Transmit power optimization ■ AI Assist ◦ Aruba support notification **NOTE:** Aruba support notification is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.
Troubleshooting	■ Network Check, CLI commands ■ Live Events for Client and AP, Packet Capture	All the features in Foundation

Feature Category	Foundation License Features	Advanced License Features
Services	▪ AirGroup (In InstantOS-based APs, the service is hosted on the IAP Virtual controller and all services are supported.) **NOTE:** AirGroup is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account. ▪ RF Management Services ◦ Adaptive Radio Management (ARM) ◦ ClientMatch ▪ Presence Analytics	▪ All the features in Foundation ▪ UCC **NOTE:** UCC is supported in this release as Early-Access features. Contact your Aruba SE or Account Manager to enable these in your Aruba Central account.
Security	▪ Guest Access ▪ Clients Profile ▪ Rogues ▪ WIPS/WIDS **NOTE:** CPDI-based Client Profile and Rouges are supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable these in your Aruba Central account.	All the features in Foundation
API	Northbound (NB) API: 1000 API calls/day per customer	▪ All the features in Foundation ▪ Streaming API

Switch Foundation License

The Switch Foundation License for Aruba Central includes the following features:

NOTE

Aruba Central does not support Switch Advanced License.

Feature Category	AOS-Switch Features	AOS-CX Features
Configuration	▪ UI- and template-based group configuration ▪ Auto-commit ▪ Configuration audit	▪ UI-, Template-, and MultiEdit-based group configuration ▪ Configuration audit
Monitoring and Reporting	▪ Network Health, Summary Dashboards ▪ Network Topology View ▪ Client List and Details ▪ Switch List and Details ▪ Access to all monitoring data for up to 30 days	▪ Network Health, Summary Dashboards ▪ Network Topology View ▪ Client List and Details ▪ Switch List and Details ▪ Access to all monitoring data for up to 30 days

Feature Category	AOS-Switch Features	AOS-CX Features
	▪ Access to reporting data for up to 90 days ▪ Access to historical Client Summary Report data for up to one year ▪ Audit Trail ▪ Alerts and Events	▪ Access to reporting data for up to 90 days ▪ Access to historical Client Summary Report data for up to one year ▪ Audit Trail ▪ Alerts and Events
AI Operations	▪ AI Search ▪ AI Insights ◦ Availability – Switch ◦ Class and Company Baselines	▪ AI Search ▪ AI Insights ◦ Availability – Switch ◦ Class and Company Baselines
Troubleshooting	▪ Network Check, Device Check, CLI commands ▪ Live Events and Packet Capture for wired client	Network Check, Device Check, CLI commands
API	Northbound (NB) API: 1000 API calls/day per customer	Northbound (NB) API: 1000 API calls/day per customer

Gateway Foundation, Foundation Base, and Advanced License

The Gateway Foundation, Foundation Base, and Advanced License for Aruba Central includes the following features:

The Foundation Base License provides all the features included in the Foundation License, but this license can support only up to 75 client devices per branch.

Feature Category	Foundation and Foundation Base License Features	Advance License Features
SD-Branch	▪ Branch Gateway and VPNC Management ▪ Stateful Firewall ▪ IPsec VPN ▪ Client VPN ▪ Static and Dynamic Routing (BGP, OSPF, RIPv2) ▪ SD-WAN Route and Tunnel orchestration ▪ Orchestrated Cloud IaaS connectivity (AWS, Azure) ▪ Orchestrated SASE Integration ▪ Dynamic Path Steering ▪ Link Redundancy ▪ 4 WAN links plus 1 LTE link ▪ Application-based policies ▪ High Availability (Active-Standby or Active-Active) ▪ Web content filtering ▪ Role-based Access Policy ▪ Full SD-LAN Control	All the features in Foundation

Feature Category	Foundation and Foundation Base License Features	Advance License Features
	▪ CPDI-based Client Profile	
Configuration	▪ UI- and template-based group configuration ▪ Configuration audit	All the features in Foundation
Monitoring and Reporting	▪ Network, WAN Health, Summary Dashboards ▪ Network Topology View ▪ Client List and Details ▪ Gateway List and Details ▪ Go Live mode for Client ▪ Application Visibility ▪ WebCC Firewall rules, visualization by reputation and category ▪ Access to all monitoring data for up to 30 days ▪ Access to reporting data for up to 90 days ▪ Access to historical Client Summary Report data for up to one year ▪ Audit Trail ▪ Alerts and Events	All the features in Foundation
AI Operations	▪ AI Search ▪ AI Insights ◦ Availability – Gateways ◦ Class and Company Baselines ▪ AI Assist ◦ Dynamic logs **NOTE:** Dynamic Logs is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.	All the features in Foundation
Troubleshooting	Network Check, CLI commands	All the features in Foundation
API	Northbound (NB) API: 1000 API calls/day per customer	Streaming API
Services	Not Applicable	SaaS Express

Gateway Foundation, Foundation Base, and Advanced License with Security

The Gateway Foundation, Foundation Base, and Advanced License with Security for Aruba Central includes the following features:

Foundation and Foundation Base with Security	Advanced with Security
All the features in Foundation	All the features in Advanced
▪ Intrusion Detection and Prevention (IDS/IPS)	▪ Intrusion Detection and Prevention (IDS/IPS)

Foundation and Foundation Base with Security	Advanced with Security
▪ Anti-malware ▪ Security Dashboard	▪ Anti-malware ▪ Security Dashboard

Virtual Gateway (VGW) License

The Virtual Gateway (VGW) License for Aruba Central includes the following features:

Feature Category	VGW License Features
SD-Branch	▪ VPNC Management ▪ Stateful Firewall ▪ IPsec VPN ▪ Client VPN ▪ GRE Tunnel ▪ Static and Dynamic Routing (BGP, OSPF, RIPv2) ▪ VGW orchestration in public cloud ▪ SD-WAN Route and Tunnel orchestration ▪ Orchestrated Cloud IaaS connectivity (AWS, Azure) ▪ Orchestrated SASE integration ▪ Link Redundancy ▪ High Availability (Active-Standby or Active-Active)
Configuration	▪ UI- and template-based group configuration ▪ Configuration audit
Monitoring and Reporting	▪ Network, WAN Health, Summary Dashboards ▪ Network Topology View ▪ Access to all monitoring data for up to 30 days ▪ Access to reporting data for up to 90 days ▪ Access to historical Client Summary Report data for up to one year ▪ Audit Trail ▪ Alerts and Events
AI Operations	▪ AI Search ▪ AI Insights ◦ Availability – Gateways ◦ Class and Company Baselines ▪ AI Assist ◦ Dynamic logs **NOTE:** Dynamic Logs is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.
Troubleshooting	Network Check, CLI commands
API	Northbound (NB) API: 1000 API calls/day per customer

For more information about the features supported, see Aruba Central Licenses Feature Details.

Aruba Central Licenses Feature Details

This section provides a description about the different configuration and monitoring options available for Aruba Central features tied to Foundation and Advanced Licenses.

Configuration

AP Configuration

License Applicability: AP configuration is available for AP Foundation License.

Network administrators can manage APs through the Aruba Instant UI, Aruba Central, or AirWave management system. Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AP deployments.

For template-based provisioning, APs must be assigned to a group with template-based configuration method enabled.

AOS-Switch Configuration

License Applicability: AOS-Switch configuration is available for Switch Foundation License.

Network administrators can manage AOS-Switches through the Aruba Central UI menu options. Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AOS-Switch deployments.

AOS-CX Configuration

License Applicability: AOS-CX configuration is available for Switch Foundation License.

Network administrators can manage AOS-CX switches through the Aruba Central UI menu options and the MultiEdit mode. The MultiEdit mode in Aruba Central provides a single window for viewing and editing the configuration for one or more AOS-CX switches. In this mode, viewing and editing the configuration is performed using the CLI syntax.

Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AOS-CX deployments.

Auto-Commit

License Applicability: Auto-Commit is available for Foundation and Advanced Licenses for APs, switches, and gateways.

Aruba Central supports a two-staged configuration commit workflow for Instant APs. When the auto-commit state is enabled for a group, the configuration changes are instantly applied to all devices where the auto-commit state is enabled.

Configuration Audit

License Applicability: Configuration Audit is available for Foundation and Advanced Licenses for APs, switches, and gateways.

In Aruba Central, the Configuration Audit page provides an audit dashboard for reviewing configuration changes of the devices provisioned in the UI and template groups. The Configuration Audit page allows you to view configuration push errors, template synchronization errors, configuration sync, and device-level configuration overrides.

Gateway Configuration

License Applicability: Gateway configuration is available for Gateway Foundation and Foundation Base Licenses.

Aruba Central supports the following methods to configure Gateway groups and Gateways in SD-Branch deployments:

- Guided Setup—You can use the Guided Setup to quickly configure basic and essential parameters on Aruba Gateways for deploying the SD-WAN solution. The Guided Setup provides a wizard-based workflow for provisioning Gateways.
- Basic Mode—Allows you to configure your Gateways in a non-linear fashion. This mode allows you to make configuration changes after you provision your gateways for the first time using a Guided setup.
- Advanced Mode—Allows you to configure advanced features for SD-WAN deployments.

Template groups in Aruba Central allow network administrators to create a common configuration output by using a combination of CLI commands and variables, and apply this configuration to the other Gateway devices provisioned in that group.

Monitoring and Reporting

Access, Spectrum, Monitor Mode of Radio Operations

License Applicability: The Access, Spectrum, and Monitor modes of the radios of an access point are available for AP Foundation and Advanced Licenses.

In the Access mode, the Instant AP serves clients, while also monitoring for rogue Instant APs in the background. In the Monitor mode, the Instant AP acts as a dedicated monitor, scanning all channels for rogue Instant APs and clients. In the Spectrum mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring Instant APs or from non Wi-Fi devices such as microwaves and cordless phones.

Alerts and Events

License Applicability: Alerts and events for APs, Gateways, and switches is part of Foundation License and does not require any extra configuration. This tab shows data for all devices irrespective of device license type.

The **Alerts and Events** dashboard displays a list of alerts and events generated for events pertaining to device provisioning, configuration, and user management. You can view the alerts and events in the **List** view and **Summary** view. **Configuration** view is used to configure alerts and is available only at the **Global** context.

Application Visibility

License Applicability: The Application Visibility feature is a part of a Foundation License. However, as API streaming is available for Advanced Licenses only, the Application Visibility streaming service is supported only for APs with an Advanced License.

Application Visibility is a custom-built Layer-7 firewall capability in Aruba Central that allows you to create firewall policies based on the types of applications in IAPs. Application Visibility provides features like deep packet inspection, application monitoring, and AirSlice Policy.

Audit Trail

License Applicability: Audit Trail logs for APs, gateways, and switches, is part of Foundation License and does not require any extra configuration. This tab shows data for all devices irrespective of device license type.

The **Audit Trail** page in Aruba Central shows the total number of logs generated for all device management, configuration, and user management events triggered in the network.

Client List and Details

License Applicability: Clients monitoring is available for the Foundation License of AP, switch, and gateway.

The **Clients** page is also called the unified clients list and it provides a list of all clients that are connected to access points, switches, or gateways in the network. The List and Summary views under the Clients tab serve as dashboards. It displays details about the network performance, client connection status, instantaneous client refresh, Go Live (only AP), and other information required for monitoring the clients.

Floorplans

License Applicability: Floorplans is available for AP and gateway Foundation Licenses. Floorplans allow you to plan sites, create and manage floorplans, and provision access points. Floorplans provide a real-time picture of the radio environment of your wireless network and the ability to plan the wireless coverage of new sites.

Reports

License Applicability: Reports is available for the Foundation License.

The Reports feature enables you to generate reports for the Clients, Infrastructure, Security Compliance, and Applications categories. The **Reports** feature is present under the **Analyze** section of the **Network Operations** app. The functionalities present are creating a report, generating a report, scheduling the report generation, previewing a report, and downloading a report in PDF and CSV formats. The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days in Aruba Central 2.5.3.

Topology

License Applicability: Topology is available for Foundation and Advanced Licenses for APs, switches, and gateways.

In Aruba Central, the Topology tab in the site dashboard provides a graphical representation of the site, including the network layout, details of the devices deployed, and the health of the WAN uplinks and tunnels. The topology map provides information about third-party devices and devices that are not managed by Aruba. It also provides information about orphan and offline third-party devices, and the VLANs configured on switches running AOS-Switch and AOS-CX software.

Web Content Classification (WebCC)

License Applicability: The WebCC feature is available for Foundation Licenses for APs and gateways.

The WebCC allows you to classify website content based on reputation and take measures to block malicious sites. It fetches information about website content classification and geolocation of IPs. The IP reputation database contains known IP addresses associated with various malicious activities or threats such as botnet, DOS, and spam sources. The geolocation IP database contains the geographical location of the IP address from where the traffic is received or to which the traffic is sent. This provides geolocation and reputation filtering as part of the security suite.

The table below lists the features supported for AP and gateway licenses:

AP Foundation	Gateway Foundation and Foundation Base
WebCC Firewall rules, visualization by reputation and category	WebCC Firewall rules, visualization by reputation and category

Wi-Fi Connectivity

License Applicability: The Wi-Fi Connectivity dashboard for APs is part of Foundation License and does not require any extra configuration.

The **Wi-Fi Connectivity** page displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase. The connection phases include the following:

- **All**—Displays the aggregated success percentage of Association, Authentication, and DHCP for all clients connected to the network.
- **Association**—Displays the percentage of successful attempts made by a client to connect to the network.
- **Authentication**—Displays the percentage of successful attempts of client authentication.
- **DHCP**—Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client.
- **DNS**—Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network.

AI Operations

AI Insights

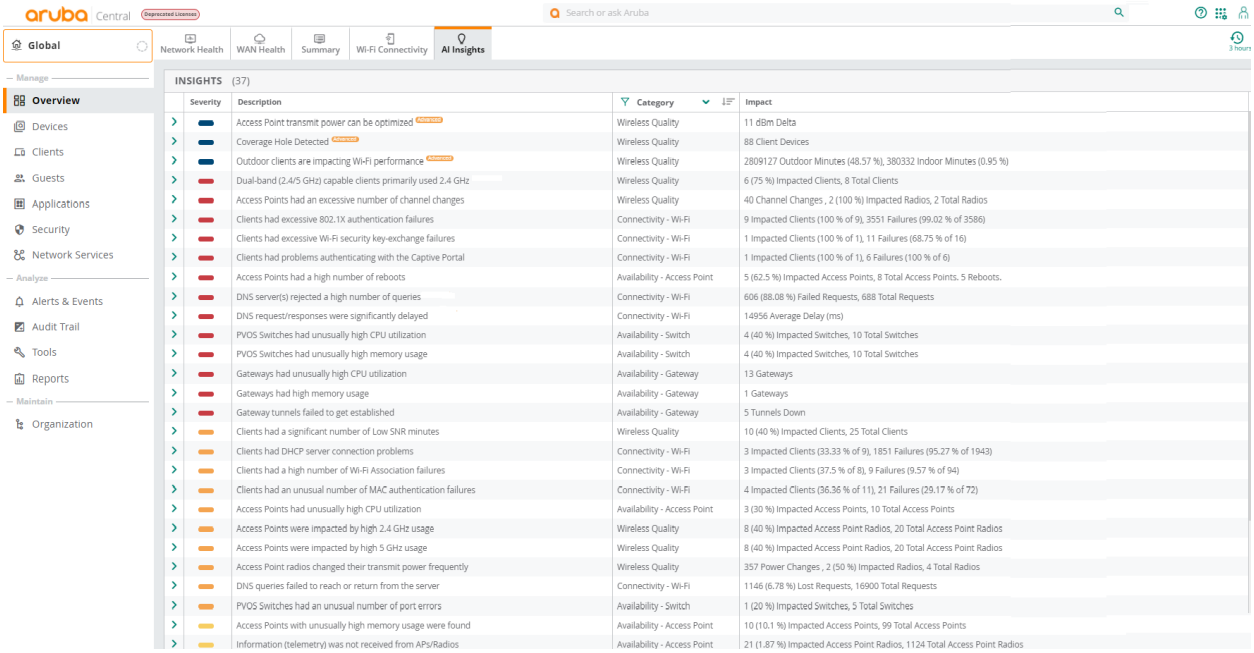
License Applicability: AI Insights is available for Foundation and Advanced Licenses for APs, switches, and gateways. The Insights that require an Advanced License are marked as Advanced in the UI.

The AI Insights dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level for the selected time range. Each insight provides specific details on the occurrences of these events for easy debugging.

Different types of insights are generated by Aruba Central and they can be accessed from different contexts such as Global, Site, Clients, and Device. Some of the insights are part of an Advanced License only and they are marked as Advanced in the user interface.

The following figure displays various AI Insights available and some are marked as Advanced.

Figure 13 *AI Insights List*



The table below lists the features supported for AP, switch, and gateway licenses:

AP Foundation License	AP Advanced License	Switch Foundation	Gateway Foundation, Foundation Base, and VGW
▪ Connectivity—Wi-Fi ▪ Wireless Quality ▪ Availability—Access Points ▪ Class and Company Baselines	▪ Wireless Quality ○ Outdoor clients impacting Wi-Fi performance ○ Coverage Hole Detection ○ Transmit power optimization	▪ Availability—Switch ▪ Class and Company Baselines	▪ Availability—Gateways ▪ Class and Company Baselines

NOTE

In this release, all AI Insights are available irrespective of the user role or Aruba Central subscription. In the upcoming Aruba Central release, AI Insights marked as **Advanced** in the user interface would require an advanced subscription.

AI Search

License Applicability: AI Search feature is available for Foundation License for AP, switch, and gateway.

The AI search feature in Aruba Central enables you to search for clients, devices, and infrastructure connected to the network. Using the search results, you can navigate to the configuration and troubleshooting pages. The search also retrieves relevant documentation to help you efficiently operate your networks. The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant search results.

Dynamic Logs

License Applicability: Dynamic Log is available for both Foundation and Advanced Licenses for APs and gateways.

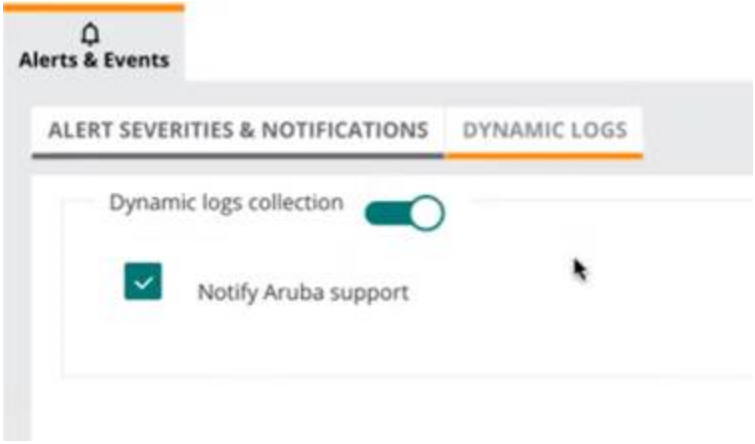
The Dynamic Logs feature enables Aruba Central to dynamically run CLI show commands on APs and gateways, and collect the output as logs. You can also enable Aruba support notification option to notify TAC support regarding the logs generated. These logs can be used to troubleshoot the APs and gateways.

NOTE

Dynamic Logs is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

The following figure displays the available options for Dynamic Logs.

Figure 14 *Dynamic Logs Option*



For devices assigned with the Foundation License, the Dynamic Logs feature only supports the log collection activity. Even if you enable the **Notify Aruba Support** option, the option is not activated for devices licensed with Foundation License.

For devices assigned with Advanced Licenses, Dynamic Logs support both log collection and the Aruba support notification option.

For example, assume an Aruba Central account with Dynamic Logs enabled, where you configure a group of three Access Points (APs), AP1, AP2, and AP3. AP1 has a Foundation License while AP2 and AP3 have Advanced Licenses. For this group, both **Dynamic logs collection** and **Notify Aruba Support** options are enabled. However, the Aruba support notification option is only applicable for AP2 and AP3, which have Advanced Licenses.

Troubleshooting

Live Events

Licensing Applicability: Live Events for clients, APs and switches is part of Foundation License and does not require any extra configuration.

The clients **Live Events** page shows information required to troubleshoot issues related to a client or a site in real time for detailed analysis. Aruba Central also allows to troubleshoot issues related to access points. The AP Live Events feature is similar to client live troubleshooting, but in this case we can enable Live Events at the AP level. Currently, users can subscribe to Radio, VPN, and Spectrum events.

Live Packet Capture (PCAP)

Licensing Applicability: Live PCAP for APs and switches is part of Foundation License and does not require any extra configuration.

Aruba Central allows users to interact and launch a targeted packet capture on a client connected to a specific AP or a switch. When the user starts packet capture from the UI, Aruba Central notifies the AP and the switch. The default packet capture duration is 15 minutes.

Troubleshooting Tools

License Applicability: Troubleshooting for APs, gateways, and switches is part of Foundation License and does not require any extra configuration.

The **Tools** menu option allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central.

The **Tools** page is divided into the following tabs:

- **Network Check**—Allows you to run diagnostic checks on networks and troubleshoot client connectivity issues.
- **Device Check**—Allows you to run diagnostic checks and troubleshoot switches.
- **Commands**—Allows you to perform network health check on devices at an advanced level using command categories.

Services

AirGroup

License Applicability: AirGroup is available for both AP Foundation and Advanced Licenses.

AirGroup is a zero–configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. AirGroup supports both wired and wireless devices.

AirGroup is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

In InstantOS-based APs, the service is hosted on the IAP Virtual controller and all services are supported.

AirMatch

License Applicability: AirMatch is available for AP Foundation License.

AirMatch channel planning evens out channel distributions in any size of network and in any subset of the contiguous network. AirMatch also minimizes channel coupling where adjacent radios are assigned to the same channel.

AirSlice

License Applicability: The AirSlice feature is available for only AP Advanced Licenses.

The AirSlice feature allows network operators to build virtual networks suitable for specific application requirements. It allows network operators to monitor applications used by clients and supports multiple services such as gaming, IoT, voice, video, and so on.

NOTE

AirSlice is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

For devices that have Advanced Licenses, the AirSlice feature supports unlimited applications and provides prioritization of custom-applications with visibility and configuration.

The table below lists the features supported for AP licenses:

Advanced
▪ Visibility and prioritization of applications ▪ Maximum number of applications as supported by the Aruba Central platform

ClientMatch

License Applicability: ClientMatch is available for AP Foundation License.

ClientMatch continually monitors the RF neighborhood for each client to provide ongoing client band steering, load balancing, and enhanced AP reassignment for roaming mobile clients.

Presence Analytics

License Applicability: Presence Analytics is available for Foundation AP License.

Presence Analytics enables businesses to collect and analyze user presence data in public venues, enterprise environments, and retail hubs. Presence Analytics also enables businesses to collect real-time data on user footprints within the wireless network range.

SaaS Express

License Applicability: SaaS Express is available for Advanced Gateway License and Advanced with Security Gateway License only.

The SaaS Express feature, on SD-WAN Gateways, enables discovery of the SaaS application servers, monitors application performance, and steers traffic to the best-available servers, and thus provides an improved user experience.

Unified Communications

License Applicability: Unified Communications is available for AP Advanced Licenses.

The Unified Communications feature enables a seamless user experience for voice calls, video calls, and application-sharing when using communication and collaboration tools. It allows you to actively monitor voice, video, and application-sharing sessions, provide traffic visibility, prioritize the required sessions, and provide rich visual metrics for analytical purposes.

NOTE

Unified Communications is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

Security

Cloud Guest

License Applicability: Cloud Guest is available for the AP Foundation License.

The Cloud Guest access enables the guest users to connect to the network. This is provided through the splash page profile that is created by the administrators for the guest users in the **Guests** tab under

Manage. The **Summary** page in the **Manage > Guest Access** application is the monitoring dashboard that displays the number of guests, guest SSID, client count, type of clients, and guest connection. Cloud Guest deals with the AP, so the license that is assigned to the AP is also applicable to Cloud Guest. By default, the Foundation License is applicable. The Advanced License features will also be available if the Cloud Guest is assigned to it.

ClearPass Device Insight-Based Clients Profile

License Applicability: ClearPass Device Insight (CPDI) based Clients Profile is available for Foundation License for APs and gateways..

The CPDI-based Clients Profile enables network and security administrators to discover, monitor, and automatically classify new and existing devices that connect to a network. You can identify devices that include IoT devices, medical devices, printers, smart devices, laptops, VoIP phones, computers, gaming consoles, routers, servers, switches, and so on.

CPDI-based Clients Profile is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

The table below lists the features supported for AP and gateway licenses:

Foundation	Advanced
▪ Basic client MAC Classification based on telemetry data ▪ Client Family, Client Category, Client OS ▪ Cloud Auth Integration	▪ Access to Collector support in Central (not including physical collector costs) ▪ ML-based client classification ▪ Advanced Security Features (Risk / Posture / Vulnerability) ▪ Security baseline of device behavior with Firewall recommendation

Intrusion Detection and Prevention (IDS or IPS)

License Applicability: IDS and IPS is available for Foundation with Security Gateway License, Foundation Base with Security Gateway License, and Advanced with Security Gateway License.

The IDS and IPS monitors, detects, and prevents threats in the inbound and outbound traffic. Aruba IDS or IPS adds an extra layer of security that focuses on users, applications, network connections, and can be integrated with the Aruba SD-Branch solution.

RAPIDS

License Applicability: RAPIDS is available for Foundation and Advanced Licenses for APs.

The RAPIDS feature enables Aruba Central to quickly identify and act on interfering APs in the network that can be later considered for investigation, restrictive action, or both. Once the interfering APs are discovered, Aruba Central sends alerts for security events to the network administrators about the possible threat and provides essential information needed to locate and manage the threat.

RAPIDS is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

This feature is part of the AP Foundation License. However, as API streaming is available for Advanced License only, Aruba Central would not stream any security events for APs with Foundation License. For APs

with Advanced License, API streaming of security events is available for further diagnosis and threat management.

API

Streaming APIs

License Applicability: The Streaming API service requires that devices such as IAPs and gateways are assigned with Advanced License.

The Streaming API feature enables you to subscribe to a select set of services, instead of polling the NB API to get an aggregated state, or statistics of the events, pertinent to the monitoring activities of Aruba Central. With Streaming API, you can write value-added applications based on the aggregated context.

For example, with Streaming API, you are notified about the following types of events:

- The UP and DOWN status of the devices
- Change in location of stations

The Streaming API feature in Aruba Central is enabled only when any one of the devices in the account has an Advanced License. If the account has devices with only Foundation License, the Steaming API tab is not displayed in Aruba Central.

If the Streaming API feature is enabled, and the account has a mix of Foundation License and Advanced License for devices, the devices that are assigned with Foundation License do not stream any data for any topics.

SD-Branch

Application-based Policy

License Applicability: The application-based policy configuration is available for Foundation License for Branch Gateways.

The Application-based policy configuration helps in deep packet inspection of application usage by clients. Using this configuration, you can define applications, security, and service aliases. You can configure Access Control Lists (ACLs) to restrict user access to an application or application category.

Dynamic Path Steering

License Applicability: Dynamic Path Steering is available for Gateway Foundation and Foundation Base License.

In the **Path Steering** tab, you can view traffic path steering details for the Dynamic Path Steering policies configured on the Branch Gateway. This tab also displays the number of policies that are compliant along with the total number of policies configured on the Branch Gateway.

Full SD-LAN Control

License Applicability: SD-LAN monitoring is available for Foundation License for Branch Gateways.

The LAN Summary page displays a graphical representation of the LAN link availability of a Branch Gateway. It also provides a summary of all the LAN interfaces and port details.

IPsec VPN

License Applicability: IPsec VPN is available for Gateway Foundation and Foundation Base License.

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the controller secures corporate data. You can configure an IPsec tunnel from virtual controller using Aruba Central.

Role-based Access Policy

License Applicability: Role-based Access Policy configuration is available for Foundation License for Branch Gateways.

The Role-based Access Policy determines client access based on the user roles assigned to a client. Each user or device connected to the branch network is associated with a user role. Once the role is assigned, traffic and security policies are applied to devices based on the role.

SD-WAN Overlay

License Applicability: SD-WAN Overlay monitoring is available for Gateway Foundation License.

The SD-WAN Overlay is an orchestrator service for branch deployments, which is done by setting up IPsec tunnels between the Branch Gateways and VPN Concentrators. This is achieved through **Tunnel** and **Route** orchestration. The tunnel configuration between the branch and hub sites is automatic and the route configuration is done by redistributing the routing information learnt from the branch in a dynamic way. The **Map** and **Grid** views of the **Tunnel** and **Route** tabs under **SD-WAN Overlay** serve as dashboards for monitoring purpose, providing information about the tunnels and routes configured for an individual Branch Gateway.

Stateful Firewalls

License Applicability: Stateful Firewalls is available for Gateway Foundation and Foundation Base License.

Aruba Gateways support stateful firewall for stateful inspection of packets. Stateful firewalls provide an additional layer of security by tracking the state of network connections and using the state information from previous communications to monitor and control new communication attempts. To protect your network from external attacks and unauthorized communication attempts, you can configure match conditions and packet filtering criteria for the Aruba Gateways.

Web Content Filtering

License Applicability: Website content filtering is available for Foundation License for Branch Gateways. Aruba Gateways enhance branch security by providing real-time web content and reputation filtering. The Website Content Classification feature on Branch Gateways allows you to classify website content based on reputation and take measures to block malicious sites.

Starting Your Free Trial

Aruba Central offers a 90-day evaluation license for customers who want to try the solution for managing their networks.

The evaluation license allows you to use the functions described in the following table:

Table 21: *Evaluation features*

Application	Function
Network Operations	▪ 10 Advanced AP Licenses ▪ 5 Foundation Switches 6100 / 25xx / low density (16 ports or less) Licenses ▪ 5 Foundation Switches 6200 / 29xx Licenses ▪ 5 Foundation Switches 6300 / 3810 Licenses ▪ 5 Foundation Switches 8xxx / 6400 / 5400 Licenses ▪ 5 Advanced 90xx Gateways with security feature Licenses ▪ 10 Advanced 70xx Gateways Licenses

Application	Function
	■ 2 Advanced 72xx Gateways Licenses
ClearPass Device Insight	Discover, monitor, and automatically classify new and existing devices that connect to a network.

Complete the following steps to evaluate Aruba Central:

Step 1: Getting Started with the Initial Setup

To get started with the trial:

1. Register for evaluating Aruba Central. For more information, see Creating an Aruba Central Account.
2. Log in to Aruba Central. For more information, see Accessing Aruba Central Portal.
   - If you signed up to evaluate only the **Network Operations** app, the **Welcome to Aruba Central** page is displayed.
     - Click **Evaluate Now**. The **Get Started With Aruba Central** page guides you through the onboarding steps.
     - Click through the steps to set up your account and start using Aruba Central. If you want to exit the wizard and complete the onboarding steps on your own, click **Exit Workflow**.

The Initial Setup wizard is displayed only when you log in to Aruba Central for the first time. The wizard is not available for Aruba Central users in the MSP mode.

   - If you signed up to evaluate both **Network Operations** and **ClearPass Device Insight**, the **Network Operations** page is displayed.

     For more information, see ClearPass Device Insight Information Center.

Step 2: Viewing Subscription Details (Optional)

At your first login, the **Initial Setup** wizard displays the details of the evaluation license details. After you exit the wizard, you can view the license details on the **Account Home** > **Global Settings** > **Key Management** page.

Viewing Subscription Key Details

The following table shows the typical contents of a license key:

Table 22: *License Key Details*

Keys	Subscription key number
Type	Type of the license. Aruba Central supports the following types of licenses: ■ **Foundation**—This license provides all the features included in the Device Management subscription and some additional features that were available as value-added services for APs in the earlier licensing model. ■ **Advanced**—This license provides all the features of a Foundation license, with additional features related to AI insights
Expiration Date	Expiration date for the license key.
Quantity	Number of licenses available.
Status	Status of the license key. For example, if you are a trial user, Aruba Central displays the status of subscription key as **Eval**.

Step 3: Adding Devices

To manage devices from Aruba Central, trial users must manually add the devices to Aruba Central's device inventory.

You can add up to 60 devices. The devices can be APs, switches, or gateways. For details about how many device licenses of each type are available, see Table 21.

Use one of the following methods to add devices to Aruba Central:

- Using the Initial Setup Wizard
- Using the Device Inventory Page

Using the Initial Setup Wizard

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number and MAC address of your devices.

   You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
3. Click **Done**.
4. Review the devices in your inventory.

Using the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.

   The **Device Inventory** page is displayed.
2. Click **Add Devices**.

   The **Add Devices** pop-up window is displayed.
3. Enter the serial number and the MAC address of each device.

   You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.

4. Click **Done**.
5. Review the devices in your inventory.

Step 4: Assigning Subscriptions

By default, an evaluation license key is assigned for users who sign up for a free trial of Aruba Central. The evaluation license key allows you to manage up to 60 devices from Aruba Central.

You can either enable automatic assignment of license or manually assign Foundation and Advanced licenses to your devices. By default, the automatic license assignment is disabled.

Enabling Automatic Assignment of Subscriptions

Use one of the following options to enable automatic assignment of licenses:

In the Initial Setup Wizard

1. Verify that you have a valid license key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the **Assign License** tab, slide the **Auto License** toggle switch to the On position.

From the License Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **License Assignment**.
2. Under **Device Licenses**, slide the **Auto License** toggle switch to the On position. All the devices in your inventory are selected for automatic assignment of a license. You can edit the list by clearing the existing selection and re-selecting devices.

Manually Assigning Subscriptions

Use one of the following options to manually assign subscriptions:

In the Initial Setup Wizard

1. In the **Assign License** tab, ensure that the **AutoLicense** toggle switch is turned off.
2. Select the devices in the list for which you want to manually assign licenses.
3. Click **Update Licenses**.

From the Subscription Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **License Assignment**.
2. On the **License Assignment** page, ensure that the **Auto License** toggle is turned off.
3. Select the devices to which you want to assign licenses.
4. Click **Update Licenses**.

For more information on subscriptions. see Managing Licenses.

Step 5: Organizing Your Devices into Groups

A group in Aruba Central functions as a configuration container for devices added in Aruba Central.

Why Should You Use Groups?

Groups allow you to create a logical subset of devices and simplify the configuration and device management tasks. Groups offer the following functions and benefits:

- Combining different types of devices under a group. For example, a group can have APs and switches. Aruba Central allows you to manage configuration of these devices in separate containers (wireless and wired management) within the same group. Any new device that is added to a group inherits the current configuration of the group.
- Assigning multiple devices to a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to member Instant APs in their respective clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.
- Cloning an existing group allows you to create a base configuration for the devices and customize it as per your network requirements.

You can also use groups for filtering your monitoring dashboard content, generating reports, and managing software upgrades.

A device can be part of only one group at any given time.
Groups in Aruba Central are independent and do not follow a hierarchical model.

For more information on groups and group configuration workflows, see Groups for Device Configuration and Management.

Assigning Devices to Groups

After you successfully complete the onboarding workflow, the **Initial Setup** wizard prompts you to assign your devices to a group. You can click **Assign Group** and assign your devices to a group. You can also use one of the following methods to assign your devices to groups:

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory.**

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 6: Assigning Sites and Labels (Optional)

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you can create a site called CampusA. You can also tag the devices within CampusA using labels. If your campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**.

For more information on sites and labels and how to assign devices to sites and labels, see Managing Sites and Managing Labels.

Step 7: Configuring Your Network

If you have added Instant APs as part of your evaluation, you can configure an employee and guest wireless network. If you have Switches or SD-Branch or SD-WAN Gateways, configure wired access network or SD-WAN respectively.

For more information, see Device Configuration and Network Management.

Step 8: Monitoring Your Network and Devices

Use monitoring dashboards to view the health of the device and network. You can also run reports, configure alerts, and view client details.

Step 9: Canceling or Upgrading Your Subscription (Optional)

During the trial period or after you complete your trial, if you want to continue using Aruba Central for managing your devices, contact Aruba Customer Support to upgrade your license.

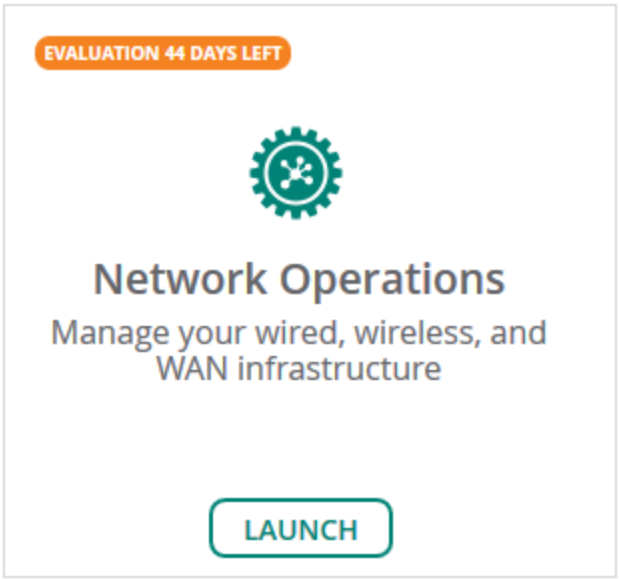
If you do not want to continue, contact Aruba support team to cancel your license or wait until the trial expires. When the trial period expires, your devices can no longer be managed from Aruba Central.

Upgrading to a Paid Account

If you have purchased a license for an AP, a switch, or a gateway, then upgrade your account by completing the following steps:

1. On the **Account Home** page, in the **Network Operation** app, click the link that shows the number of days left for the evaluation to expire.

   Figure 15 *Network Operations Evaluation Account*

   The **Add a New License** window is displayed.
2. Enter the new license key that you purchased from Aruba.
3. Click **Add License**.

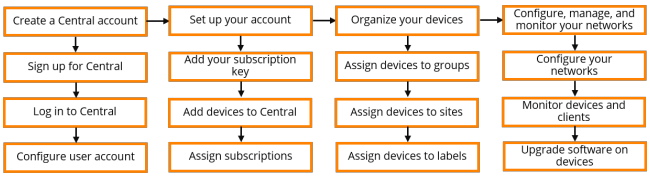
After you upgrade your account, you can add more devices, enable services, and continue using Aruba Central.

Setting up Your Aruba Central Instance

If you have purchased a license key to manage your devices and networks from Aruba Central, get started with steps described in this topic.

Figure 16 illustrates the steps required for setting up your Aruba Central instance:

Figure 16 *Getting Started Workflow*



Getting Started with Aruba Central

Complete the following steps to start using Aruba Central for managing your devices and setting up your networks.

- Step 1: Getting Started
- Step 2: Adding a Subscription Key
- Step 3: Adding Devices
- Step 4: Assigning Subscriptions
- Step 5: Organizing Your Devices into Groups
- Step 6: Assigning Sites and Labels (Optional)
- Step 7: Configuring Users
- Step 8: Configuring and Managing Networks
- Step 9: Monitoring Your Network and Devices
- Step 10: Upgrading Software Images on Devices
- Step 11: Running Diagnostic Checks and Troubleshooting Issues

Step 1: Getting Started

To get started:

1. Sign up to create your Aruba Central account. For more information, see Creating an Aruba Central Account.
2. If you already have an Aruba Central account, log in to Aruba Central with your credentials. When you log in for the first time, the **Initial Setup** wizard opens and guides you through the onboarding workflow.
3. Click **Get Started**.
4. Click through the wizard to complete the onboarding workflow. If you want to exit the wizard and complete the onboarding steps on your own, click **Exit and go to Aruba Central**.

The Initial Setup wizard is displayed only when you log in to Aruba Central for the first time. The wizard is not available for Aruba Central users in the MSP mode.

Step 2: Adding a Subscription Key

At your first login, the **Initial Setup** wizard prompts you add your license key.

If you are not using the wizard, complete the following steps to add your license key.

1. On the **Account Home** page, under **Global Settings**, click **Key Management**.

   The **Key Management** page is displayed.
2. Enter your license key.
3. Click **Add Key**.

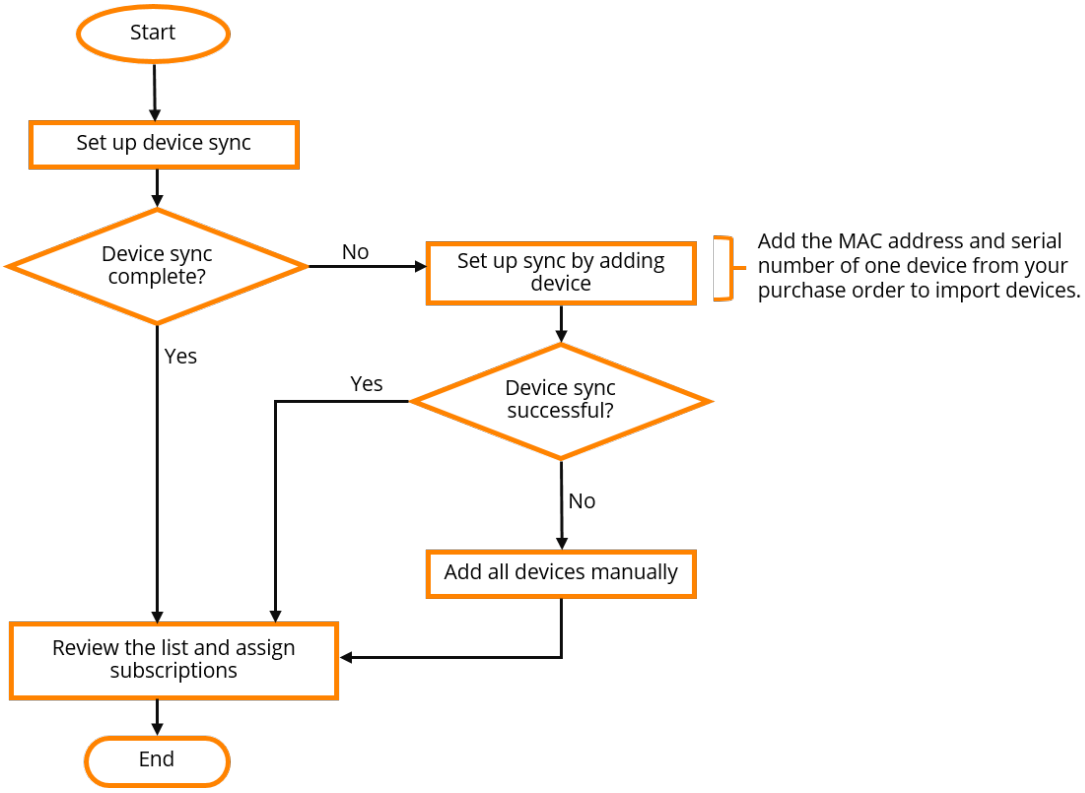
   The license key is added to Aruba Central and the contents of the license key are displayed in the **Manage Keys** table. Review the license details.

   If you add a **Device Management** token, the key is listed in the **Convert Deprecated Licenses** page. For more information, see Converting Legacy Tokens to New Licenses.

Step 3: Adding Devices

If you have a paid license, you can automatically import devices from the Activate database to the Aruba Central device inventory.

Figure 17 *Typical Workflow for Device Sync Setup*



Setting up Device Sync for Automatic Device Addition

To set up device sync, use one of the following methods:

- In the Initial Setup Wizard
- From the Device Inventory Page

In the Initial Setup Wizard

1. Ensure that you have added a license key and click **Next**.
2. In the **Add Devices** tab, enter the serial number and MAC address of any one device from your purchase order.

   Most Aruba devices have the serial number and MAC address on the front or back of the hardware.
3. Click **Add Device**. Aruba Central imports all other devices mapped to your purchase order.
4. Review the devices in your inventory.
5. Perform the following options:
   - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
   - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
   - **Contact support**—Contact Aruba Technical Support.

From the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.

   The **Device Inventory** page is displayed.

Aruba Central imports only devices associated with your account from Activate.

2. Do any one of the following:
   - Click **Sync Devices**. Enter the serial number and MAC address and click **Add Device**.
   - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
   - If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.

Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home** > **Audit Trail** page.

3. Review the devices in your inventory.
4. Perform the following options:
   - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
   - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
   - **Contact support**—Contact Aruba Technical Support.

Manually Adding Devices

To add devices using MAC address and serial number, use any one of the following methods:

- In the Initial Setup Wizard
- From the Device Inventory Page

In the Initial Setup Wizard

If you are using the Initial Setup wizard:

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number or the MAC address of your device.
3. Click **Done**.
4. Review the list of devices.

From the Device Inventory Page

To add devices from the **Device Inventory** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The **Device Inventory** page is displayed.
2. Perform one of the following:
   - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
   - If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.

Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home** > **Audit Trail** page.

3. Click **Done**.
4. Review the devices added to the inventory.

When you add the serial number and MAC address of one AP from a cluster or a switch stack member, Aruba Central imports all devices associated in the AP cluster and switch stack respectively.

For more information on adding devices, see Onboarding Devices.

Step 4: Assigning Subscriptions

Aruba Central supports the following types of licenses:

- Foundation—This license provides all the features included in the Device Management subscription and some additional features that were available as a value- added services for APs in the earlier licensing model.
- Advanced—This license provides all the features of a Foundation License, with additional features related to AI insights.

You can either enable automatic assignment of license or manually assign licenses to your devices. By default, the automatic license assignment is disabled.

Enabling Automatic Assignment of Licenses

Use any one of the following options to enable automatic assignment of licenses:

- In the Initial Setup Wizard
- From the License Assignment Page

In the Initial Setup Wizard

1. Verify that you have a valid license key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the **License Assignment** tab, slide the **Auto Assign Licenses** toggle switch to the On position.

From the License Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **License Assignment**.
2. Under **Device Subscriptions**, toggle the **Auto Assign Licenses** slider to ON. All the devices in your inventory are selected for automatic assignment of licenses. You can edit the list by clearing the existing selection and re-selecting devices.
   For more information on how auto licensing works, see Automatic License Assignment Workflow.

Manually Assigning Licenses

Use any one of the following methods to manually assign the licenses:

- In the Initial Setup Wizard
- From the License Assignment Page

In the Initial Setup Wizard

1. In the **Assign License** tab, ensure that the **Auto License** toggle switch is turned off.
2. Select the devices in the list for which you want to manually assign subscriptions.
3. Click **Update License**.

From the License Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **License Assignment**.
2. On the **License Assignment** page, ensure that the **Auto License** toggle is turned off.
3. Select the devices to which you want to assign licenses.
4. Click **Update License**.

For more information on subscriptions and how to assign network service and SD-WAN Gateway subscriptions. see Managing License Assignments.

Step 5: Organizing Your Devices into Groups

A group in Aruba Central functions as a configuration container for devices added in Aruba Central.

Why Should You Use Groups?

Groups allow you to create a logical subset of devices and simplify the configuration and device management tasks. Groups offer the following functions and benefits:

- Combining different types of devices under a group. For example, a group can have Instant APs and Switches. Aruba Central allows you to manage the configuration of these devices in separate containers (wireless and wired management) within the same group. Any new device that is added to a group inherits the current configuration of the group.
- Assigning multiple devices to a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to member Instant APs in their respective clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.

- Cloning an existing group allows you to create a base configuration for the devices and customize it according to your network requirements.

You can also use groups for filtering your monitoring dashboard content, generating reports, and managing software upgrades.

A device can be part of only one group at any given time.
Groups in Aruba Central are independent and do not follow a hierarchical model.

For more information on groups and group configuration workflows, see Groups for Device Configuration and Management.

Assigning Devices to Groups

After you successfully complete the onboarding workflow, the **Initial Setup** wizard prompts you to assign your devices to a group. You can click **Assign Group** and assign your devices to a group. You can also use any one of the following methods to assign your devices to groups.

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory.**

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 6: Assigning Sites and Labels (Optional)

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you could create a site called CampusA. You can also tag the devices within CampusA using labels. If your campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**.

For more information on sites and labels and how to assign devices to sites and labels, see Managing Sites and Managing Labels.

Step 7: Configuring Users

Add system users, assign user roles, and configure role-based access control.

For more information, see Configuring System Users.

Step 8: Configuring and Managing Networks

To start configuring your network setup:

1. Connect your devices to Aruba Central. For more information, see Connecting Devices to Aruba Central.
2. Provision Instant APs, switches, or gateways to set up your WLAN, wired access, and SD-WAN network.

Step 9: Monitoring Your Network and Devices

Use monitoring dashboards to view the health of the device and network.

You can also run reports, configure alerts, and view client details.

Step 10: Upgrading Software Images on Devices

View software images available for the devices provisioned in your account, run a compliance check for the recommended software version, and upgrade devices.

For more information and step-by-step instructions, see Managing Software Upgrades.

Step 11: Running Diagnostic Checks and Troubleshooting Issues

Run diagnostic checks and troubleshooting commands to analyze network connectivity, latency issues, and debug device issues, if any. For more information and step-by-step instructions, see Using Troubleshooting Tools.

Configuring Email Notifications for Software Upgrades

Aruba Central administrators would receive email notifications before software upgrades, scheduled maintenance activity, or any unplanned outage. By default, email notifications are enabled. The banner is updated in the Aruba Central UI seven days before the upgrade and an email notification is sent seven days before the upgrade. In case of an unplanned outage, an email notification is sent immediately and the banner is also updated immediately in the Aruba Central UI.

The email notification contains the following details:

- Start date and time.
- Estimated end date and time.
- Link to the **What's New** page where users can view the list of new features and enhancements included in the release.
- Impact of the outage.

Users can no longer check the status of Aruba Central using the following URLs:

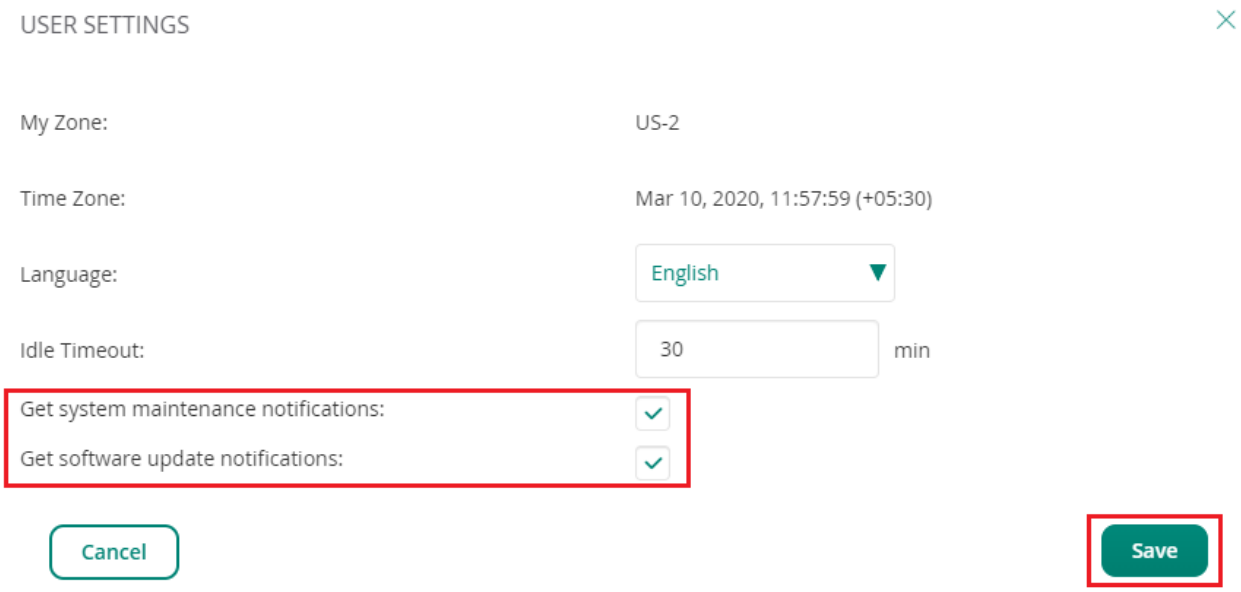
- US—http://status.central.arubanetworks.com
- Canada—http://ca-status.central.arubanetworks.com
- APAC—http://apac-status.central.arubanetworks.com
- APAC East—http://apaceast-status.central.arubanetworks.com
- Europe—http://eu-status.central.arubanetworks.com

Enabling Email Notifications

By default, email notifications are enabled. However, if email notifications are disabled and you wish to enable system maintenance or software update email notifications, complete the following steps:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **User Settings**.
3. In the **User Settings** pop-up window, do the following:
   a. Select the **Get system maintenance notifications** check box to receive system maintenance notification on the registered email ID. Email notifications are sent before any scheduled maintenance activity or unplanned outage.
   b. Select the **Get software update notifications** check box to receive software update notification on the registered email ID.
4. Click **Save**.

Figure 18 *Email Notifications*



Configuring Idle Timeout

Aruba Central allows you to set a timeout value for inactive user sessions. The value is in minutes and is the amount of time a user can be inactive before the user's session times out and closes.

To configure idle timeout, complete the following steps:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **User Settings**.
3. In the **User Settings** pop-up window, enter the timeout value in the **Idle Timeout** field. The value must be within the range of 5 to 10080 minutes.
4. Click **Save**.

Opening Firewall Ports for Device Communication

Most of the communication between devices on the remote site and Aruba Central server in the cloud is carried out through HTTPS (TCP 443). To allow devices to communicate over a network firewall, ensure that the following domain names and ports are open.

This section includes the following topics:

- Domain names for Aruba Central Portal Access
- Domain Names for Device Communication with Aruba Central
- Domain Names for Device Communication with Aruba Activate
- Cloud Guest Server Domains for Guest Access Service
- Domain Names for OpenFlow
- Other Domain Names

Domain names for Aruba Central Portal Access

Table 23: *Domain Names and URLs for Aruba Central Portal Access*

Region	Domain Name	Protocol
US-1	portal.central.arubanetworks.com	HTTPS TCP port 443
US-2	portal-prod2.central.arubanetworks.com	HTTPS TCP port 443
US-WEST-4	portal-uswest4.central.arubanetworks.com	HTTPS TCP port 443
EU-1	portal-eu.central.arubanetworks.com	HTTPS TCP port 443
EU-2	portal-eucentral2.central.arubanetworks.com	HTTPS TCP port 443
EU-3	portal-eucentral3.central.arubanetworks.com	HTTPS TCP port 443
Canada-1	portal-ca.central.arubanetworks.com	HTTPS TCP port 443
China-1	portal.central.arubanetworks.com.cn	HTTPS TCP port 443
APAC-1	portal-apac.central.arubanetworks.com	HTTPS TCP port 443
APAC-EAST1	portal-apaceast.central.arubanetworks.com	HTTPS TCP port 443
APAC-SOUTH1	portal-apacsouth.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with Aruba Central

Table 24: *Domain Names for Device Communication with Aruba Central*

Region	Aruba Central URL	URL for Device Connectivity	Protocol	FQDNs for SD-WAN Orchestrator Service
US-1	app.central.arubanetworks.com	app1.central.arubanetworks.com	HTTPS	app1-h2.central.arubanetworks.com

Region	Aruba Central URL	URL for Device Connectivity	Protocol	FQDNs for SD-WAN Orchestrator Service
			TCP port 443	
US-2	app-prod2.central.arubanetworks.com	device-prod2.central.arubanetworks.com	HTTPS TCP port 443	device-prod2-h2.central.arubanetworks.com
US-WEST-4	app-uswest4.central.arubanetworks.com	device-uswest4.central.arubanetworks.com	HTTPS TCP port 443	device-uswest4-h2.central.arubanetworks.com
EU-1	app2-eu.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443	device-eu-h2.central.arubanetworks.com
EU-2	app-eucentral2.central.arubanetworks.com	device-eucentral2.central.arubanetworks.com	HTTPS TCP port 443	device-eucentral2-h2.central.arubanetworks.com
EU-3	app-eucentral3.central.arubanetworks.com	device-eucentral3.central.arubanetworks.com	HTTPS TCP port 443	device-eucentral3-h2.central.arubanetworks.com
Canada-1	app-ca.central.arubanetworks.com	device-ca.central.arubanetworks.com	HTTPS TCP port 443	device-ca-h2.central.arubanetworks.com
China-1	app.central.arubanetworks.com.cn	device.central.arubanetworks.com.cn	HTTPS TCP port 443	device-h2.central.arubanetworks.com.cn
APAC-1	app2-ap.central.arubanetworks.com	app1-ap.central.arubanetworks.com	HTTPS TCP port 443	app1-ap-h2.central.arubanetworks.com
APAC-EAST 1	app-apaceast.central.arubanetworks.com	device-apaceast.central.arubanetworks.com	HTTPS TCP port 443	device-apaceast-h2.central.arubanetworks.com
APAC-SOUTH1	app-apacsouth.central.arubanetworks.com	device-apacsouth.central.arubanetworks.com	HTTPS TCP port 443	device-apacsouth-h2.central.arubanetworks.com

Domain Names for AOS-CX Device Communication with Aruba Central

Table 25: *Domain Names for AOS-CX Device Communication with Aruba Central*

Region	Aruba Central URL	URL for Device Connectivity	Protocol
US-1	app.central.arubanetworks.com	device-prod-d2.central.arubanetworks.com	HTTPS TCP port 443
US-2	app-prod2.central.arubanetworks.com	device-prod2.central.arubanetworks.com	HTTPS TCP port 443
US-WEST-4	app-uswest4.central.arubanetworks.com	device-uswest4-d2.central.arubanetworks.com	HTTPS TCP port 443
EU-1	app2-eu.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443
EU-2	app-eucentral2.central.arubanetworks.com	device-eucentral2-d2.central.arubanetworks.com	HTTPS TCP port 443
EU-3	app-eucentral3.central.arubanetworks.com	device-eucentral3-d2.central.arubanetworks.com	HTTPS TCP port 443
Canada-1	app-ca.central.arubanetworks.com	device-ca.central.arubanetworks.com	HTTPS TCP port 443
China-1	app.central.arubanetworks.com.cn	device.central.arubanetworks.com.cn	HTTPS TCP port 443
APAC-1	app2-ap.central.arubanetworks.com	app1-ap.central.arubanetworks.com	HTTPS TCP port 443
APAC-EAST1	app-apaceast.central.arubanetworks.com	device-apaceast.central.arubanetworks.com	HTTPS TCP port 443
APAC-SOUTH1	app-apacsouth.central.arubanetworks.com	device-apacsouth.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with Aruba Activate

Table 26: *Domain Names for Device Communication with Aruba Activate*

Domain Name	Protocol
device.arubanetworks.com	HTTPS TCP port 443
devices-v2.arubanetworks.com	
est.arubanetworks.com *	

* Required for Aruba 2530 switches to provision certificate using the EST server in activate.

Cloud Guest Server Domains for Guest Access Service

Table 27: *Domain Names for Cloud Guest Server Access*

Region	Domain Name	Protocol
US-1	nae1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	nae1-elb.cloudguest.central.arubanetworks.com	TCP port 443
US-2	naw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	naw2-elb.cloudguest.central.arubanetworks.com	TCP port 443
US-WEST-4	uswest4.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	uswest4-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-1	euw1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	euw1-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-2	naw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	naw2-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-3	euw1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	euw1-elb.cloudguest.central.arubanetworks.com	TCP port 443
Canada-1	ca.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	ca-elb.cloudguest.central.arubanetworks.com	TCP port 443
APAC-1	ap1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443

Region	Domain Name	Protocol
	ap1-elb.cloudguest.central.arubanetworks.com	TCP port 443
APAC-EAST1	apaceast.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	apaceast-elb.cloudguest.central.arubanetworks.com	TCP port 443
APAC-SOUTH1	apacsouth.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	apacsouth-elb.cloudguest.central.arubanetworks.com	TCP port 443

Domain Names for OpenFlow

Table 28: *Domain Names for OpenFlow*

Region	Domain Name
US-1	https://app2-ofc.central.arubanetworks.com
US-2	https://ofc-prod2.central.arubanetworks.com
US-WEST-4	https://ofc-uswest4.central.arubanetworks.com
EU-1	https://app2-eu-ofc.central.arubanetworks.com
EU-2	https://ofc-eucentral2.central.arubanetworks.com
EU-3	https://ofc-eucentral3.central.arubanetworks.com
Canada-1	https://ofc-ca.central.arubanetworks.com
China-1	https://ofc.central.arubanetworks.com.cn
APAC-1	https://app2-ap-ofc.central.arubanetworks.com
APAC-EAST1	https://ofc-apaceast.central.arubanetworks.com
APAC-SOUTH1	https://ofc-apacsouth.central.arubanetworks.com

Other Domain Names

Table 29: *Other Domain Names*

Domain Name	Protocol	Description
sso.arubanetworks.com	TCP port 443	Allows users to access their accounts on the internal server.
internal.central.arubanetworks.com internal2.central.arubanetworks.com	TCP port 443	Allows users to access the Aruba Central Internal portal.
pool.ntp.org	UDP port 123	Allows users to update the internal clock and configure time zone when a factory default device comes up.

Domain Name	Protocol	Description
		By default, the Aruba devices contact **pool.ntp.org** and use NTP to synchronize their system clocks.
activate.arubanetworks.com	TCP port 443	Allows users to configure provisioning rules in Activate.
stun.pqm.arubanetworks.com	UDP or TCP port 3478 and 3479	Allows users to discover public IP over the WAN uplinks configured on devices.
pqm.arubanetworks.com	ICMP or UDP port 4500	Allows users to check the health of WAN uplinks configured on Branch Gateways.
images.arubanetworks.com	TCP port 80	Allows users to access the server that hosts software images available for upgrading devices.
http://h30326.www3.hpe.com	TCP port 80	Allows users to access the Aruba switch software images. To view the URL for software updates, use the **show activate software-update** command.
d2vxf1j0rhr3p0.cloudfront.net	TCP port 443	Allows users to access the CloudFront server for locating Instant AP software images.
rcs-m.central.arubanetworks.com (For all other regions) central-eu-rcs.central.arubanetworks.com (For Europe region)	TCP port 443	Allows users to access a device console through SSH.
cloud.arubanetworks.com	TCP port 80	Allows users to open the Aruba Central evaluation sign-up page.
aruba.brightcloud.com	TCP port 443	Enables devices to access the Webroot Brightcloud server for application, application categories, and website content classification.
bcap15-dualstack.brightcloud.com	TCP port 443	Allows Aruba devices to look up the Webroot Brightcloud server for Website categories.
api-dualstack.bcti.brightcloud.com	TCP port 443	Allows Aruba devices to access the IP Reputation and IP Geolocation service on the Webroot Brightcloud server.
database-dualstack.brightcloud.com	TCP port 443	Allows Aruba devices to download the website classification database from the Webroot Brightcloud server.

When configuring ACLs to allow traffic over a network firewall, use the domain names instead of the IP addresses.
For Branch Gateways to set up IPsec tunnel with the VPN concentrators, the UDP 4500 port must be open.

Connecting Devices to Aruba Central

Aruba devices support automatic provisioning, also known as ZTP. In other words, Aruba devices can download provisioning parameters from Aruba Activate and connect to their management entity once they are powered on and connected to the network.

Although most of the communication between devices on the remote site and Aruba Central server in the cloud is carried out through HTTPS (TCP 443), you may want to open the following ports for devices to communicate over network firewall.

This section includes the following topics:

Domain names for Aruba Central Portal Access

Table 30: *Domain Names and URLs for Aruba Central Portal Access*

Region	Domain Name	Protocol
US-1	portal.central.arubanetworks.com	HTTPS TCP port 443
US-2	portal-prod2.central.arubanetworks.com	HTTPS TCP port 443
US-WEST-4	portal-uswest4.central.arubanetworks.com	HTTPS TCP port 443
EU-1	portal-eu.central.arubanetworks.com	HTTPS TCP port 443
EU-2	portal-eucentral2.central.arubanetworks.com	HTTPS TCP port 443
EU-3	portal-eucentral3.central.arubanetworks.com	HTTPS TCP port 443
Canada-1	portal-ca.central.arubanetworks.com	HTTPS TCP port 443
China-1	portal.central.arubanetworks.com.cn	HTTPS TCP port 443
APAC-1	portal-apac.central.arubanetworks.com	HTTPS TCP port 443
APAC-EAST1	portal-apaceast.central.arubanetworks.com	HTTPS TCP port 443
APAC-SOUTH1	portal-apacsouth.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with Aruba Central

Table 31: *Domain Names for Device Communication with Aruba Central*

Region	Aruba Central URL	URL for Device Connectivity	Protocol	FQDNs for SD-WAN Orchestrator Service
US-1	app.central.arubanetworks.com	app1.central.arubanetworks.com	HTTPS TCP port 443	app1-h2.central.arubanetworks.com
US-2	app-prod2.central.arubanetworks.com	device-prod2.central.arubanetworks.com	HTTPS TCP port 443	device-prod2-h2.central.arubanetworks.com
US-WEST-4	app-uswest4.central.arubanetworks.com	device-uswest4.central.arubanetworks.com	HTTPS TCP port 443	device-uswest4-h2.central.arubanetworks.com
EU-1	app2-eu.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443	device-eu-h2.central.arubanetworks.com
EU-2	app-eucentral2.central.arubanetworks.com	device-eucentral2.central.arubanetworks.com	HTTPS TCP port 443	device-eucentral2-h2.central.arubanetworks.com
EU-3	app-eucentral3.central.arubanetworks.com	device-eucentral3.central.arubanetworks.com	HTTPS TCP port 443	device-eucentral3-h2.central.arubanetworks.com
Canada-1	app-ca.central.arubanetworks.com	device-ca.central.arubanetworks.com	HTTPS TCP port 443	device-ca-h2.central.arubanetworks.com
China-1	app.central.arubanetworks.com.cn	device.central.arubanetworks.com.cn	HTTPS TCP port 443	device-h2.central.arubanetworks.com.cn
APAC-1	app2-ap.central.arubanetworks.com	app1-ap.central.arubanetworks.com	HTTPS TCP port 443	app1-ap-h2.central.arubanetworks.com
APAC-EAST1	app-apaceast.central.arubanetworks.com	device-apaceast.central.arubanetworks.com	HTTPS TCP port 443	device-apaceast-h2.central.arubanetworks.com
APAC-SOUTH1	app-apacsouth.central.arubanetworks.com	device-apacsouth.central.arubanetworks.com	HTTPS TCP port 443	device-apacsouth-h2.central.arubanetworks.com

Domain Names for AOS-CX Device Communication with Aruba Central

Table 32: *Domain Names for AOS-CX Device Communication with Aruba Central*

Region	Aruba Central URL	URL for Device Connectivity	Protocol
US-1	app.central.arubanetworks.com	device-prod-d2.central.arubanetworks.com	HTTPS TCP port 443
US-2	app-prod2.central.arubanetworks.com	device-prod2.central.arubanetworks.com	HTTPS TCP port 443
US-WEST-4	app-uswest4.central.arubanetworks.com	device-uswest4-d2.central.arubanetworks.com	HTTPS TCP port 443
EU-1	app2-eu.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443
EU-2	app-eucentral2.central.arubanetworks.com	device-eucentral2-d2.central.arubanetworks.com	HTTPS TCP port 443
EU-3	app-eucentral3.central.arubanetworks.com	device-eucentral3-d2.central.arubanetworks.com	HTTPS TCP port 443
Canada-1	app-ca.central.arubanetworks.com	device-ca.central.arubanetworks.com	HTTPS TCP port 443
China-1	app.central.arubanetworks.com.cn	device.central.arubanetworks.com.cn	HTTPS TCP port 443
APAC-1	app2-ap.central.arubanetworks.com	app1-ap.central.arubanetworks.com	HTTPS TCP port 443
APAC-EAST1	app-apaceast.central.arubanetworks.com	device-apaceast.central.arubanetworks.com	HTTPS TCP port 443
APAC-SOUTH1	app-apacsouth.central.arubanetworks.com	device-apacsouth.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with Aruba Activate

Table 33: *Domain Names for Device Communication with Aruba Activate*

Domain Name	Protocol
device.arubanetworks.com	HTTPS TCP port 443
devices-v2.arubanetworks.com	
est.arubanetworks.com *	

* Required for Aruba 2530 switches to provision certificate using the EST server in activate.

Cloud Guest Server Domains for Guest Access Service

Table 34: *Domain Names for Cloud Guest Server Access*

Region	Domain Name	Protocol
US-1	nae1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	nae1-elb.cloudguest.central.arubanetworks.com	TCP port 443
US-2	naw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	naw2-elb.cloudguest.central.arubanetworks.com	TCP port 443
US-WEST-4	uswest4.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	uswest4-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-1	euw1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	euw1-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-2	naw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	naw2-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-3	euw1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	euw1-elb.cloudguest.central.arubanetworks.com	TCP port 443
Canada-1	ca.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	ca-elb.cloudguest.central.arubanetworks.com	TCP port 443
APAC-1	ap1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443

Region	Domain Name	Protocol
	ap1-elb.cloudguest.central.arubanetworks.com	TCP port 443
APAC-EAST1	apaceast.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	apaceast-elb.cloudguest.central.arubanetworks.com	TCP port 443
APAC-SOUTH1	apacsouth.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	apacsouth-elb.cloudguest.central.arubanetworks.com	TCP port 443

Domain Names for OpenFlow

Table 35: *Domain Names for OpenFlow*

Region	Domain Name
US-1	https://app2-ofc.central.arubanetworks.com
US-2	https://ofc-prod2.central.arubanetworks.com
US-WEST-4	https://ofc-uswest4.central.arubanetworks.com
EU-1	https://app2-eu-ofc.central.arubanetworks.com
EU-2	https://ofc-eucentral2.central.arubanetworks.com
EU-3	https://ofc-eucentral3.central.arubanetworks.com
Canada-1	https://ofc-ca.central.arubanetworks.com
China-1	https://ofc.central.arubanetworks.com.cn
APAC-1	https://app2-ap-ofc.central.arubanetworks.com
APAC-EAST1	https://ofc-apaceast.central.arubanetworks.com
APAC-SOUTH1	https://ofc-apacsouth.central.arubanetworks.com

Other Domain Names

Table 36: *Other Domain Names*

Domain Name	Protocol	Description
sso.arubanetworks.com	TCP port 443	Allows users to access their accounts on the internal server.
internal.central.arubanetworks.com internal2.central.arubanetworks.com	TCP port 443	Allows users to access the Aruba Central Internal portal.
pool.ntp.org	UDP port 123	Allows users to update the internal clock and configure time zone when a factory default device comes up.

Domain Name	Protocol	Description
		By default, the Aruba devices contact **pool.ntp.org** and use NTP to synchronize their system clocks.
activate.arubanetworks.com	TCP port 443	Allows users to configure provisioning rules in Activate.
stun.pqm.arubanetworks.com	UDP or TCP port 3478 and 3479	Allows users to discover public IP over the WAN uplinks configured on devices.
pqm.arubanetworks.com	ICMP or UDP port 4500	Allows users to check the health of WAN uplinks configured on Branch Gateways.
images.arubanetworks.com	TCP port 80	Allows users to access the server that hosts software images available for upgrading devices.
http://h30326.www3.hpe.com	TCP port 80	Allows users to access the Aruba switch software images. To view the URL for software updates, use the **show activate software-update** command.
d2vxf1j0rhr3p0.cloudfront.net	TCP port 443	Allows users to access the CloudFront server for locating Instant AP software images.
rcs-m.central.arubanetworks.com (For all other regions) central-eu-rcs.central.arubanetworks.com (For Europe region)	TCP port 443	Allows users to access a device console through SSH.
cloud.arubanetworks.com	TCP port 80	Allows users to open the Aruba Central evaluation sign-up page.
aruba.brightcloud.com	TCP port 443	Enables devices to access the Webroot Brightcloud server for application, application categories, and website content classification.
bcap15-dualstack.brightcloud.com	TCP port 443	Allows Aruba devices to look up the Webroot Brightcloud server for Website categories.
api-dualstack.bcti.brightcloud.com	TCP port 443	Allows Aruba devices to access the IP Reputation and IP Geolocation service on the Webroot Brightcloud server.
database-dualstack.brightcloud.com	TCP port 443	Allows Aruba devices to download the website classification database from the Webroot Brightcloud server.

When configuring ACLs to allow traffic over a network firewall, use the domain names instead of the IP addresses.
For Branch Gateways to set up IPsec tunnel with the VPN concentrators, the UDP 4500 port must be open.

Connecting Instant APs to Aruba Central

To bring up Instant APs in Aruba Central, perform the following steps:

1. Connect the Instant AP to a provisioning network.
2. Ensure that Instant AP is operational and is connected to the Internet.
3. Ensure that the Instant AP has a valid DNS server address either through DHCP or static IP configuration.
4. Ensure that NTP server is running and Instant AP system clock is configured.

Connecting Aruba Switches to Aruba Central

Note the following points about automatic provisioning of switches:

- Pre-configured switches can now join Aruba Central. You can also import configuration from these switches to generate a template. For more information, see Creating a Configuration Template.
- If the switches ship with a version lower than the minimum supported firmware version, a factory reset may be required, so that the switch can initiate a connection to Aruba Central. For information, on the minimum firmware versions supported on the switches, see Supported AOS-Switch Platforms.
- During Zero Touch Provisioning, the Aruba switches can join Aruba Central only if they are running the factory default configuration, and have a valid IP address and DNS settings from a DHCP server.
- The provisioning of the Aruba Mobility Access Switch fails when the provisioning process is interrupted during the initial booting and if the switch has a static IP address with no DNS server configured.

Connecting SD-WAN Gateways to Aruba Central

The Aruba gateways have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The gateways also support multiple active uplinks for ZTP (also referred to as automatic provisioning). The supported ZTP ports for different hardware platforms are listed in the following table. All these ZTP ports are assigned to VLAN 4094.

Table 37: *ArubaOS Hardware Platforms and Supported ZTP Ports*

ArubaOS Hardware Platform	Supported ZTP Ports
Aruba 7005 Gateway	ALL ports except 0/0/1
Aruba 7008 Gateway	ALL ports except 0/0/1
Aruba 7010 Gateway	ALL ports except 0/0/1
Aruba 7030 Gateway	ALL ports except 0/0/1
Aruba 7024 Gateway	ALL ports except 0/0/1
Aruba 7210 Gateway	ALL ports except 0/0/1
Aruba 7220 Gateway	ALL ports except 0/0/1
Aruba 7240 Gateway	ALL ports except 0/0/1
Aruba 7280 Gateway	ALL ports except 0/0/1
Aruba 9004 Gateway	ALL ports except 0/0/1

Table 37: *ArubaOS Hardware Platforms and Supported ZTP Ports*

ArubaOS Hardware Platform	Supported ZTP Ports
Aruba 9004-LTE Gateway	ALL ports except 0/0/1
Aruba 9012 Gateway	ALL ports except 0/0/1

To know the minimum software version required for the gateways, see Supported SD-Branch Components.

To automatically provision the gateways:

1. Connect your gateway to the provisioning network.
2. Wait for the device to obtain an IP address through DHCP. Gateways support multiple uplink ports. The first port to receive the DHCP IP connects to the Activate server and completes the provisioning procedure:
   - If the device has factory default configuration, it receives an IP address through DHCP, connects to Aruba Activate, and downloads the provisioning parameters. When a device identifies Aruba Central as its management entity, it automatically connects to Aruba Central.
   - If the device is running a software version that does not have the SD-WAN image, the devices are automatically upgraded to a supported SD-WAN software version.

Aruba 72xx gateways with the ArubaOS 8.3.0.9 factory default image use only port 0/0/1 (the last copper port) for ZTP. When the factory default gateways connect to Activate through ZTP for the first time, Activate recommends a base SD-WAN image, which the gateways will download. In the SD-WAN image, port 0/0/1 is used as a debug port, and DHCP requests will not be sent out of port 0/0/1 for subsequent ZTP requests. Hence, ZTP workflow for Aruba 72xx gateways with the ArubaOS 8.3.0.9 factory default image will not work. You must manually upgrade the Aruba 72xx gateways to the SD-WAN image or use other methods like full-setup and static-activate to provision the gateways.

3. Observe the LED indicators. Table 2 describes the LED behavior.

Table 38: *LED Indicators*

LED Indicator	LCD Text	Description
Solid Amber	Getting DHCP IP	Indicates that the uplink connection is UP, but DHCP IP is yet to be retrieved.
Blinking Amber	Activate Wait	Indicates that the device was able to reach the DHCP server and the connection to the Activate server is yet to be established.
Solid Green	Activate OK	Indicates that the device was able to retrieve provisioning parameters from the Activate server.
Alternating Solid Green and Amber	Activate Error	Indicates that the device was not able to retrieve provisioning parameters.

After successfully connecting to Aruba Central, the gateways download the configuration from Aruba Central.

- From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch Gateways no longer require additional reboot when they receive the controller IP from Aruba Central after the ZTP process. Some services are restarted, resulting in an expected network impact, but the gateways do not reload for the second time. However, the gateways will reboot if there are any subsequent controller IP changes.
- The gateways also include service ports that the technicians can use for manually provisioning devices in the event of ZTP failure. For more information on ports available for Aruba 7000 Series Mobility Controllers and Aruba 7200 Series Mobility Controllers, see *ArubaOS User Guide*.

Device Configuration and Network Management

Aruba Central supports provisioning, managing, monitoring, and troubleshooting workflows for the following types of Aruba devices:

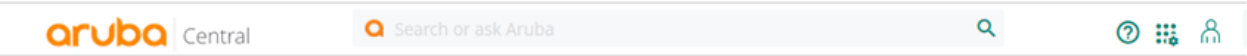
- Instant APs—Know more about Instant AP, supported hardware platforms and software versions and learn how to manage your WLAN deployments with Instant APs. For more information, see Instant APs.
- Switches—Know more about Aruba switches, supported hardware platforms and software versions, and learn how to manage wired access using switches. For more information, see AOS-Switches Overview.
- Gateways—Know more about SD-WAN Gateways, supported hardware platforms and software versions, and learn how to build and manage SD-WAN deployments. For more information, see Aruba SD-Branch Solution.
- Virtual Gateways—Deploy, connect, and manage Virtual Gateways hosted on customer VPC from Aruba Central. For more information, see Deploying Aruba Virtual Gateways.

Using the Search Bar

The search bar in the **Network Operations** app enables users to search for clients, devices, and infrastructure connected to the network. The search also retrieves relevant documentation to help users efficiently operate their networks. The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant search results.

The following figure illustrates the search bar option in Aruba Central.

Figure 19 *Search Bar*



To start a search in the Aruba Central UI, click the search bar or press **/** (forward slash) on your computer keyboard.

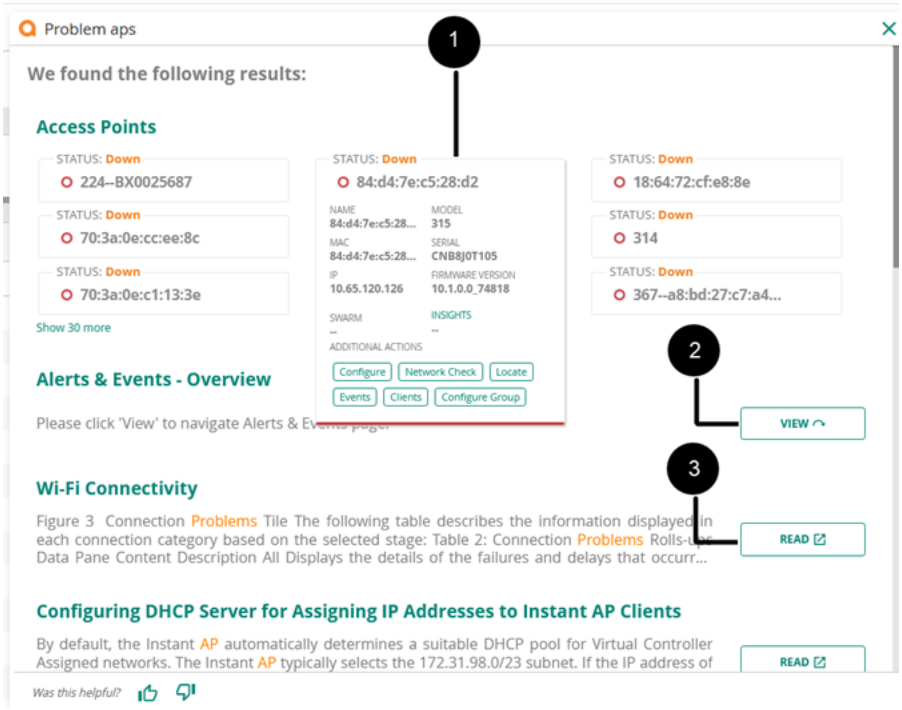
When you click the search bar, you can see the search suggestions in the **Recent** and **Suggested Search** list.

Recent—Shows the searches performed recently in the search bar. These suggestions help you quickly look at the previous searches.

Suggested Search—Shows search suggestions corresponding to the workflow that you follow in the **Network Operations** app. The suggested search help you perform onboarding, monitoring, configuring, and troubleshooting tasks. For more information, see the Suggested Search page.

The following figure illustrates the sample search result in Aruba Central.

Figure 20 *Sample Search Result*



From the search results, you can navigate to:

1. **Search Cards**—displays monitoring summary and links to configuration, monitoring, and troubleshooting pages in the **Network Operations** app.
2. **View**—relevant links to the corresponding pages in the **Network Operations** app.
3. **Read**—relevant links to the help pages in the Aruba Central Help Center.

Suggested Search

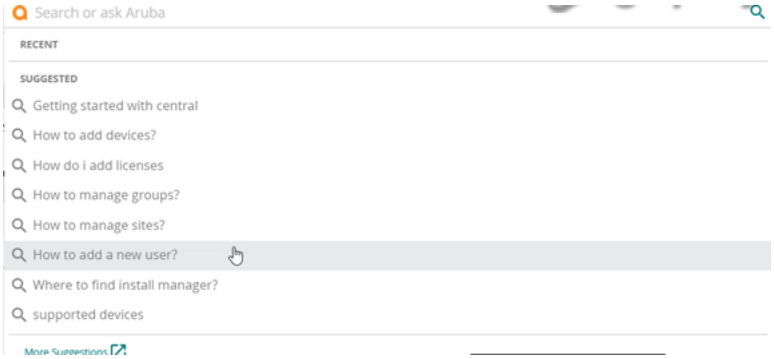
The search bar displays search suggestions corresponding to the workflow that you follow as a user of the platform. The suggestions help you perform on-boarding tasks and bring up the devices in the network, configure and troubleshoot the network issues.

The following are some of the sample queries to get you started on the on-boarding journey. These sample queries in the **Network Operations** app search bar can guide you into getting started with Central, adding devices, assigning licenses to devices, creating groups and sites, and so on:

- Getting started with Central
- How to add devices
- How do I add licenses
- How to create groups
- How to create sites
- How to add device to a site
- How to add a new user
- Where to find install manager
- Install manager issues

The following figure illustrates search suggestions to get started with Aruba Central.

Figure 21 *Suggestions to Get Started with Aruba Central*

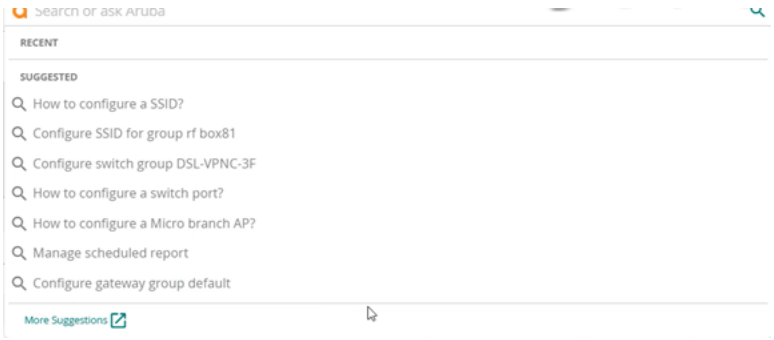


The following sample queries in the Network Operations app search bar can guide you to create SSIDs, configure a switch group, configure a gateway and so on:

- How to configure an SSID
- Configure SSID for group <Group Name> (Detect an AP group without SSID configuration)
- How to configure a switch group
- Configure switch group <Group Name>
- How to configure a switch port
- How to configure a Micro branch AP
- Configure Micro branch group <Name>
- How to configure a gateway.
- Configure gateway group <Group Name>

The following figure illustrates search suggestions for the next actions to perform in Aruba Central based on the workflow that you follow in the **Network Operations** app.

Figure 22 *Suggestions to Get Started with Aruba Central*



Client Search Terms

The search bar helps you to search a client's information, navigate to the configuration and troubleshooting pages of the client in the **Network Operation** app.

The sample search terms in this page help you with the list of terms for troubleshooting the client issues in the **Network Operations** app.

Using the search bar you can perform the following tasks:

- Hover over a client search card to view more details and links to the monitoring, configuration, and troubleshooting pages.

- Click the client name to open the **Client Details** page.
- Click **View** to open the corresponding page in Aruba Central. For example, clicking the **View** button corresponding to **High DHCP Failures** opens the **AI Insights** dashboard.
- Click **Read** to navigate to the documentation page in the Aruba Central Help Center relevant to the search terms.

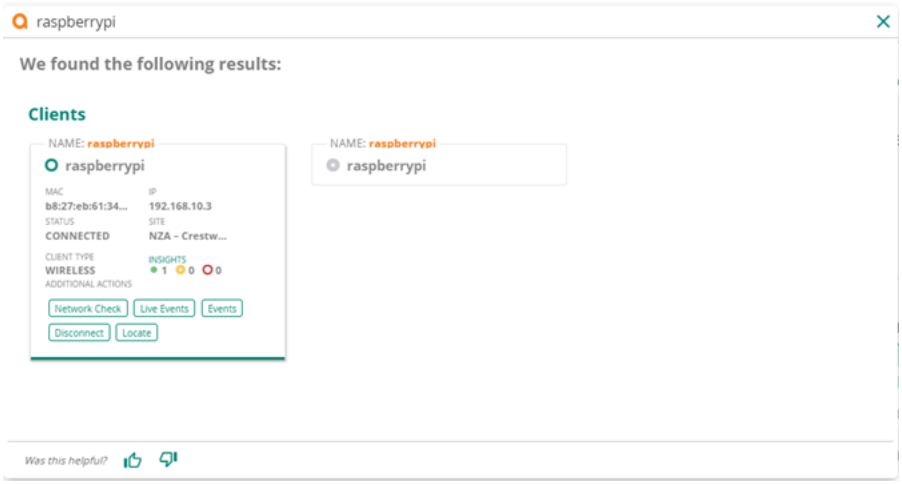
Search Cards for Clients

The search results in Aruba Central displays certain cards with monitoring information and links to the configuration and troubleshooting pages for the client. You can click the links to navigate to that particular page of the client in the **Network Operations** app.

You can see the search cards when you search with the client name, IP address, or MAC address.

Following is an example of the search card that appears when you search with a client name:

Figure 23 *Search Card for Client Name Search*

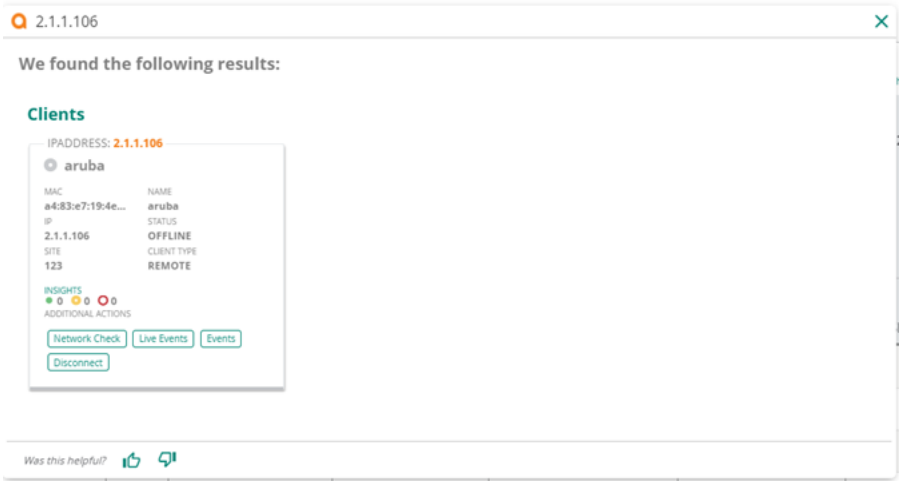


Options available on the client's search card:

- **Network Check**—Opens the **Network Check** page for the client.
- **Live Events**—Opens the **Live Troubleshooting** page for the client.
- **Events**—Opens the **Alerts & Events** page for the client.
- **Disconnect**—Opens the **Client Details** page to disconnect the client.
- **Insights**—Opens the **AI Insights** page for the client.

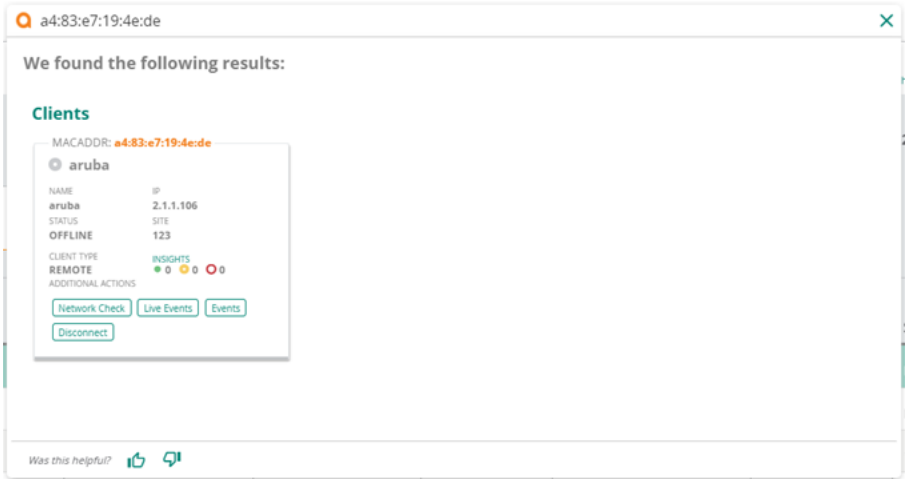
Following is an example of the search card that appears when you search with a client IP address:

Figure 24 *Search Card for Client IP Address Search*



Following is an example of the search card that appears when you search with a client MAC address:

Figure 25 *Search Card_Client MAC Address*



Sample Search Terms for a Client

The following table lists the sample search terms for a client.

Table 39: *Client Search Terms*

Typical Queries	Search Terms	Result
View client(s) facing issues in the network	**client issues** **client anomalies** **problem clients**	Returns client(s) that failed to connect and client(s) experiencing issues such as high DHCP failures, authentication failures, high roaming latency, and so on.
View failed client (s)	**client failures** **failed clients**	Returns client(s) that failed to connect to the network.

Table 39: *Client Search Terms*

Typical Queries	Search Terms	Result
View client(s) running Windows operation system	**list windows clients**	Returns a list of the client(s) running Windows operation system.
View client(s) running Android operation system	**list android clients**	Returns a list of the client(s) running Android operation system.
View client(s) in a site	Enter **list clients in site** followed by the site name. Example—**list clients in site***California*	Returns a list of all client(s) in the site.
View offline client (s) in a site	Enter **show offline clients in site** followed by the site name. Example—**show offline clients in site** *California*	Returns a list of offline client(s) in the site.
View connected client(s) in a particular site	Enter **show connected clients in site** followed by the site name. Example—**show connected clients in site** *California*	Returns a list of the connected client(s) in the site.
Search by client name	Enter the name of the client. Example—*myipad*	Returns the client whose name matches the search term.
Search by client MAC address	Enter **client** followed by the MAC address. Example—**client***00:01:00:10:9f:20*	Returns the client whose MAC address matches the search term.

User Experience Search Terms

The following table provides a list of recommended search terms with the corresponding search results. These sample search terms can help you in gauging the network performance and identifying anomalies affecting user experience in the **Network Operations** app.

Table 40: *User Experience Search Terms*

Search Terms	Result
user experience issues	Returns the following links: ▪ Client-related insights generated for the last three hours ▪ **Network Health** dashboard Click **View** to open the corresponding page.

Table 40: *User Experience Search Terms*

Search Terms	Result
user experience issues last month	Returns client-related insights generated for the last one month.
client issues last week	Returns the following: ■ Client(s) that failed to connect to the network in the last one week ■ Client-related insights generated for the last one week
how is my network today	Returns the following links: ■ **Wi-Fi Connectivity** dashboard ■ **Network Health** > **List** page Click **View** to open the corresponding page.
is everything ok	Returns a link to the **AI Insights** dashboard. Click **View** to open the **AI Insights** dashboard and review the insights triggered.
roaming issues	Returns links to the following insights: ■ Clients who Roamed Excessively ■ Clients with High Roaming Latency Click **View** to open the corresponding insight and identify roaming anomalies.
authentication issues	Returns links to the following insights: ■ Clients with High 802.1X Authentication Failures ■ Clients with High MAC Authentication Failures Click **View** to open the corresponding insight and identify authentication anomalies.
problem clients	Returns client(s) that failed to connect and client(s) experiencing issues such as high DHCP failures, authentication failures, high roaming latency, and so on.
coverage issues	Returns links to the following insights: ■ Clients with Low SNR Minutes ■ Coverage Holes Identified Click **View** to open the corresponding insight and identify coverage anomalies.

Device Search Terms

The search bar helps you to search all devices monitored by Aruba Central. The search enables you to navigate to the monitoring, configuration, and troubleshooting pages of the devices in the **Network Operation** app.

The sample search terms in this page help you with the list of terms for troubleshooting the devices issues in the **Network Operations** app.

Using the search bar you can perform the following tasks:

- Hover over a device search card to view more details and links to the monitoring, configuration, and troubleshooting pages.
- Click the device name to open the corresponding **Device Details** page.
- Click **View** to open the corresponding page in Aruba Central. For example, clicking the **View** button corresponding to **Alerts & Events Overview** opens the **Alerts & Events** page.
- Click **Read** to navigate to the documentation page in the Aruba Central Help Center relevant to the search terms.

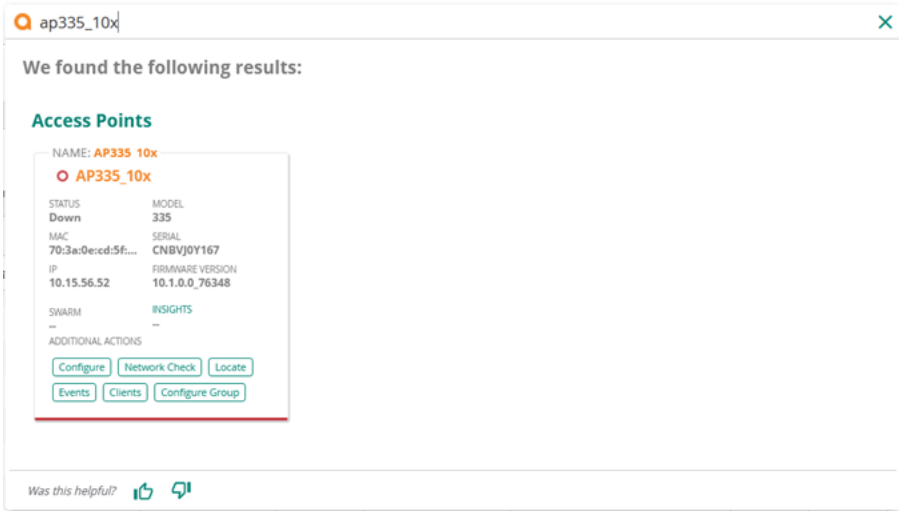
Search Cards for Devices

The search results in Aruba Central displays certain cards with monitoring information and links to the configuration and troubleshooting pages for the device. You can click the links to navigate to that particular page of the device in the **Network Operations** app.

You can see the search cards when you search with the device name, IP address, MAC address, group, site, or label name. Following are the examples for APs, switches, and gateways.

Following is an example of the search card that appears when you search with an Access Point name:

Figure 26 *Search Card for the Access Point Name Search*

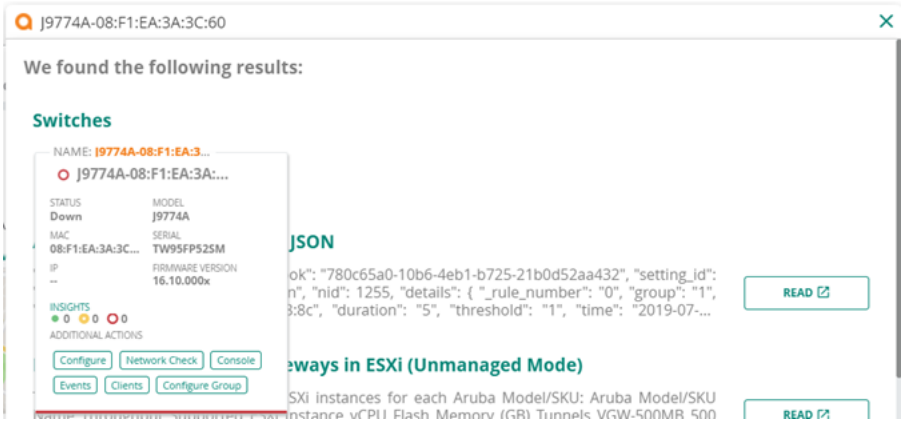


Options available on the AP name search card:

- **Configure**—Opens the **AP Configuration** page.
- **Network Check**—Opens the **Network Check** page.
- **Locate**—Locates the AP in the network.
- **Events**—Opens the **Alerts & Events** page for the AP.
- **Clients**—Opens the **Clients** page for the AP.
- **Configure Group**—Opens the **Access Points** page to configure a group for the AP.
- **Insights**—Opens the **AI Insights** page for the AP.

Following is an example of the search card that appears when you search with a Switch name:

Figure 27 *Search Card for the Switch Name Search*

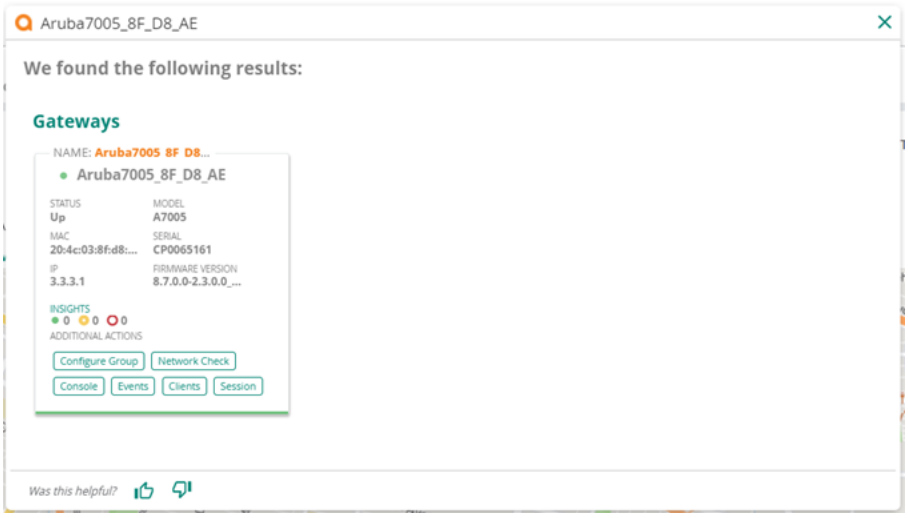


Options available on the switch name search card:

- **Configure**—Opens the **Switch Configuration** page.
- **Network Check**—Opens the **Network Check** page for the switch.
- **Console**—Opens the Switch Details page.
- **Events**—Opens the **Alerts & Events** page for the switch.
- **Clients**—Opens the **Clients** page for the AP.
- **Configure Group**—Opens the **Switches** page to configure a group for the switch.
- **Insights**—Opens the **AI Insights** page for the switch.

The following is an example of the search card that appears when you search with a gateway name:

Figure 28 *Search Card for the Gateway Name Search*



Options available on the gateway name search card:

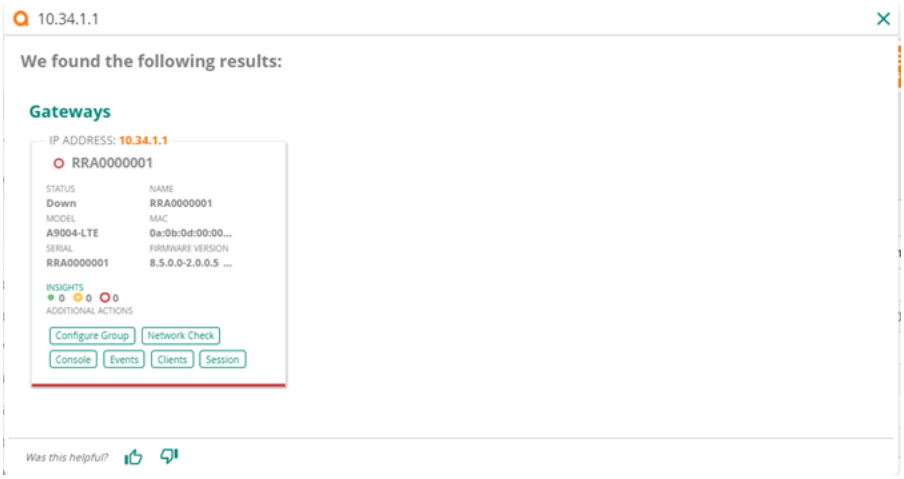
- **Configure Group**—Opens the **Gateways** page to configure a group for the gateway.
- **Network Check**—Opens the **Network Check** page for the gateway.
- **Console**—Opens the **Gateway Summary** page for the gateway.
- **Events**—Opens the **Alerts & Events** page for the gateway.
- **Clients**—Opens the **Clients** page for the gateway.
- **Session**—Opens the **Sessions** page for the gateway.

The following is an example of the search card that appears when you search with a device serial:

Figure 29 *Search Card for the Device Serial Search*

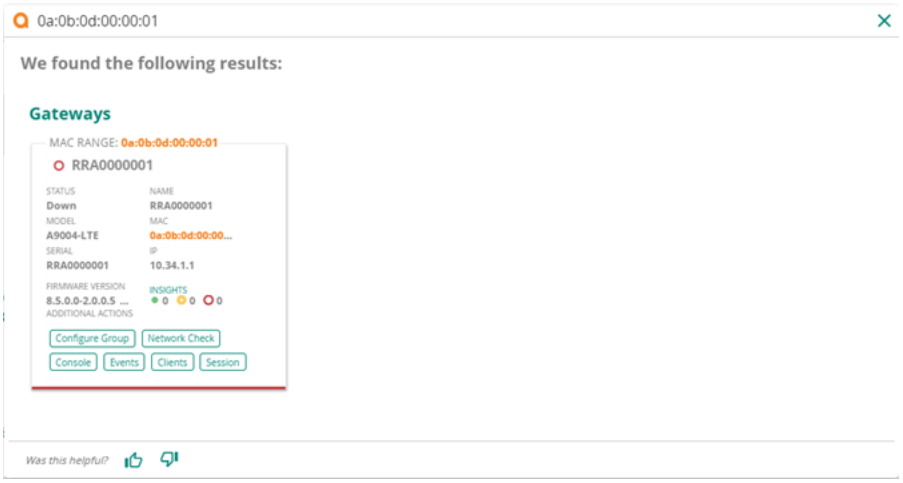
The following is an example of the search card that appears when you search with a device IP address:

Figure 30 *Search Card for the Device IP Address Search*



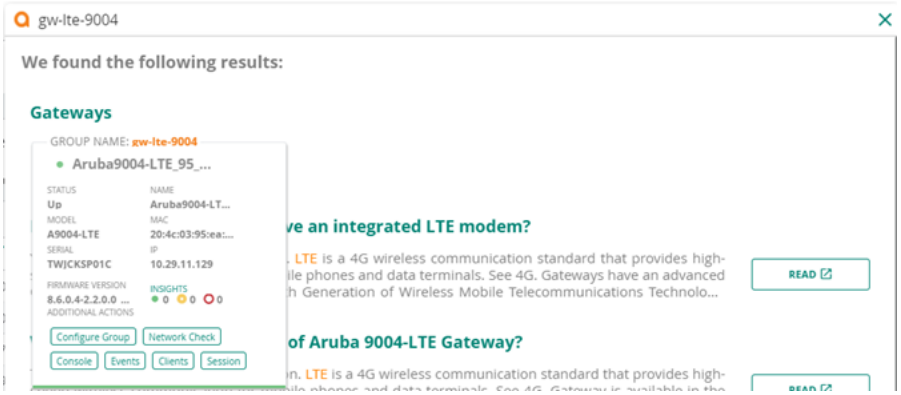
The following is an example of the search card that appears when you search with a device MAC address:

Figure 31 *Search Card for the Device MAC Address Search*



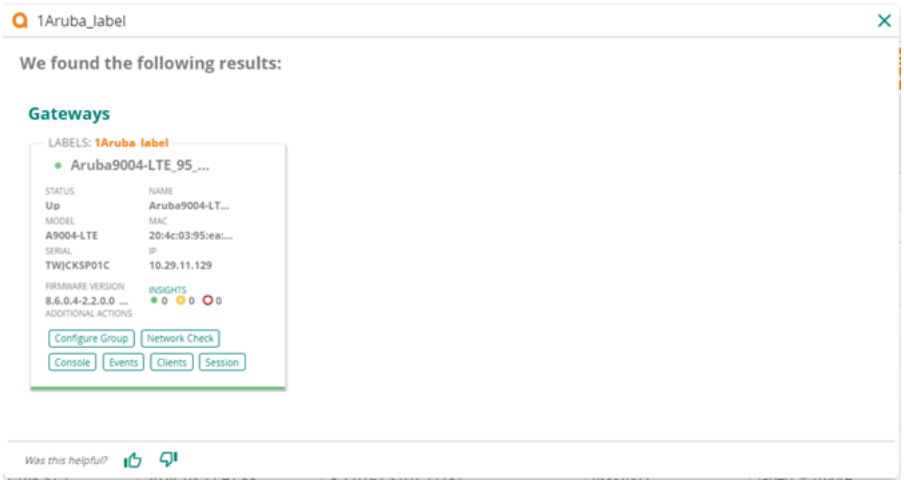
The following is an example of the search card that appears when you search with a device group name:

Figure 32 *Search Card for the Device Group Name Search*



The following is an example of the search card that appears when you search with a device label:

Figure 33 *Search Card for the Label Search*



Sample Device Search Terms

The following table lists the search terms for AP, switch, and gateway.

Table 41: *Device Search Terms*

Typical Queries	Search Terms	Result
Access Point		
View AP(s) facing issues in the network	**AP issues** **AP anomalies** **problem APs**	Returns a list of the AP(s) that are offline, AP radios changing channels more frequently, AP (s) experiencing higher than normal channel utilization, AP(s) experiencing frequent transmit power changes, and AP(s) that missed sending telemetry data, and so on.
View AP(s) in a site	Enter **list aps in site** or **show aps in site** followed by the site name. Example—**list aps in site** *California*	Returns a list of the AP(s) in the site.

Table 41: *Device Search Terms*

Typical Queries	Search Terms	Result
View a list of online AP(s)	**online aps**	Returns a list of the AP(s) that are online.
View AP(s) belonging to a group	Enter **list aps in group** followed by group name. Example—**list aps in group***default*	Returns a list of the AP(s) that are belonging to the group.
View AP(s) tagged with a particular label	Enter **list aps in label** followed by the label name. Example—**list aps in label***lobby*	Returns a list of the AP(s) that are tagged with the label.
View AP(s) by model number	Enter **show ap model** followed by the model number. Example—**show ap model***ap-105*	Returns a list of the AP(s) whose model number matches the search term.
Search by AP name	Enter the name of the AP. Example—*printer-room*	Returns the AP whose name matches the search term.
Search by AP MAC address	Enter **ap** followed by the MAC address. Example—**ap** *94:b4:0f:d9:ba:cc*	Returns the AP whose MAC address matches the search term.
Search by AP serial number	Enter **ap serial** followed by the serial number. Example—**ap serial***CNJJKPN1G5*	Returns the AP whose serial number matches the search term.
Switch		
View switch(es) facing issues in the network	**switch issues** **switch anomalies** **problem switches**	Returns a list of switch(es) that are offline, switch(es) experiencing high CPU and memory utilization, switch(es) facing PoE issues, and so on.
View switch(es) in a site	Enter **list switches in site** or **show switches in site** followed by the site name. Example—**list switches in site** *California*	Returns a list of switch(es) in the site.
View a list of online switch(es)	**online switches**	Returns a list of switch(es) that are online.
View switch(es) belonging to a group	Enter **list switches in group** followed by group name. Example—**list switches in group***default*	Returns a list of switch(es) belonging to the group.

Table 41: *Device Search Terms*

Typical Queries	Search Terms	Result
View switch(es) tagged with a label	Enter **list switches in label** followed by the label name. Example—**list switches in label***store*	Returns a list of switch(es) that are tagged with the label.
Search by switch name	Enter the name of the switch. Example—*store-switch*	Returns the switch whose name matches the search term.
Search by switch MAC address	Enter **switches** followed by the MAC address. Example—**switch** *f8:60:f0:b6:22:00*	Returns the switch whose MAC address matches the search term.
Search by switch serial number	Enter **switch serial** followed by the serial number. Example—**switch serial***CN90HKX045*	Returns the switch whose serial number matches the search term.
Gateway		
View gateway(s) facing issues in the network	**gateway issues** **gateway anomalies** **problem gateways**	Returns a list of gateway(s) that are down, gateway(s) experiencing high CPU and memory utilization, gateway tunnel(s) that are down, and so on.
View gateway(s) in a site	Enter **list gateways in site** or **show gateways in site** followed by the site name. Example—**list gateways in site** *California*	Returns a list of gateway(s) in the site.
Configure gateway(s) in a particular group	Enter **configure gateways in group** followed by the site name. Example—**configure gateways in group***default*	Returns a link to the gateway configuration page.
View a list of online gateway(s)	**online gateways**	Returns a list of gateway(s) that are online.
View gateway(s) belonging to a group	Enter **list gateways in group** followed by group name. Example—**list gateways in group***default*	Returns a list of gateway(s) belonging to the group.
View gateway(s) tagged with a label	Enter **list gateways in label** followed by the label name.	Returns a list of gateway(s) that are tagged with the label.

Table 41: *Device Search Terms*

Typical Queries	Search Terms	Result
	Example—**list gateways in label***lobby*	
Search by gateway name	Enter the name of the gateway. Example—*branch*	Returns the gateway whose name matches the search term.
Search by gateway MAC address	Enter **gateway** followed by the MAC address. Example—**gateway** *00:0b:86:f9:0d:d2*	Returns the gateway whose MAC address matches the search term.
Search by gateway serial number	Enter **gateway serial** followed by the serial number. Example—**gateway serial***CZ0003248*	Returns the gateway whose serial number matches the search term.

Network & Services Search Terms

The following table provides a list of recommended search terms with the corresponding search results for network and services.

Table 42: *Network & Services Search Terms*

Search Terms	Result
service issues	Returns the following links: ▪ **Wi-Fi Connectivity** dashboard ▪ **AI Insights** dashboard Click **View** to open the corresponding page.
dhcp issues	Returns a link to the Clients with DHCP Server Connection Problems insight. Click **View** to open the insight and identify the DHCP failures impacting the network.
dns issues	Returns links to the following insights: ▪ DNS Queries Failed to Reach or Return from the Server ▪ Delayed DNS Request or Response ▪ DNS Servers Rejected High Number of Queries Click **View** to open the corresponding insight and identify DNS anomalies.
authentication issues	Returns links to the following insights: ▪ Clients with High 802.1X Authentication Failures ▪ Clients with High MAC Authentication Failures Click **View** to open the corresponding insight and identify authentication anomalies.

Site Search Terms

The search bar helps you to search all sites monitored by Aruba Central.

The sample search terms in this page help you with the list of terms for troubleshooting the site issues in the **Network Operations** app.

Using the search bar you can perform the following tasks for a site:

- Hover over a site search card to view more details and links to the monitoring and troubleshooting pages.
- Click the site name to open the **Site Health** page.
- Click **View** to open the corresponding page in Aruba Central. For example, clicking the **View** button corresponding to **Site Issues** opens the **AI Insights** dashboard.

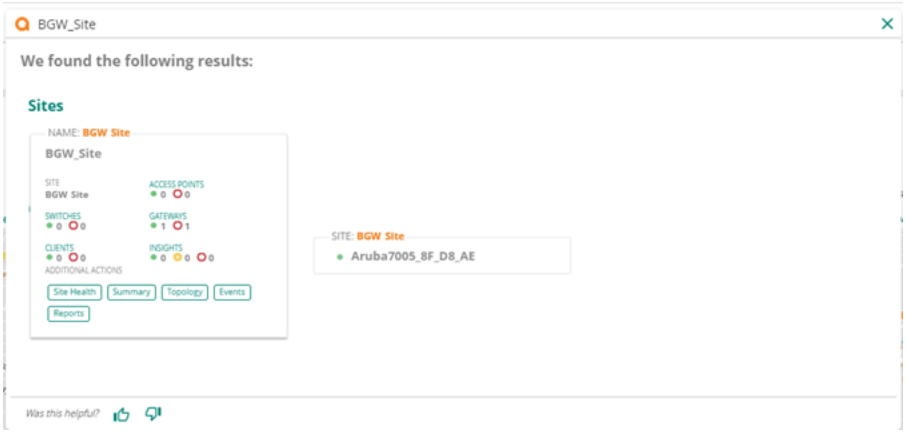
Search Cards for Sites

The search results in Aruba Central displays certain cards with monitoring information and links to the troubleshooting pages for the site. You can click the links to navigate to that particular page of the site in the **Network Operations** app.

You can see the search cards when you search with the site name.

Following is an example of the search card that appears when you search with a site name:

Figure 34 *Search Card for a Site Name Search*



Options available on the site search card:

- **Site Health**—Opens the **Site Health** page.
- **Summary**—Opens the **Summary** page for the site.
- **Topology**—Opens the **Topology** page for the site.
- **Events**—Opens the **Alerts & Events** page for the site.
- **Reports**—Opens the **Reports** page for the site.

The following table lists the search terms for a site.

Table 43: *Site Search Terms*

Typical Queries	Search Terms	Result
View problems in a site	Enter **any problems in site** followed by the site name. Example—**any problems in site** *California*	Returns the link to navigate to the **AI Insights** dashboard for the site.

Table 43: *Site Search Terms*

Typical Queries	Search Terms	Result
View client(s) in a site	Enter **list clients in site** followed by the site name. Example—**list clients in site** *California*	Returns a list of all client(s) in the site.
View offline client (s) in a site	Enter **show offline clients in site** followed by the site name. Example—**show offline clients in site** *California*	Returns a list of offline client(s) in the site.
View connected client(s) in a site	Enter **show connected clients in site** followed by the site name. Example—**show connected clients in site** *California*	Returns a list of connected client(s) in the site.
View AP(s) in a site	Enter **list aps in site** or **show aps in site** followed by the site name. Example—**list aps in site** *California*	Returns a list of AP(s) in the site.
View switch(es) in a site	Enter **list switches in site** or **show switches in site** followed by the site name. Example—**list switches in site** *California*	Returns a list of switch(es) in the site.
View gateway(s) in a site	Enter **list gateways in site** or **show gateways in site** followed by the site name. Example—**list gateways in site** *California*	Returns a list of gateway(s) in the site.
View alerts at a specific site	Enter **list gateways in site** or **show gateways in site** followed by the site name. Example—**list gateways in site** *California*	Returns a list of gateway(s) in the site.

Navigation Search Terms

The following table provides a list of recommended search terms with the corresponding search results. These sample search terms can help you navigate through Aruba Central. Based on the displayed results, click **View** to open the corresponding page in Aruba Central.

Table 44: *Navigation Search Terms*

Search Terms	UI Page
network health	**Network Health** > **List**
access points usage statistics **ap device summary**	**Devices > Access Points > Summary**
list alerts	**Global > Alerts & Events > Summary**
client overview	**Clients** > **Summary**
bandwidth usage	**Global > Overview** > **Summary**

Table 44: *Navigation Search Terms*

Search Terms	UI Page
configure ssid	Group > Devices > Access Points > Config > WLANs > Wireless SSIDs
configure vpn	Group > Devices > Access Points > Config > VPN
assign virtual controller config ap ports	Group > Devices > Access Points > Interfaces > Wired
radios profile	Group > Devices > Access Points > Config > Radios
manage firmware for virtual controller	Global > Firmware > Access Points
where can I configure switch	Devices > Switches > Config
configure switch stacks	Devices > Switches > Stacks > Config
enable cdp for switches	Devices > Switches > System > CDP
configuration conflicts for switches	Devices > Switches > Configuration Audit
switch dhcp pools	Devices > Switches > IP Settings > DHCP Pools
switch security dhcp	Devices > Switches > Security > DHCP Snooping
how to configure switch igmp	Devices > Switches > IGMP
switch port priority	Devices > Switches > Interface > PoE
manage switch ports	Devices > Switches > Interface > Ports
configure VLANs	Devices > Switches > Interface > VLANs
configure gateways	Devices > Gateways > Config
config audit gateway	Devices > Gateways > Config > Advanced Mode > Config Audit
wan transport health	Devices > Gateways > Summary
wan performance	Global > Overview > WAN Health > List
show branch uplinks utilization	Global > Overview > WAN Health > Summary
virtual gateway settings	Global > Network Services > Virtual Gateways
how to upgrade gateway	Global > Firmware > Gateways
overlay route orchestrator topology	Global > Network Services > SD-WAN Overlay > Route
topology	Site > Overview > Topology
list all saas apps saas express summary	Global > Applications > SaaS Express > Map

Table 44: *Navigation Search Terms*

Search Terms	UI Page
ssh threats	Global > Security > Gateway IDS/IPS > Threats List
current threat map	Global > Security > Gateway IDS/IPS > Summary
configure presence analytics	Global > Guests > Presence Analytics > Config
view wifi connected devices	Global > Guests > Presence Analytics > Summary
setup guest access	Global > Guests > Guest Access
setup guest network	Group > Guests > Config > Guest Networks
ucc settings enable call prioritization for ucc	Global > Applications > UCC > Config > Settings
list ucc call	Global > Applications > UCC > List
tutorials	WalkMe Menu for launching guided tutorials

Aruba Central is a cloud-native network operations and assurance solution for wired, wireless, and SD-WAN networks. Aruba Central unifies traditional management with AI-based network and user insights, and IoT device profiling in a single interface for simplified and secure management and control.

Apps

From the **Account Home** page, you can manage network inventory, subscriptions, and user access. You can provision or launch the following apps:

- **Network Operations**
- **ClearPass Device Insight**

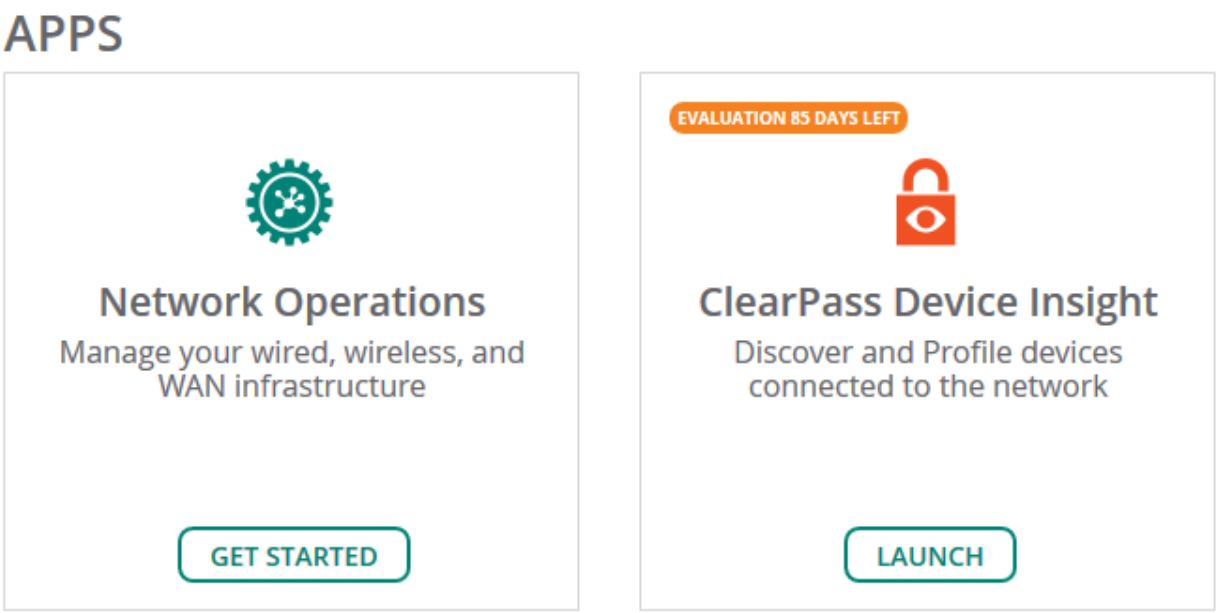
The application(s) displayed in the **Apps** section of the page are dependent on the app(s) that you selected while signing up for Aruba Central.

For more information, see Creating an Aruba Central Account.

To provision an app, click **Get Started**. After the app is provisioned, click **Launch** to navigate to the corresponding application UI.

If the app provisioning fails, you can retry or contact Aruba Technical Support.

Figure 35 *All Apps*



Network Operations

Network Operations is a unified network operations, assurance and security platform that simplifies the deployment, management, and service assurance of wireless, wired and SD-WAN environments. Network Operations provides a cloud-based network management platform for managing your wireless, WAN, and

wired networks with Aruba APs, Gateways, and Switches. Along with device and network management functions, the app also offers value-added services such as customized guest access, client presence, and service assurance analytics.

For more information, see Aruba Central Help Center.

ClearPass Device Insight

ClearPass Device Insight enables network and security administrators to discover, monitor, and automatically classify new and existing devices that connect to a network. You can identify devices that include IoT devices, medical devices, printers, smart devices, laptops, VoIP phones, computers, gaming consoles, routers, servers, and switches.

For more information, see Aruba ClearPass Device Insight Information Center.

Global Settings

In Aruba Central, most of the general administration tasks are grouped under **Global Settings**. The following table lists all the options and relevant app(s) to which the option is applicable:

Table 45: *Options & Apps*

Option	App(s)
User and Roles	■ **Network Operations** ■ **ClearPass Device Insight**
Key Management	■ **Network Operations** ■ **ClearPass Device Insight**
Device Inventory	**Network Operations**
License Assignment	**Network Operations**
Data Collectors	**Data Collectors** option appears only if the **ClearPass Device Insight** app is provisioned.
Audit Trail	**Network Operations**
Single Sign On	**Network Operations**
API Gateway	**API Gateway** option appears only if the **Network Operations** app is provisioned and if the API Gateway license is enabled.
Webhooks	**Network Operations**

Users and Roles

Aruba Central users are broadly categorized as follows:

- Network Administrators—Network administrators manage, configure, and monitor devices in their respective network or organization using the Aruba Central Standard Enterprise interface.
- Service Provider Administrators—Service Provider administrators are referred to as the MSP administrators who create, manage, and monitor accounts for multiple organizations (tenants). For MSP

accounts, the Network Operations app provides a separate interface called the MSP View, using which MSP administrators can provision and manage their respective tenant accounts. Tenant account users' access is limited to their respective account or network setup. For more information on creating tenant accounts, see the *Aruba Central MSP User Guide*.

Within each Aruba Central account, the admin users of the respective accounts can configure and manage the following types of users:

- System users—Users who authenticate to the Aruba SSO server (public cloud deployments) or LocalDB servers (private cloud deployments). System users can access both the UI and API interface with their Aruba Central login credentials. Access for the system users is determined by the role to which they are mapped. For more information on configuring system users, see Configuring System Users.
- External users—Users who log in to Aruba Central using an external authentication source. External user accounts are maintained by IT administrators of the respective organizations. External users are also referred to as federated users. To provide a secure and seamless sign-on experience for external users, Aruba Central supports a federation configuration module based on the SAML SSO framework. For more information on configuring the SAML SSO framework for federated users, see the Aruba Central SAML SSO Solution Guide.

The following table lists the tasks that you can perform from the **Users and Roles** page:

Table 46: *Users and Roles—Tasks*

Task	For more information...
Create, modify, or delete users	Configuring System Users
Create, modify, or delete user roles	Configuring User Roles
Resend email invitation to users	Resend Email Invite
Enable Two-Factor Authentication (2FA)	Two-Factor Authentication
Enable support access to debug issues	Support Access

Configuring System Users

In the **Account Home** page, the **Users and Roles** option under **Global Settings** allows you to create, modify, and delete users.

This section describes the procedure for configuring users in an enterprise account. For information on how to configure system users in the MSP mode, see the *Aruba Central Managed Service Provider User Guide*.

Adding a System User

To add a user, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
   The **Users and Roles** page is displayed.
2. Click **Add User**.
   The **New User** window is displayed.

3. Configure the following parameters:
   - **Username**—Email ID of the user. Enter a valid email address.
   - **Description**—Description of the user role. You can enter up to a maximum of 32 characters including alphabets, numbers, and special characters in the text field.
   - **Language**—Select a language. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
   - **Account Home**—Select a user role for the **Account Home** page. If there are common modules between **Account Home** and other app(s), the **Account Home** user role has higher precedence. For example, the **Devices and Subscription** module in the **Network Operations** app.

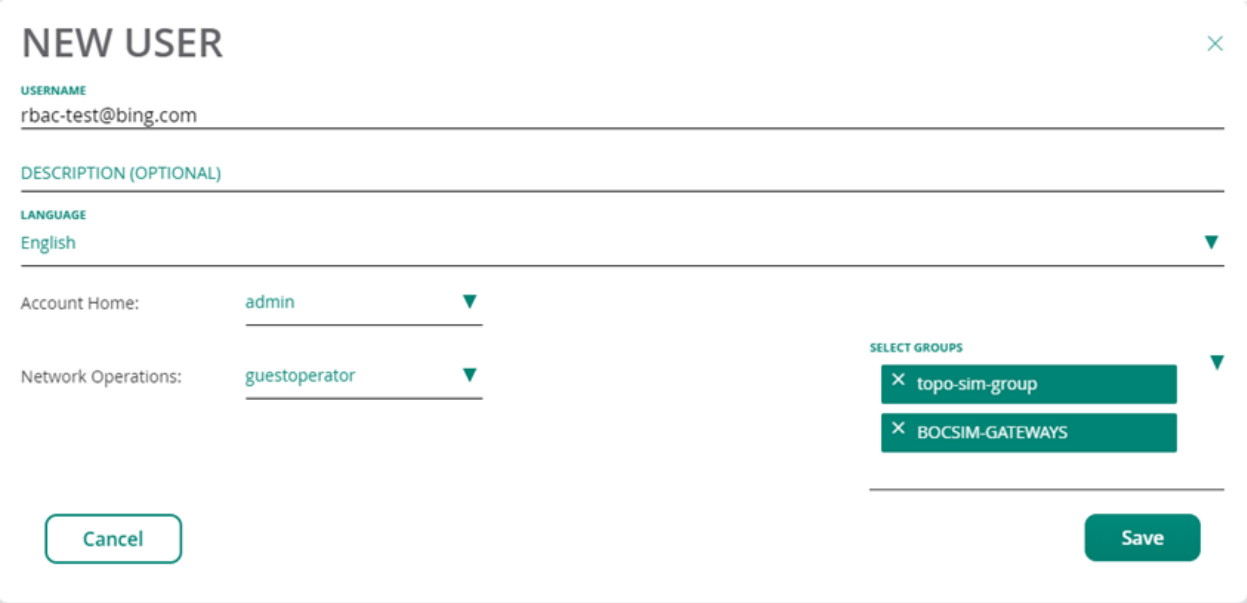
If an application is not provisioned, that application is not listed in the **New User** pop-up window.

   - **Network Operations**—Select a user role for the **Network Operations** application.

     If you assign the user role **guestoperator**, **readonly**, or **readwrite**, from the **Select Groups** drop-down list, select group(s). By default, the **admin** user role has access to all groups.
   - **ClearPass Device Insight**—Select a user role for the **ClearPass Device Insight** application.

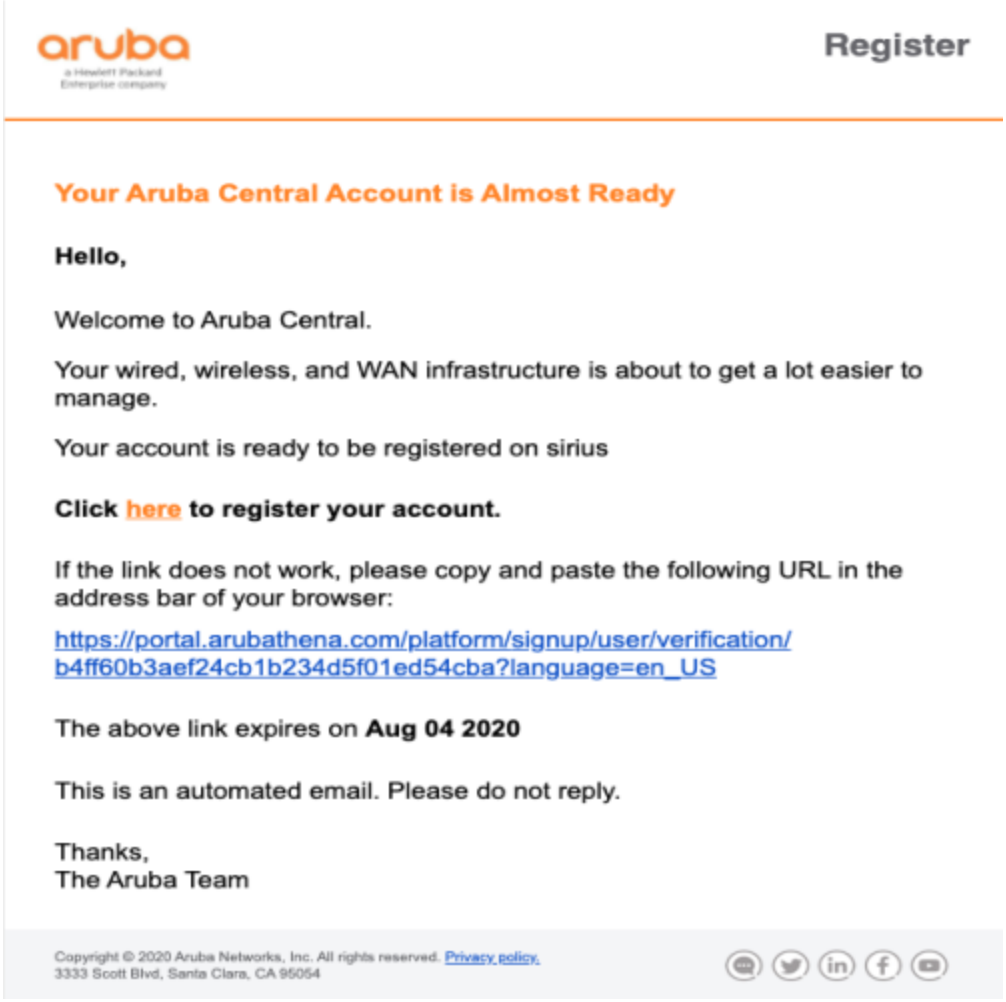
     For more information on user roles, see Configuring User Roles.
4. Click **Save**. An email invite is sent to the user with a registration link. Users can use this link to access Aruba Central.

Figure 36 *New User Window*



The registration link in the email invite is valid for 15 days. The link expiry date is also mentioned in the registration email notification:

Figure 37 *Aruba Central Registration Email*



aruba
a Hewlett Packard Enterprise company

Register

Your Aruba Central Account is Almost Ready

Hello,

Welcome to Aruba Central.

Your wired, wireless, and WAN infrastructure is about to get a lot easier to manage.

Your account is ready to be registered on sirius

Click here to register your account.

If the link does not work, please copy and paste the following URL in the address bar of your browser:

https://portal.arubathena.com/platform/signup/user/verification/b4ff60b3aef24cb1b234d5f01ed54cba?language=en_US

The above link expires on **Aug 04 2020**

This is an automated email. Please do not reply.

Thanks,
The Aruba Team

Copyright © 2020 Aruba Networks, Inc. All rights reserved. Privacy policy.
3333 Scott Blvd, Santa Clara, CA 95054

Resend Email Invite

If any user has not received the email invite, complete the following steps to resend the invite:

1. Click **Actions** and slide the **Resend Invitation To Users** toggle button to the right.
2. Enter the email ID and click **Resend Invite**.

Viewing User Details

In the **Account Home** page, under **Global Settings**, click **Users and Roles**. The **Users** tab is displayed. The **List of Users** table displays the following information:

- Email ID of the user.
- Type of user. The user can be system user or external user.
- Description of the user.
- Role assigned for the **Network Operations** app.
- Role assigned for the **ClearPass Device Insight** app. This option is displayed only if the **ClearPass Device Insight** app is provisioned and if you have subscribed to the app.
- Role assigned for the **Account Home** page.
- Allowed groups for the user.

- Last active time of the user. If the last active time cell is blank, the user has not logged in after the product upgrade.

Editing a User

To edit a user account, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
   The **Users** tab opens.
2. In the **List of Users** table, select the user and click the edit icon.
3. In the **Edit User <"Username">** window, modify description, role, or allowed groups.
4. Click **Save**.

Deleting a User

To delete a user account:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
   The **Users** tab opens.
2. In the **List of Users** table, select the user and click the delete icon.
3. Confirm user deletion in the **Confirm Action** dialog box.

Viewing Audit Trail Logs for Users

Audit logs are generated when a new user is created and an existing user is modified or deleted from the Aruba Central account. It also records the login and logout activities of users.

To view audit logs for Aruba Central users:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**.
   The **Audit Trail** page is displayed.
2. To view audit logs for user addition, modification, or deletion, click the filter in the **Classification** column, and select **User Management**.
3. To filter audit logs about user activity, click the filter in the **Classification** column, and select **User Activity**.

Configuring User Roles

A role refers to a logical entity used for determining user access to devices and application services in Aruba Central. Users are always tagged to roles that govern the level of user access to the Aruba Central applications and services.

Access control for federated users is determined by the attributes set in the IDP.

Aruba Central supports a set of predefined roles with different privileges and access permissions. You can also configure custom roles.

The following sections are covered in this page:

- Predefined Roles
- Module Permissions

- Custom Roles
- Viewing Role Details
- Editing a Role
- Deleting a Role

Predefined Roles

The **Users and Roles** page allows you to configure the following types of users with system-defined roles:

Table 47: *Predefined Roles*

Application	Role	Privilege
Account Home	**admin**	Administrator for the **Account Home** page. If there are common modules between **Account Home** and other app(s), the **Account Home** role has higher precedence and the user is granted permission if the operation is initiated from the **Account Home** page.
	guestoperator	Has guest operator access to the **Network Operations** application. User does not have access to **Account Home** > **Global Settings**.
	readwrite	Can view and modify settings in the **Account Home** page and all **Global Settings** pages. **NOTE:** The **readwrite** role does not have modify permission for the following pages: ▪ **Users and Roles** ▪ **Single-Sign-On**
	readonly	Can view the **Account Home** page and all **Global Settings** pages.
Network Operations	**admin**	Administrator for the **Network Operations** application. Has access to **Account Home** > **Global Settings**. This is applicable only if the **Account Home** role is not set or is not conflicting.
	deny-access	Cannot view the **Network Operations** application.
	guestoperator	Has guest operator access to the **Network Operations** application. User does not have access to **Account Home** > **Global Settings**.
	readonly	Has read-only access to **Account Home** > **Global Settings** and the **Network Operations** application.
	readwrite	Has read-write access to **Account Home** > **Global Settings** and the **Network Operations** application. Has access to view and modify data using the Aruba Central UI or APIs. However, the user cannot execute APIs to: ▪ Enable or disable MSP mode. ▪ Perform operations in the following pages: ◦ **Account Home** > **Users and Roles** ◦ **Network Operations** application > **Organization** > **Labels and Sites**
ClearPass Device Insight	**admin**	Administrator for the **ClearPass Device Insight** application.
	deny-access	Cannot view the **ClearPass Device Insight** application.
	readonly	Can launch and view all the pages in the **ClearPass Device Insight** application.

Module Permissions

Aruba Central enables you to define roles with view or modify permissions. You can also block user access to some modules. If a module is blocked for a specific role, the corresponding pages are not displayed in the UI or can access the pages but no data is displayed and all actions are disabled for the role.

Aruba Central supports setting permissions for the following modules:

Table 48: *Permissions*

Application	Module	Description
Account Home	**Devices and Subscription**	Enables users to add devices and assign keys and subscriptions to devices in the **Account Home** page.
	Users	Enables users to define a role with access (View, Modify, or Block) to the user details in the **Users** tab in the **Users and Roles** page. To define the role, navigate to **Account Home > Global Settings > Users and Roles**.
	Roles	Enables users to define a role with access (View, Modify, or Block) to the role details in the **Roles** tab in the **Users and Roles** page. To define the role, navigate to **Account Home > Global Settings > Users and Roles**.
	SSO	Enables users to define a role with access (**View**, **Modify**, and **Block**) to the **Single Sign On** profiles details in the **Users** tab in the **Single-Sign-On** page (**Account Home** > **Single-Sign-On**). Enables users to define a role with access (**View**, **Modify**, or **Block**) to the **Single Sign On** profiles details in the **Single Sign On** page. To navigate to the **Single Sign On** page, go to **Account Home > Single Sign On**.
Network Operations	**MSP**	Enables users with administrator role and privileges to define user access to MSP modules such as Customer Management and Portal Customization. The MSP tenant account user does not have access to the **MSP** application. Even if a tenant account user is assigned a custom role having **MSP** application privileges: ■ Tenant account user does have access to the **MSP** application. ■ **MSP** does not appear in the **Account Home** > **Global Settings** > **Users and Roles** > **Roles** > **Allowed Applications** list.
	Group Management	Enables users to create, view, modify, and delete groups and assign devices to groups.
	Devices and Subscription	Users cannot edit or set permissions for this module. **Modify** and **Block** options are disabled. By default, the **View Only** permission is set.
	Network Management	Enables users to configure, troubleshoot, and monitor Aruba Central-managed networks. You can customize the permissions (**View** or **Modify** or **Block**) for the following sub-modules: ■ Configuration ■ Configuration Variables

Application	Module	Description
		■ Privileged Configuration ■ Firmware ■ Troubleshooting ■ Other Modules **NOTE:** For the **Privileged Configuration**, the **Block** option disables the **Admin** tab (**Gateway** > **System** > **Admin**) for the user. The user management privileges are disabled for this user for gateways at the device and group level.
	Guest Management	Enables users to configure cloud guest splash page profiles.
	AirGroup	Enables users to define or block user access to the AirGroup pages.
	Presence Analytics	Enables users to access the Presence Analytics app and analyze user presence data.
	Floorplans	Enables user to access Floorplans and RF heatmaps.
	Unified Communications	Enables users to access the Unified Communications pages.
	Install Manager	Enables users to manage installer profiles and site installations.
	Reports	Enables users to view and create reports.
	Other Applications	Enables users to access other applications modules such as notifications and Virtual Gateway deployment service.
ClearPass Device Insight **NOTE:** This option is displayed only if the **ClearPass Device Insight** app is provisioned and if you have subscribed to the app.	**Classified devices**	Enables users to view or modify system and user-classified devices.
	Generic devices	Enables users to view or modify devices which are not classified by system or user.
	User classified devices	Enables users to view or modify user-classified devices.
	Discovery settings	Enables users to view, create, modify, or delete discovery settings.
	Application settings	Enables users to view or modify application level user settings
	Reports	Enables users to view create and view reports
	Other Applications	Enables users to define or block access to other applications.

Custom Roles

Along with the predefined roles, Aruba Central also enables you to create custom roles with specific security requirements and access control. However, only users with the administrator role and privileges can create, modify, clone, or delete a custom role in Aruba Central.

With custom roles, you can configure access control at the application level and specify access rights to view or modify specific application services or modules. For example, you can create a custom role that enables access to a specific applications such as **Guest Management** or **Network Management** and assign it to a user.

MSP tenant account users cannot add, edit, or delete roles.

Adding a Custom Role

The following are the permissions that you can associate with a custom role:

- Roles with **Modify** permission can perform add, edit, or delete actions within the specific module.
- Roles with **View Only** permission can only view the specific module.
- Roles with **Block** permission cannot view that particular module or can view the corresponding pages but no data is displayed and all actions are disabled.

To add a custom role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. Click **Add Role**. The **New Role** window is displayed.
4. Specify a name for the role.
5. From the drop-down list, select one of the following:
   - **Account Home**—To manage access to devices and subscriptions in Aruba Central.
   - **Network Operations**—To set permissions at the module level in the **Network Operations** application.
   - **ClearPass Device Insight**—To set permissions at the module level in the **ClearPass Device Insight** application. This option is displayed only if the **ClearPass Device Insight** app is provisioned and if you have subscribed to the app.
6. For Network Management and MSP modules, you can set access rights at the module level.

   To set view or edit permissions or block the users from accessing a specific module, complete the following steps:
   a. Click **Customize**.
   b. Select one of the following options for each module as required:
      - **View Only**
      - **Modify**
      - **Block**
7. Click **Save**.
8. Assign the role to a user account as required.

Viewing Role Details

To view the details of a role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab. The **Roles** tab displays the following information:
   - **Role Name**—Name of the role.
   - **Allowed Applications**—The application(s) to which the user account is subscribed to.
   - **Assigned Users**—Number of users assigned to a role.

Editing a Role

To edit a role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the edit icon.
4. In the **Edit Role <"Rolename">** window, modify the permissions set for module(s).
5. Click **Save**.

Deleting a Role

To delete a role, ensure that the role is not associated to any user and complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the delete icon.
4. Confirm role deletion in the **Confirm Action** dialog box.

Configuring SAML SSO for Aruba Central

The SSO solution simplifies user management by allowing users to access multiple applications and services with a single set of login credentials. If the applications services are offered by different vendors, IT administrators can use the SAML authentication and authorization framework to provide a seamless login experience for their users.

To provide seamless login experience for users whose identity is managed by an external authentication source, Aruba Central now offers a federated SSO solution based on the SAML 2.0 authentication and authorization framework. SAML is an XML-based open standard for exchanging authentication and authorization data between trusted partners; in particular, between an application service provider and identity management system used by an enterprise. With Aruba Central's SAML SSO solution, organizations can manage user access using a single authentication and authorization source.

SAML SSO Solution Overview

The SAML SSO solution consists of the following key elements:

- **Service Provider (SP)**—The provider of a business function or service; For example, Aruba Central. The service provider requests and obtains an identity assertion from the IdP. Based on this assertion, the service provider allows a user to access the service.
- **Identity Provider (IdP)**—The Identity Management system that maintains identity information of the user and authenticates the user.
- **SAML Request**—The authentication request that is generated when a user tries to access the Aruba Central portal.
- **SAML Assertion**—The authentication and authorization information issued by the IdP to allow access to the service offered by the service (Aruba Central portal).
- **Relying Party**—The business service that relies on SAML assertion for authenticating a user; For example, Aruba Central.
- **Asserting Party**—The Identity management system or the IdP that creates SAML assertions for a service provider.

- **Metadata**—Data in the XML format that is exchanged between the trusted partners (IdP and Aruba Central) for establishing interoperability.
- **SAML Attributes**—The attributes associated with the user; for example, username, customer ID, role, and group in which the devices belonging to a user account are provisioned. The SAML attributes must be configured on the IdP according to specifications associated with a user account in Aruba Central. These attributes are included in the SAML assertion when Aruba Central sends a SAML request to the IdP.
- **Entity ID**—A unique string to identify the service provider that issues a SAML SSO request. According to the SAML specification, the string should be a URL, although not required as a URL by all providers.
- **Assertion Services Consumer URL**—The URL that sends the SAML request and receives the SAML response from the IdP.
- **User**—User with SSO credentials.

- Aruba Central SAML SSO solution supports only the HTTP Redirect POST method for sending and receiving SAML requests and response.
- The SAML SSO integration allows federated users to access only the Central UI. The API Gateway access is restricted to system users that are configured and managed from Aruba Central.

How SAML SSO Works

Aruba Central supports the following types of SAML SSO workflows:

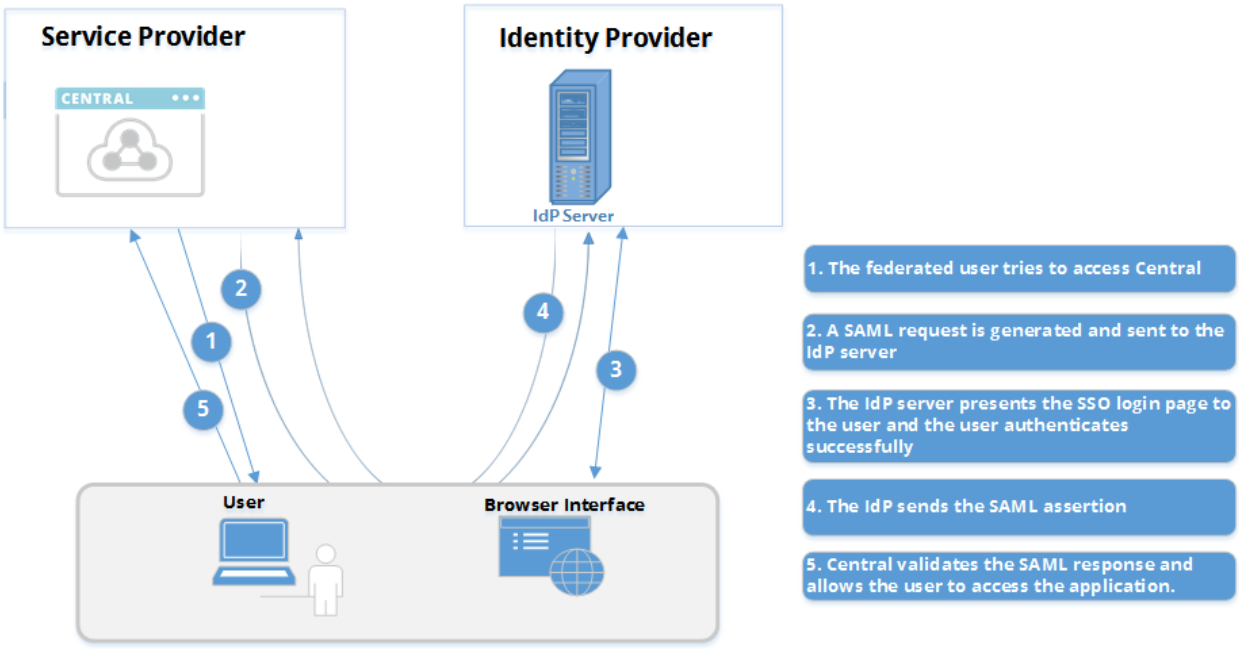
- SP-initiated SSO
- IdP-initiated SSO

SP-initiated SSO

In an SP Initiated SSO workflow, the SSO request originates from the service provider domain, that is, from Aruba Central. When a user tries to access Aruba Central, a federation authentication request is created and sent to the IdP server.

The following figure illustrates the standard SP-Initiated SAML SSO workflow:

Figure 38 *SP-Initiated SSO*



The SP-initiated SSO workflow with Aruba Central is supported only through the HTTP Redirect POST method. In other words, Aruba Central sends an HTTP redirect message with an authentication request to the IdP through the user's browser. The IdP sends a SAML response with an assertion to Aruba Central through HTTP POST.

The SP-initiated SSO workflow with HTTP Redirect POST includes the following steps:

1. The user tries to access Aruba Central and the request is redirected to the IdP.
2. Aruba Central sends an HTTP redirect message with the SAML request to the IdP for authentication through the user's browser.
3. The user logs in with the SSO credentials.
4. On successful authentication, the IdP sends a digitally signed HTML form with SAML assertion and attributes to Aruba Central through the web browser.
5. If the digital signature and the attributes in the SAML assertion are valid, Aruba Central allows access to the user.

IdP-initiated SSO

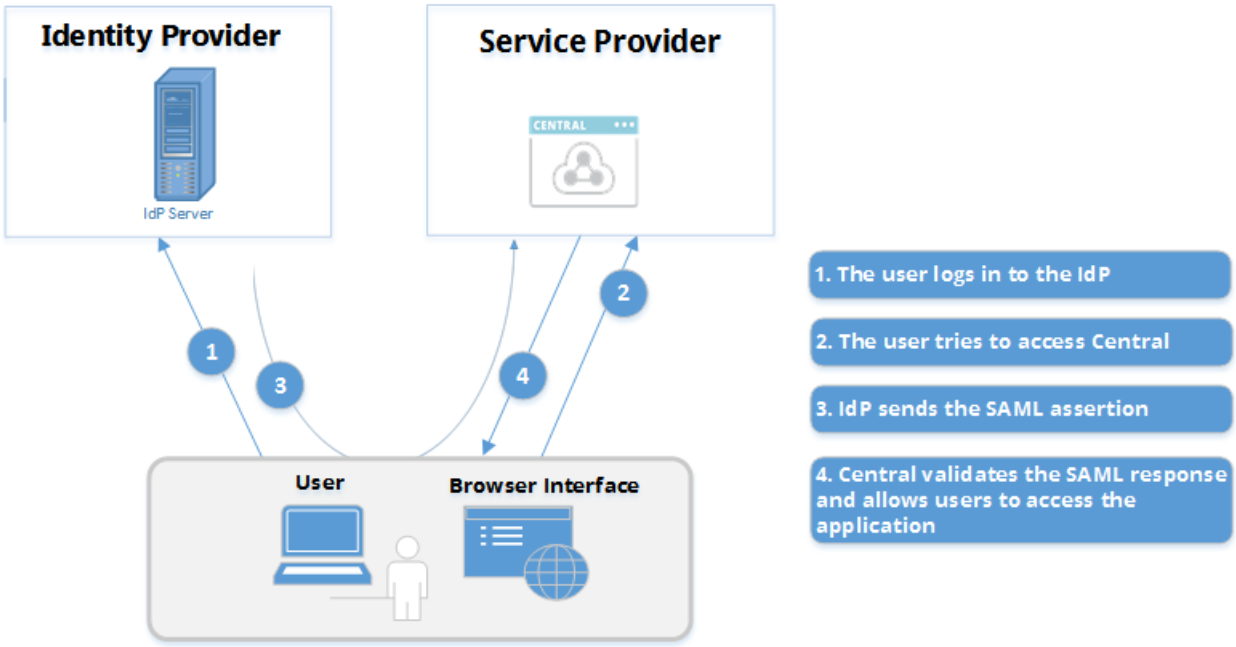
In the IdP-Initiated workflow, the SSO request originates from the IdP domain. The IdP server creates a SAML response and redirects the users to Aruba Central.

The Aruba Central SAML SSO deployments support the IdP-initiated SSO workflow through the HTTP POST method. The IdP-initiated SSO workflow consists of the following steps:

1. The user is logged in to the IdP and tries to access Aruba Central.
2. The IdP sends a digitally signed HTML form with SAML assertion and attributes to Aruba Central through the web browser.
3. If the digital signature and the attributes in the SAML assertion are valid, Aruba Central allows access to the user.

The following figure illustrates the standard IdP-Initiated SAML SSO workflow:

Figure 39 *IdP-Initiated SSO*



SAML SSO Single Logout

Aruba Central supports Single Logout (SLO) of SAML SSO users. SLO allows users to terminate server sessions established using SAML SSO by initiating the logout process once. SAML SLO can be initiated either from the Service Provider or the IdP. However, Aruba Central supports only the IdP-initiated SLO.

IdP-initiated SAML SLO

The IdP-initiated logout workflow includes the following steps:

1. User logs out of the IdP.
2. The IdP sends a logout request to Aruba Central.
3. Aruba Central validates the logout request from the IdP, terminates the user session, and sends a logout response to the IdP.
4. User is logged out of Aruba Central.
5. After the IdP receives logout response from all service providers, the IdP logs out the user.

Configuring SAML SSO

The SAML SSO configuration for Aruba Central includes the following steps:

1. Configuring user accounts and roles in Aruba Central. For more information, see the *Managing User Access* topic in *Aruba Central Help Center*.
2. Configure SAML authorization profile in Aruba Central.
3. Configuring Service Provider metadata such as metadata URL, service consumer URL, Name and other attributes on the IdP server.

Configuring SAML Authorization Profiles in Aruba Central

For SAML SSO solution with Aruba Central, you must configure a valid SAML authorization profile in the Aruba Central portal.

Important Points to Note

Following are the important points to note about the SAML authorization in Aruba Central:

- The SAML authorization profile configuration feature is available only for the admin users of an Aruba Central account. Aruba Central allows only MSP admin users to configure SAML authorization profiles for their respective tenant accounts.
- Each domain can have only one federation. There must be at least one verified user belonging to the domain in the system users' list.
- Aruba Central allows only one authorization profile per domain.
- SAML user access is determined by the role attribute included in the SAML token provided by the IdP.
- SAML users with admin privileges can configure system users in Aruba Central.
- SAML users can initiate a Single Sign On request by trying to log in to Aruba Central (SP-initiated login). However, SAML users cannot initiate a single logout request from Aruba Central.
- The following menu options in Aruba Central UI are not available for a SAML user.
  - **Enable MSP** and **Disable MSP**—SAML users cannot enable or disable MSP deployment mode in Aruba Central.
  - **Change Password**—Aruba Central does not support changing the password of a SAML user account.

Before You Begin

Before you begin, ensure that you have the following information:

- **Entity ID**—A unique string that identifies the service provider that issues a SAML SSO request. According to the SAML specification, the string should be a URL, although not required as URL by all providers.
- **Login URL**—Login URL configured on the IdP server.
- **Logout URL**—Logout URL configured on the IdP server.
- **Certificate Details**—SAML signing certificate in the Base64 encoded format. The SAML signing certificates are required for verifying the identity of IdP server and relying applications such as Aruba Central.
- **Metadata URL**—Service provider metadata URL configured on the IdP server.

SAML profiles can also be configured using NB APIs. If you want to use NB APIs for configuring SAML profiles, use the APIs available under the **SSO Configuration** category in Aruba Central API Gateway.

Configuring a SAML Authorization Profile

To configure the SAML authorization profiles in Aruba Central, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Single Sign On**. The **Single Sign On** page is displayed.
2. To add an authorization profile, enter the domain name.

- Ensure that the domain has at least one verified user.
- For public cloud deployments, Aruba Central does not support adding **hpe.com**, **arubanetworks.com** and other free public domain names, such as Gmail.com, Yahoo.com, or Facebook.com, for SAML authorization profiles.

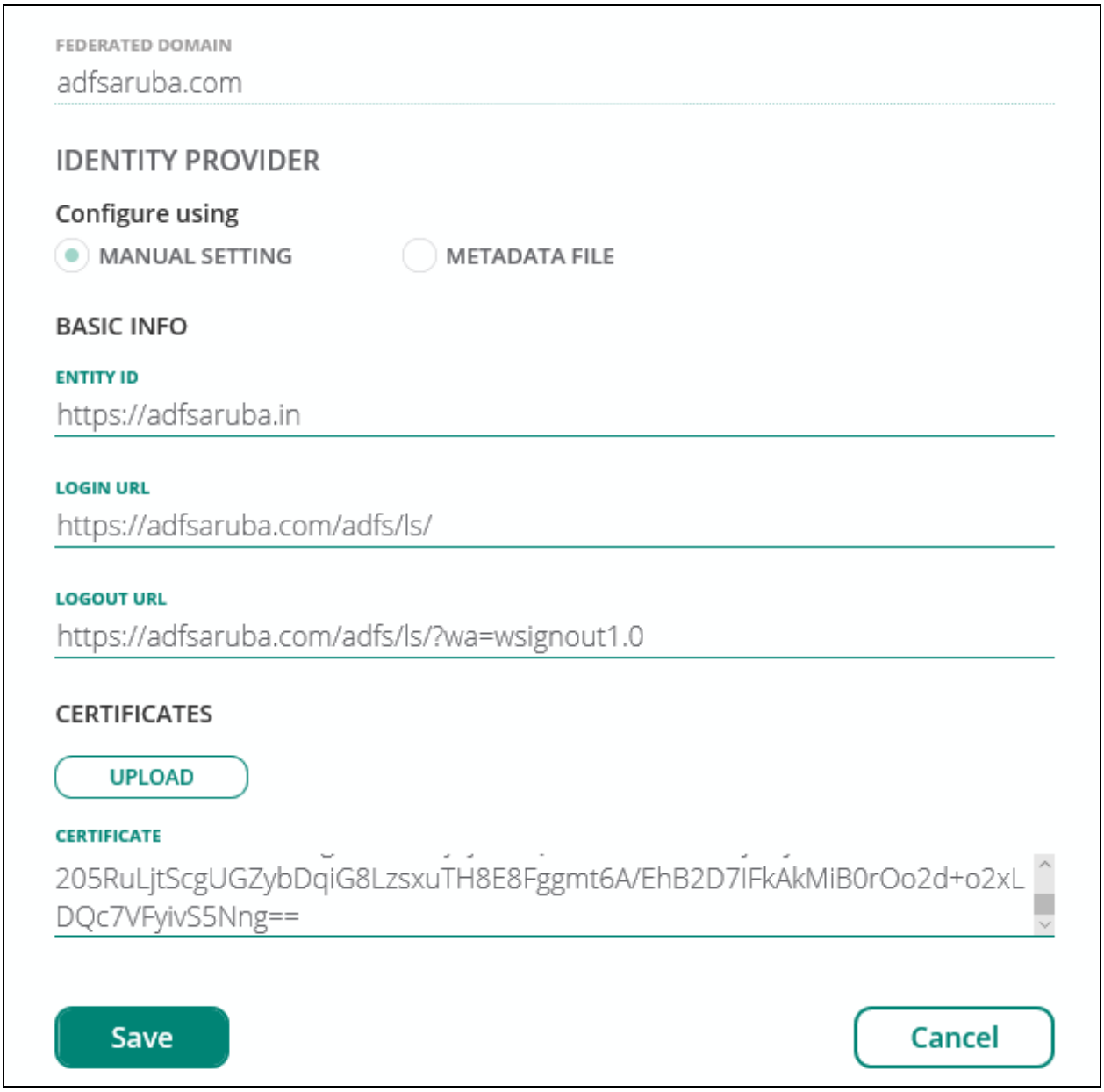
3. Click **Add SAML Profile**.
4. To manually enter the metadata:
   a. Select **Manual Setting** and enter the following information:
      - **Entity ID**—Entity ID configured on the IdP server.
      - **Login URL**—Login URL configured on the IdP server.
      - **Logout URL**—Login URL configured on the IdP server.
      - **Certificate**—Certificate details. Ensure that the certificate content is in the Base64 encoded format. You can either upload a certificate or paste the contents of the certificate in the text box.

Ensure that the Entity ID, Login URL, and Logout URL fields have valid HTTPS URLs.

   b. Click **Save**.

The following figure shows an example for the manual entry of metadata:

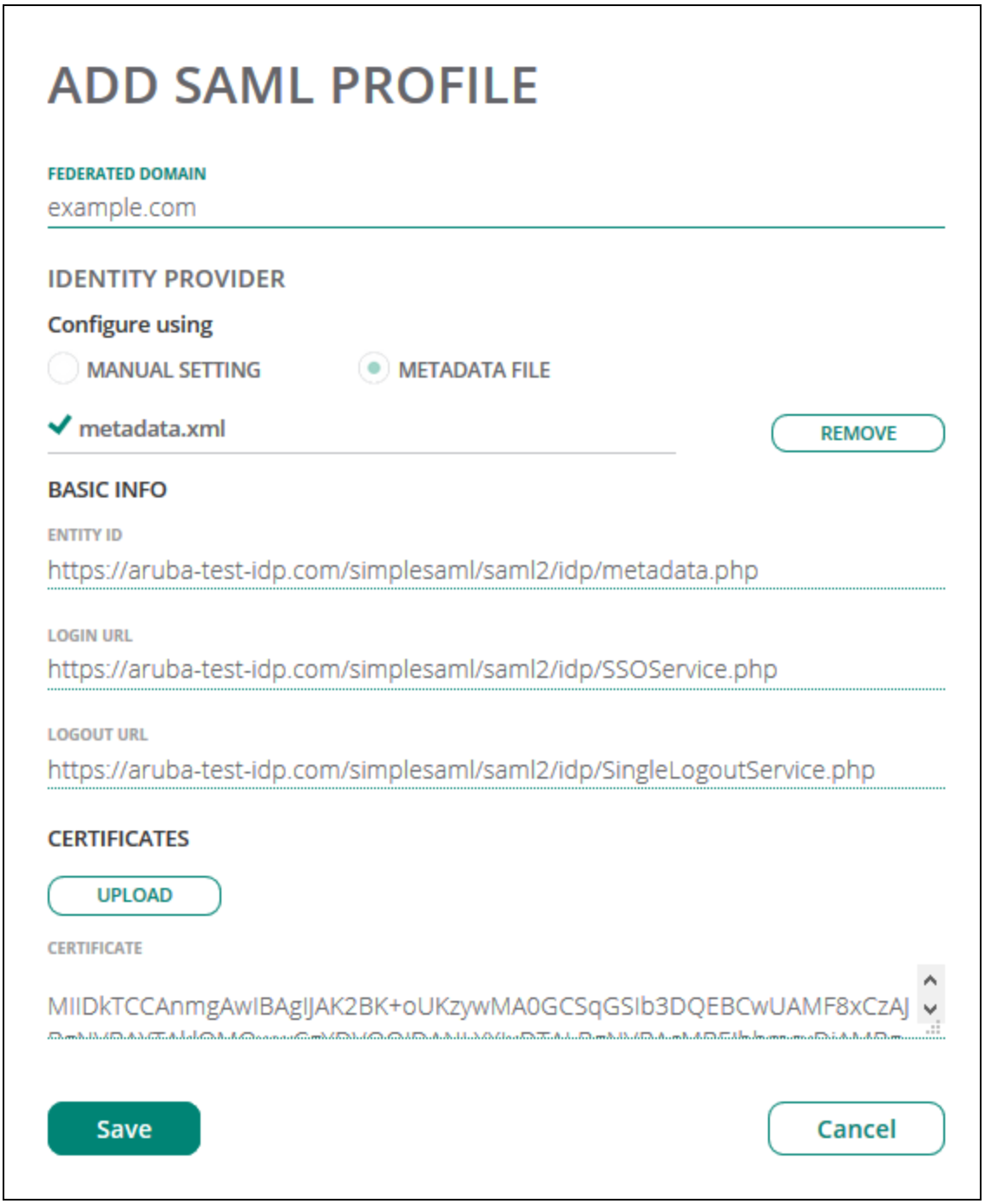
Figure 40 *Manual Addition of Metadata*



5. If you have already configured the IdP server and downloaded the metadata file, you can upload the metadata file. To upload a metadata file:
   a. Select **Metadata File**. Ensure that the metadata file is in the XML format and it includes valid certificate content and HTTPS URLs for the Entity ID, Login URL, and Logout URL fields.
   b. Click **Browse** and select the IdP metadata file. Aruba Central extracts the **Entity ID**, **Login URL**, **Logout URL**, and certificate content.
   c. Verify the details.
   d. Click **Save**.

   The following figure shows an example for the content imported from a metadata file:

Figure 41 *Importing Information from a Metadata File*



Configuring Service Provider Metadata in IdP

Aruba Central supports SAML SSO authentication framework with various Identity Management vendors such as ADFS, PingFederate, Aruba ClearPass Policy Manager, and so on.

Aruba recommends that you look up the instructions provided by your organization for adding service provider metadata to the IdP server in your setup.

Some of the generic and necessary attributes required to be configured on the IdP server for SAML integration with Aruba Central are described in the following list:

- **Metadata URL**—URL that provides service provider metadata.
- **Entity ID**—A unique string that identifies the service provider that issues a SAML SSO request. According to the SAML specification, the string should be a URL, although not required as URL by all providers.
- **Assertion Services Consumer URL**—The URL that sends SAML SSO login requests and receives authentication response from the IdP.
- **NameID**—The **NameID** attribute must include the email address of the user.

  <NameID>johnnyadmin1@adfsaruba.com</NameID>

  If the **NameID** attribute does not return the email address of the user, you can use the **aruba_user_email** attribute. Ensure that you configure the **NameID** or the **aruba_user_email** attribute for each user.
- **SAML Attributes**—The following example shows the syntax structure for SAML attributes:

```
#customer 1
 aruba_1_cid = <customer-id>
 # app1, scope1
 aruba_1_app_1 = central
 aruba_1_app_1_role_1 = <readonly>
 aruba_1_app_1_role_1_tenant = <admin>
 aruba_1_app_1_group_1 = groupx, groupy
 aruba_1_app_2 = device_profiling
 aruba_1_app_2_role_1 = <readonly>
 aruba_1_app_3 = account_setting
 aruba_1_app_3_role_1 = <readonly>
```

```
#customer 2
 aruba_2_cid = <customer-id>
 # app1, scope1
 aruba_2_app_1 = central
 aruba_2_app_1_role_1 = <readonly>
 aruba_2_app_1_role_1_tenant = <admin>
 aruba_2_app_1_group_1 = groupx, groupy
 aruba_2_app_2 = device_profiling
 aruba_2_app_2_role_1 = <readonly>
 aruba_2_app_3 = account_setting
 aruba_2_app_3_role_1 = <readonly>
```

Note the following points when defining SAML attributes in the IdP server:

- **cid**—Customer ID. If you have multiple customers, define attributes separately for each customer ID.
- **app**—Application. Set the value as per the following:
  - **Network Operations**—central
  - **Clear Pass Device Insight**—device_profiling
  - **Account Home**—account_setting
- **role**—User role. Specify the user role. If no role is defined, Aruba Central assigns read-only role to the user.
- **tenant role**—Tenant user role. If the tenant role is not defined in the IdP, the MSP role is assigned to the SAML user.
- **group**—Group in Aruba Central. When a group is specified in the attribute, the user is allowed to access only the devices in that group. If the attribute does not include any group, Aruba Central allows SAML

SSO users to access all groups. You can also configure custom attributes to add multiple groups if the user requires access to multiple groups.

Aruba Central recommends you to configure the **Account Home**. However, If you do not return the **Account Home** application from the Idp, then the **Network Operations** role is applied by default.

See Also:

- Configuring Service Provider Metadata in Microsoft ADFS
- Configuring Service Provider Metadata in PingFederate IdP
- Configuring Service Provider Metadata in ArubaClearPass Policy Manager

Configuring Service Provider Metadata in Microsoft ADFS

This procedure describes the steps required for configuring service provider metadata in Microsoft Active Directory Federation Services (ADFS) for SAML integration with Aruba Central.

ADFS runs on Windows Servers and provides users with SSO access to application services hosted by the trusted service providers.

This topic provides a basic set of guidelines required for setting up the ADFS instance on a Windows Server 2016 as an IdP. The images used in this procedure may change with Windows Server updates.

Before you Begin

- Go through the SAML SSO feature description to understand how SAML framework works in the context of Aruba Central.
- Ensure that the ADFS is installed and available for configuration on a Windows server. For more information, see the ADFS Deployment Guide.
- Ensure that an Active Directory security group is configured and the users are added as group members. For more information, see the ADFS Deployment Guide.

Steps to Configure Service Provider Metadata in ADFS

To enable SAML integration with ADFS, complete the following steps:

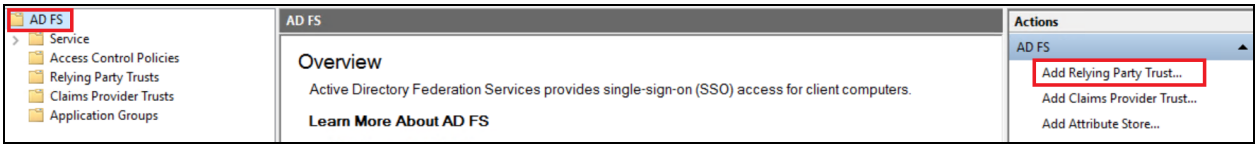
- Step 1:Adding a Relying Party Trust
- Step 2:Configure the Name ID Attribute
- Step 3:Configure the Customer ID Attribute
- Step 4:Configure the Application Attribute
- Step 5:Configure the Role Attribute
- Step 6:Configure the Group Attribute
- Step 7:Configure the Logout URL
- Step 8:Exporting Token-signing Certificate
- Step 9:SAML Authorization Profile in Aruba Central

Step 1:Adding a Relying Party Trust

To configure Aruba Central and ADFS as trusted partners, complete the following steps:

1. On Windows Server, click **Start > Administrative Tools > AD FS Management**. The ADFS administrative console opens.
2. Click **AD FS** folder and select **Add Relying Party Trust** from the **Actions** menu.

Figure 42 *AD FS Management*

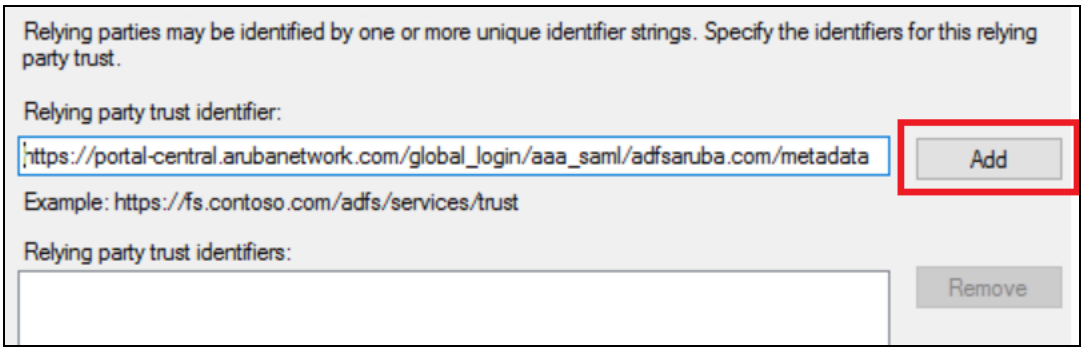


3. Select **Enter data about the relying party manually**.
4. Click **Next**.
5. Enter a **Display Name**. The name entered here will be displayed in the management console and to the users logging in to Aruba Central.
6. Click **Next**.
7. Select **AD FS Profile** and then click **Next**.
8. Select **Enable support for the SAML 2.0 WebSSO protocol** check box and enter the consumer URL that you want to use for sending SAML SSO login requests and receiving SAML response from the IdP.

Figure 43 *Enabling Support for SAML 2.0 WebSSO Protocol*

9. Click **Next**.
10. Add Aruba Central URL as the relying party trust identifier.

Figure 44 *Adding Replying Party Trust Identifier*



11. Click **Next**.
12. Select the preferred security setting. You can select **Permit all users to access this relying party** option to permit access to all users.
13. Click **Close**.
14. Verify if Aruba Central is added to the list of relying party trust.

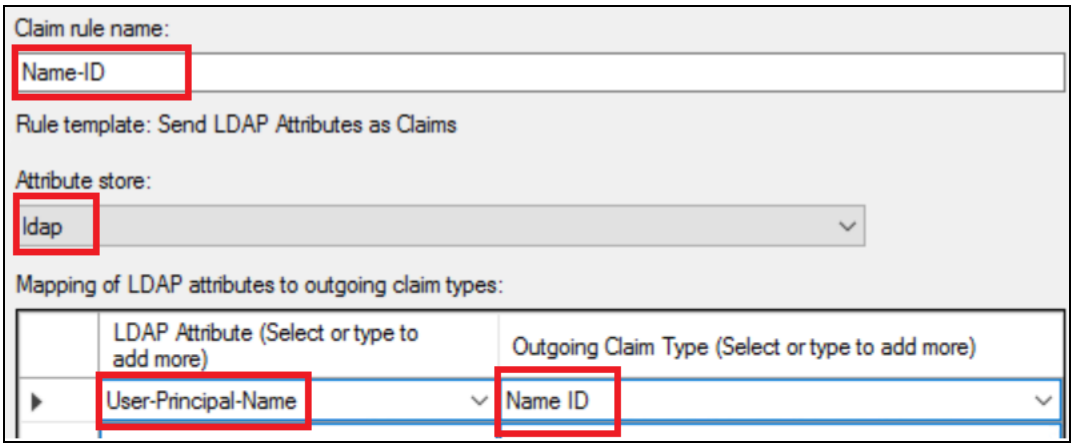
Step 2:Configure the Name ID Attribute

The Name ID attribute is used for user identification. For SAML integration with Aruba Central, the Name ID attribute must include the email address of the user. If the Name ID attribute does not return the email address of the user, use the **aruba_user_email** attribute.

To configure the Name-ID attribute:

1. Select the display name you just added for Aruba Central and click **Edit Claim Issuance Policy**.
2. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
3. Set the Claim Rule template to **Send LDAP Attributes as Claims rule**.
4. Click **Next**.
5. In the **Claim rule name** text box, enter **Name-ID**.

   Figure 45 *Adding Claim Rule Name*



6. Select the LDAP as the **Attribute store**.
7. Select the **User-Principal-Name** as LDAP attribute and **Name ID** for the **Outgoing Claim Type.**
8. Click **Finish**.

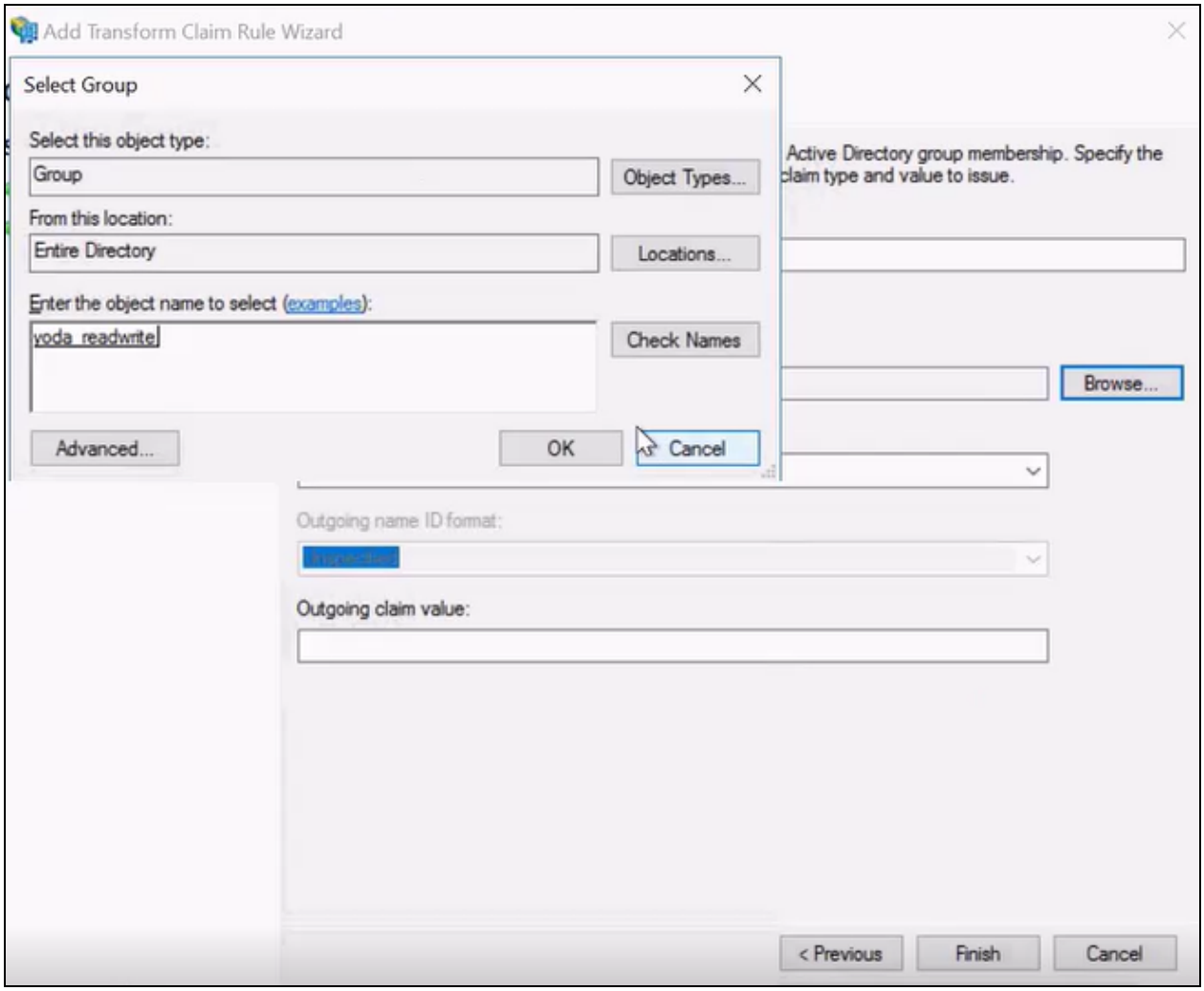
Step 3:Configure the Customer ID Attribute

To create a rule with the customer ID attribute:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.
3. Click **Next**.
4. In the **Claim rule name** text box, enter the customer ID attribute. For example, **aruba-cid**.

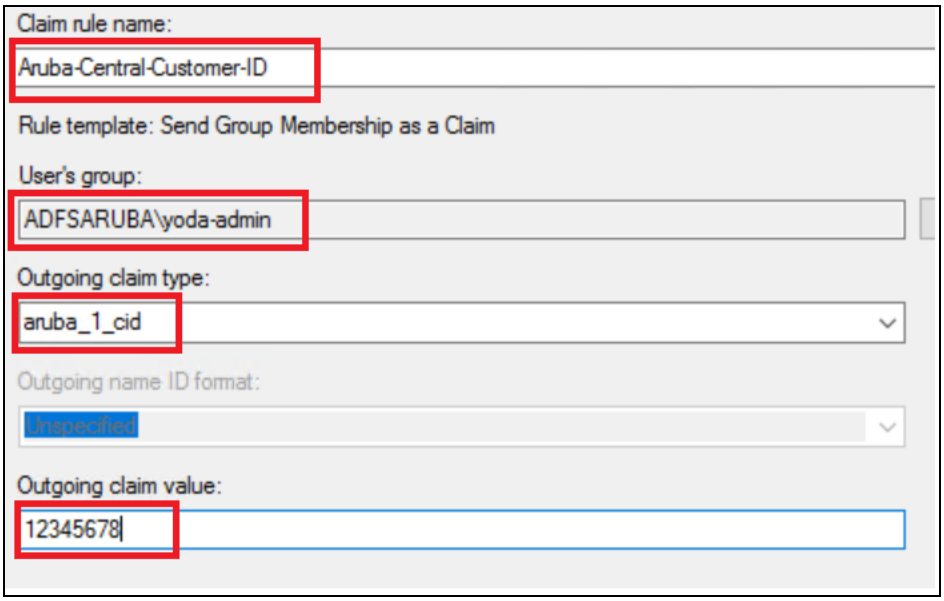
5. Select a user group.

Figure 46 *Selecting a User Group*



6. Click **OK**.
7. Select a customer ID attribute for the **Outgoing claim rule** and enter a value for the **Outgoing claim value**.

Figure 47 *Configuring Claim Rule Details*



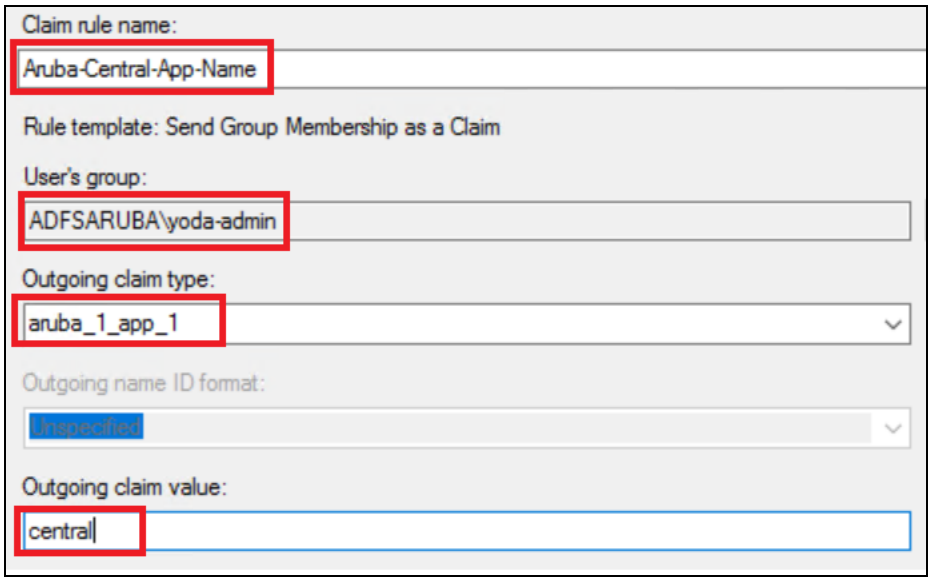
8. Click **Finish**.
9. If you have multiple customers, define the customer ID attribute separately for each customer ID.

Step 4:Configure the Application Attribute

To add a rule for the application attribute, complete the following steps:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.
3. Click **Next**.
4. In the **Claim rule name** text box, enter the application attribute. For example, **Aruba Central App Name**.
5. Select a user group.
6. Select the application attribute for **Outgoing claim type** and enter a value for the **Outgoing claim value.**

Figure 48 *Configuring the Application Attribute*



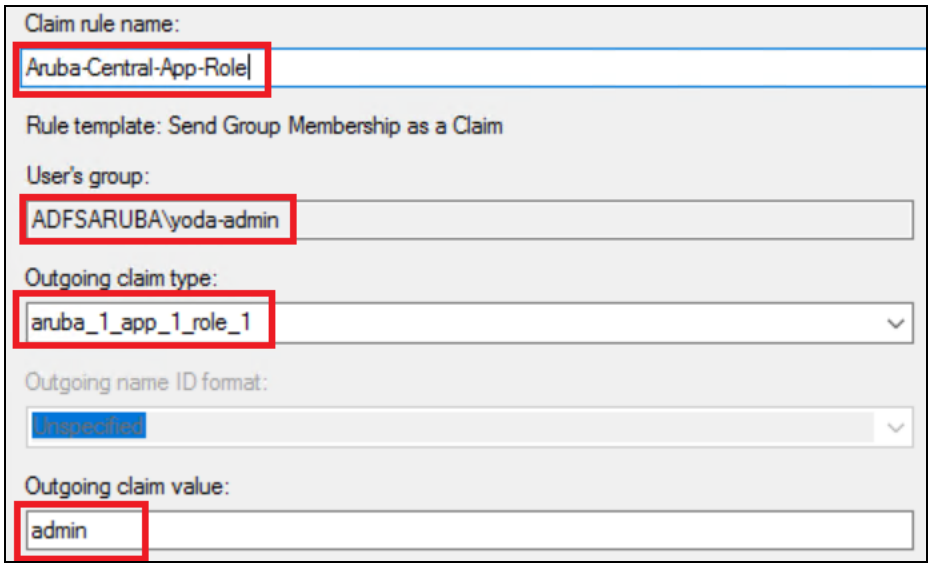
7. Click **Finish**.

Step 5:Configure the Role Attribute

To add a rule for a role attribute, complete the following steps:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.
3. Click **Next**.
4. In the **Claim rule name** text box, enter the application attribute. For example, **Aruba Central App Role**.
5. Select a user group.
6. Select the role attribute for **Outgoing claim type** and enter a value for the **Outgoing claim value.**

Figure 49 *Configuring the Role Attribute*



7. Click **Finish**.

If the role attribute is not configured, Aruba Central assigns a read-only role to the user.

Step 6:Configure the Group Attribute

If you want to restrict user access to a group in Aruba Central, you can configure the group attribute. If the group attribute is not configured, Aruba Central allows SAML SSO users to access all groups.

To add a rule for a group attribute, complete the following steps:

1. In the **Edit Claim Issuance Policy** window, click **Add Rule**.
2. To send a claim based on a user's Active Directory group membership, set the Claim Rule template to **Send Group Membership as a Claim**.
3. Click **Next**.
4. In the **Claim rule name** text box, enter the application attribute. For example, **Aruba Central App Group**.
5. Select a user group.
6. Select a group attribute for **Outgoing claim type** and enter a value for the **Outgoing claim value.**
7. Click **Finish**.

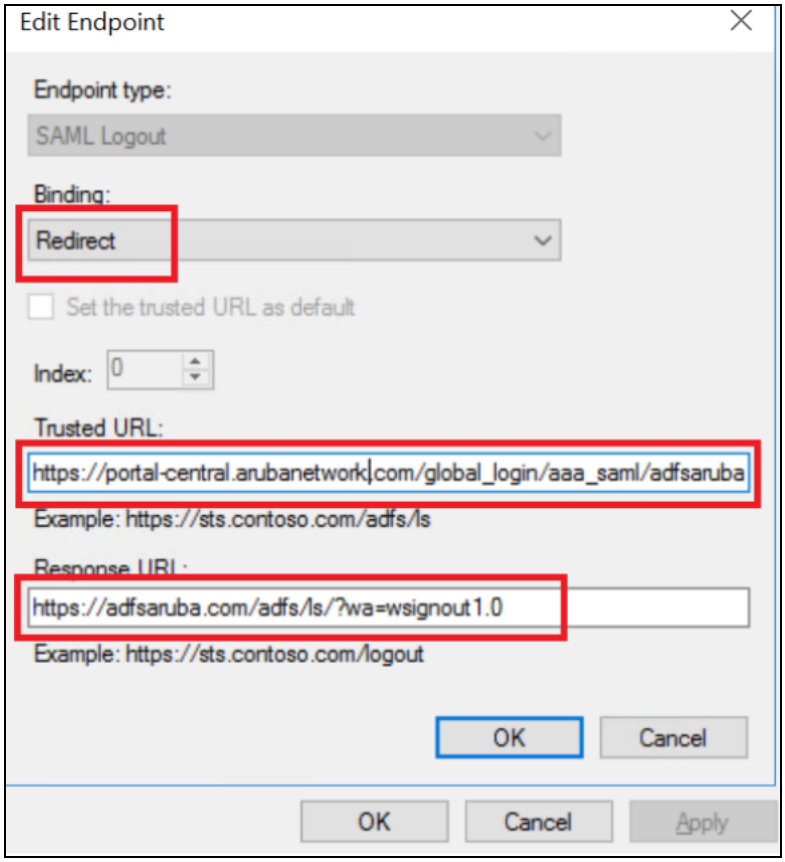
Step 7:Configure the Logout URL

To enable IdP-initiated logout, complete the following steps:

1. Select the relying party trust entry created for Aruba Central and click **Properties**.
2. Click **Endpoints**.
3. To add a logout URL, click **Add SAML**.
4. Select the endpoint type as **SAML Logout**.
5. Select **Redirect** for **Binding**.
6. Enter the Aruba Central logout URL for **Trusted URL**. Sample Trusted URL:
   `https://portal-yoda.arubathena.com/global_login/aaa_saml/adfsaruba.com?sls`

7. Enter the IdP logout URL for **Response URL**.

   Figure 50 *Configuring the Logour URL*



8. Click **OK**.

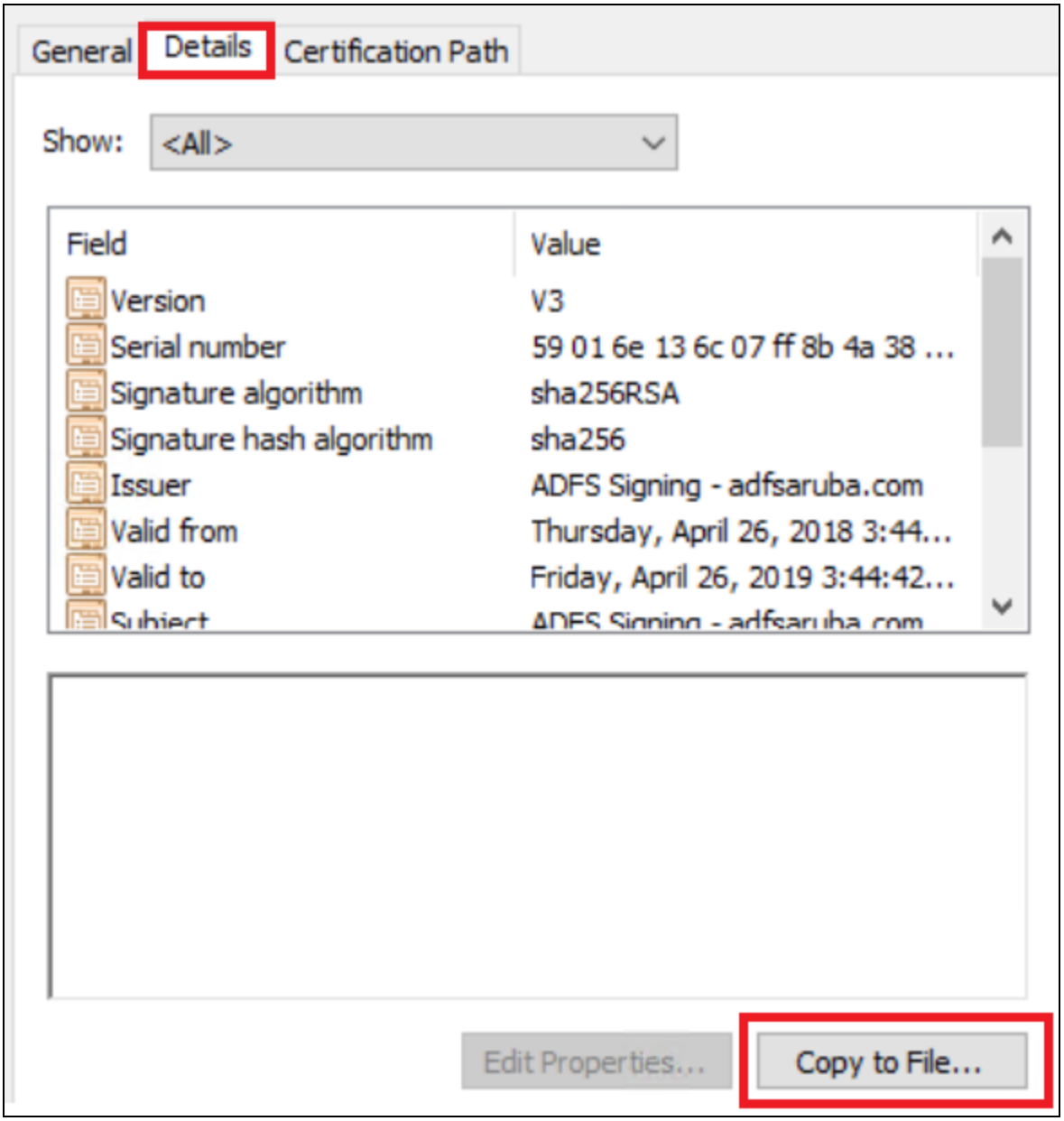
Step 8:Exporting Token-signing Certificate

The token-signing certificate is required SAML authentication. To export the token-signing certificate:

1. In the ADFS management console, go to **AD FS > Service > Certificates**.
2. Click the certificate under Token-signing and select **View Certificate** from the contextual menu.

3. Click **Details > Copy to File**.

Figure 51 *Exporting Token-Signing Certificate*



4. Click **Next** and select **Base-64 encoded X.509 (.CER)** as the certificate format.
5. Click **Next**.
6. Save the certificate file on your local directory.

Step 9:SAML Authorization Profile in Aruba Central

For information on how to configure a SAML authorization profile, see Configuring SAML Authorization Profiles in Aruba Central.

Configuring Service Provider Metadata in PingFederate IdP

This procedure describes the steps required for configuring service provider metadata in PingFederate.

NOTE

This topic provides a basic set of guidelines required for service provider metadata on the PingFederate server. The images and attributes may change with PingFederate software updates.

Before you Begin

Go through the SAML SSO feature description to understand how SAML framework works in the context of Aruba Central.

Steps to Configure Service Provider Metadata in PingFederate

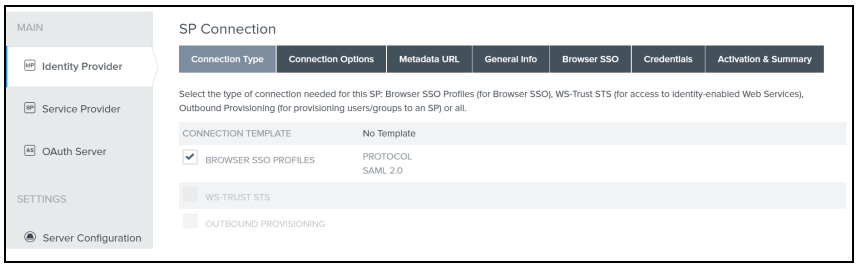
To configure service provider metadata in PingFederate, complete the following steps:

- Step 1:Create an SP Connection Profile
- Step 2:Configure Browser SSO Settings
- Step 3:Configure Credentials
- Step 4:Review Configuration
- Step 5:SAML Authorization Profile in Aruba Central

Step 1:Create an SP Connection Profile

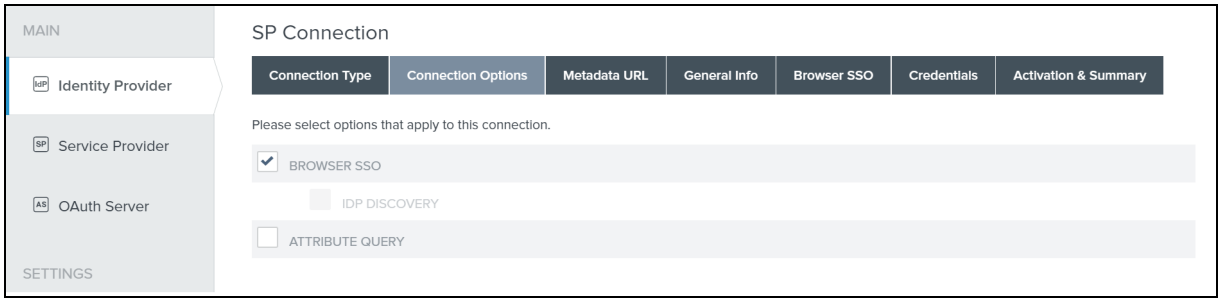
1. Log in to the PingFederate administration console.
2. Click **IdP Configuration** > **SP Connections** > **Create New**. The **SP Connections** page opens.

   Figure 52 *SP Connections Window*



3. In the **Connection Type** tab, select **Browser SSO Profiles**.

   Figure 53 *Connection Options*



4. Click the **General Info** tab.

5. Verify the Entity ID and select the logging mode.

Figure 54 *General Info*

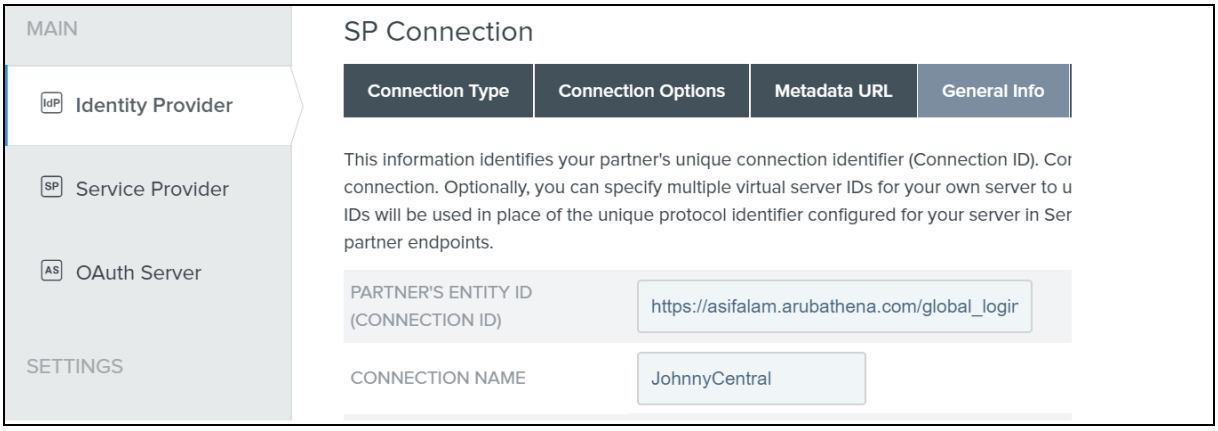
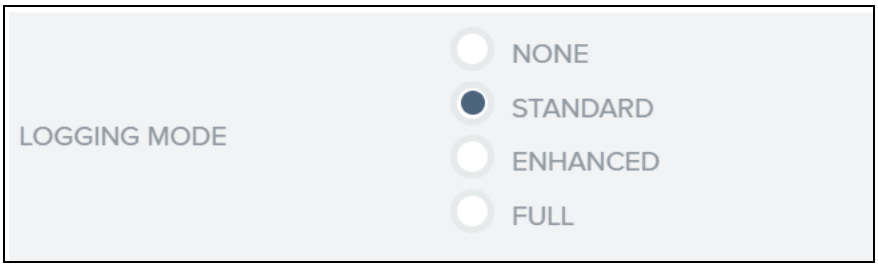


Figure 55 *Logging Mode*

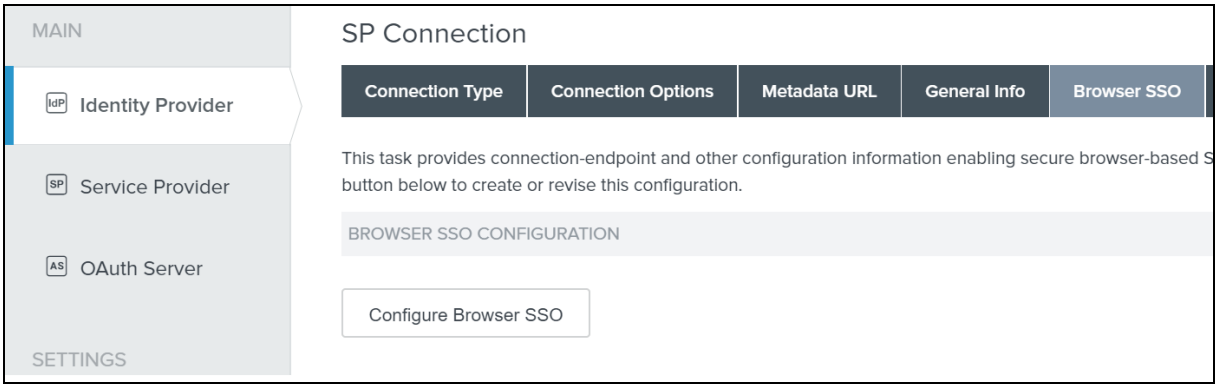


6. Click **Next** to configure the Browser SSO Settings.

Step 2:Configure Browser SSO Settings

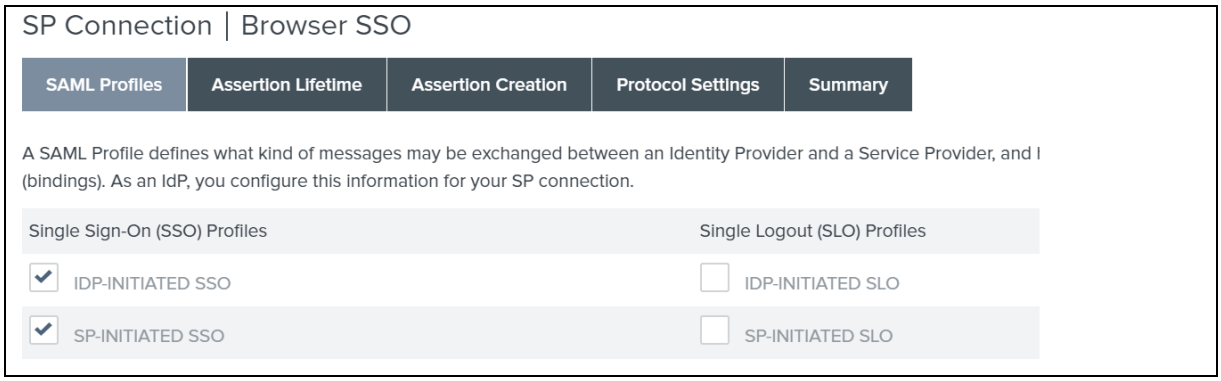
1. On the **SP Connections** page in PingFederate administrative console, click **Browser SSO**.

Figure 56 *Browser SSO*



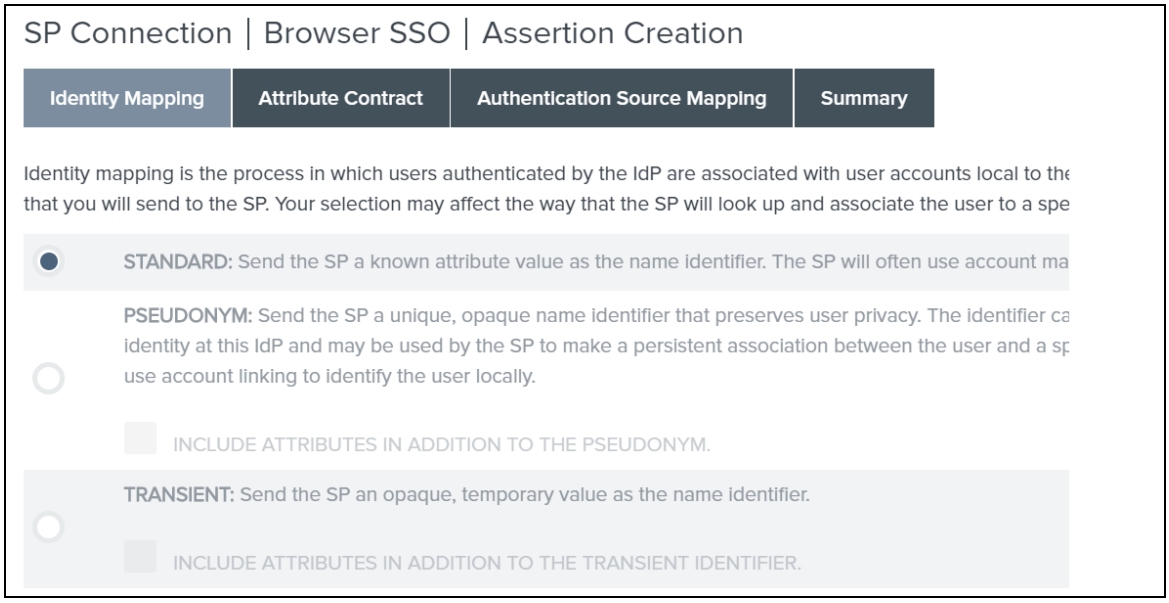
2. Click **Configure Browser SSO**.
3. Select the following SAML profiles:
   - Select IDP-INITITATED SSO
   - Select SP-INITITATED SSO

Figure 57 *SAML Profiles*



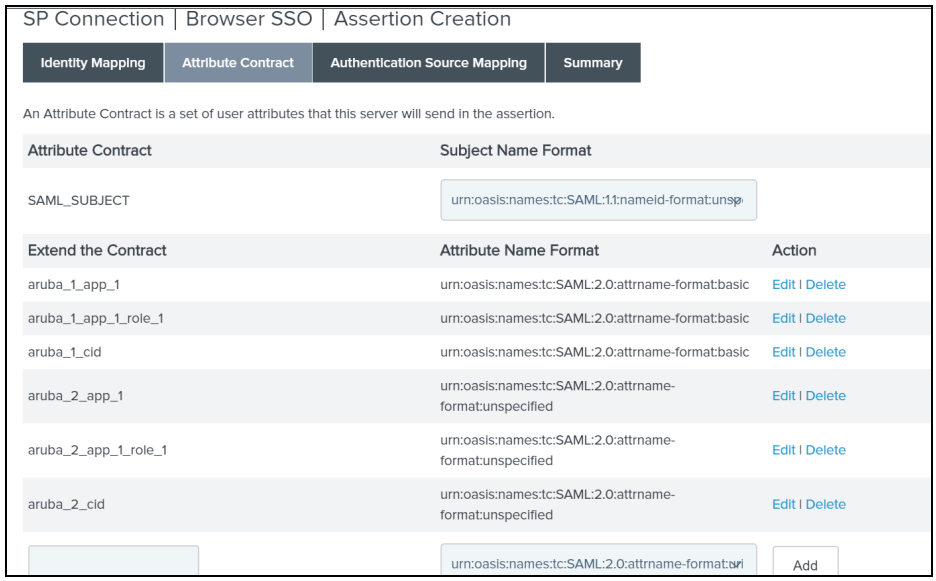
4. Click **Next**. The **Assertion Lifetime** tab opens.
5. Click **Next**. The **Assertion Creation** page opens.
   a. Click **Configure Assertion Creation**. The **Assertion Creation** wizard opens.

      Figure 58 *Assertion Creation Window*



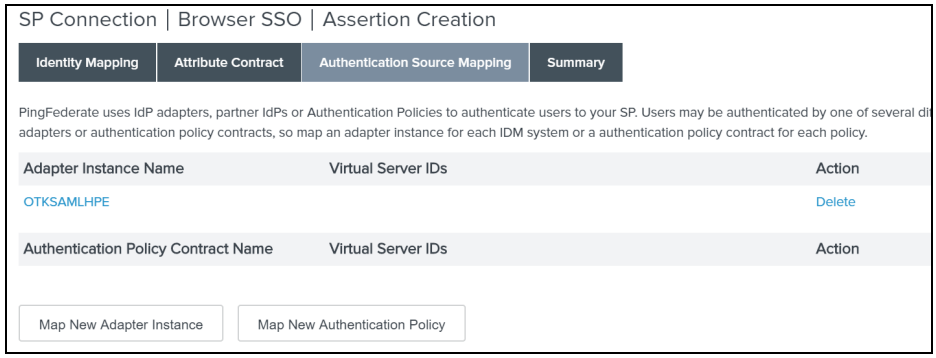
   b. Click **Next**. The **Attribute Contract** page opens.
   c. Add the SAML attributes in the SAML assertion. The IdP sends these attributes in the SAML Assertion.

Figure 59 *Attribute Contract*



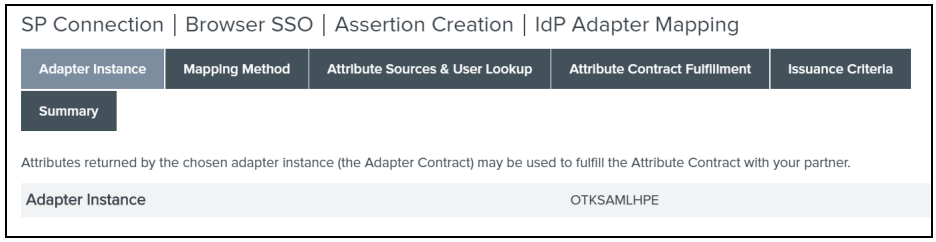
d. Click **Next**. The **Authentication Source Mapping** tab opens.

Figure 60 *Authentication Source Mapping*



e. Click **Map New Adapter Instance**. The adapter configuration screen opens.

Figure 61 *Adapter Insurance*



f. Complete the following configuration steps:

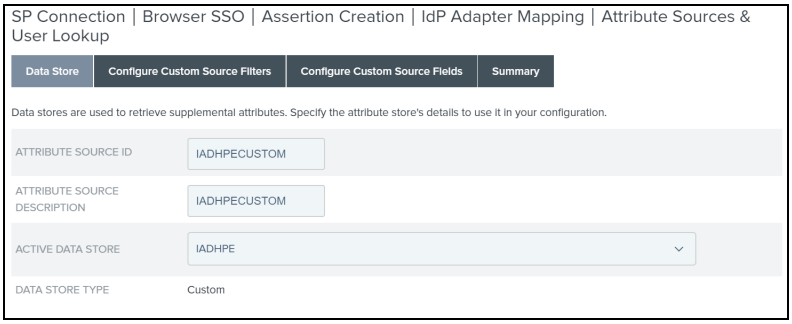
i. Click **Mapping Method** and select a mapping option.

Figure 62 *Mapping Method Selection*

ii. Click **Attribute Sources and User Lookup**

iii. To add a data source, click **Add Attribute Store** and add the data store ID as shown in the following figure:

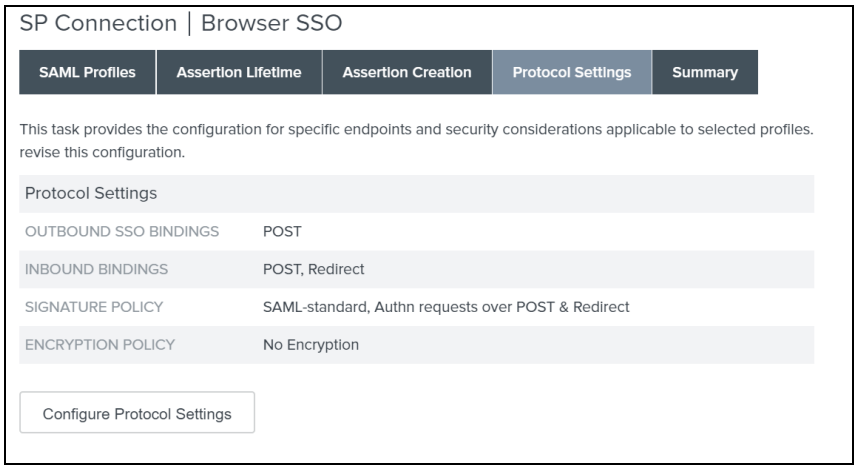
Figure 63 *Add Data Store ID*



iv. Click **Save**.

6. On the **SP Connections** > **Browser SSO Settings** page, click **Protocol Settings** to configure the Browser SSO Protocol Settings, SSO service URLs, and SAML bindings.

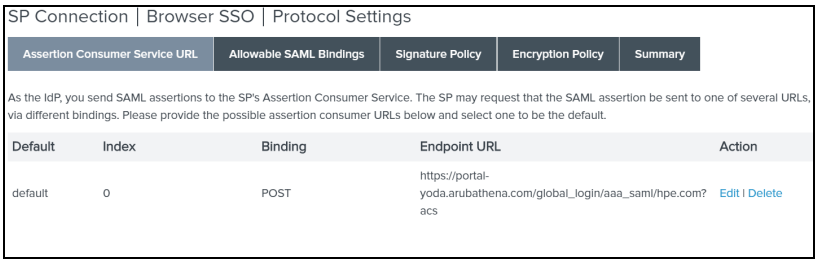
Figure 64 *Protocol Settings*



7. Click **Configure Protocol Settings** and complete the following steps:

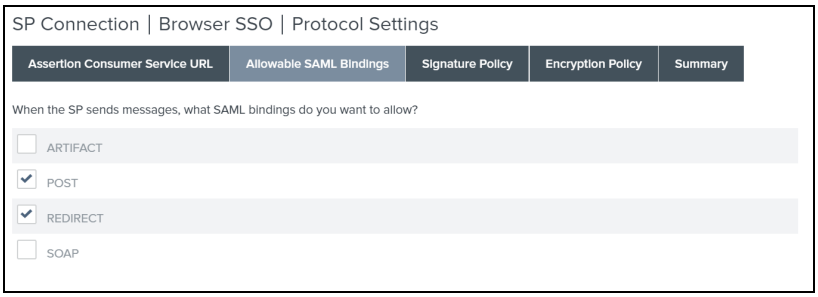
a. Verify the **Assertion Consumer Service URL**. The endpoint URLs for Redirect and Post bindings are both automatically populated from the metadata. If not, enter the URL manually. The URL will be the same for both bindings.

Figure 65 *Assertion Consumer Service URL Verification*



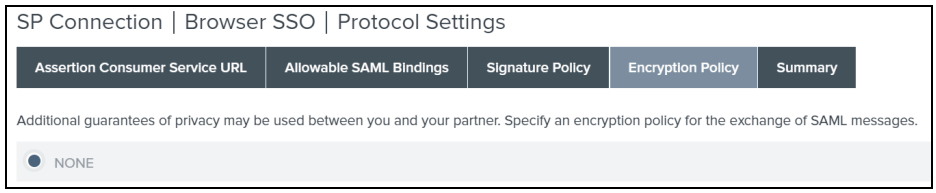
b. Click **Next**. The **Allowable SAML Bindings** tab opens.
c. Select **Post** and **Redirect**.

Figure 66 *SAML Bindings Selection*



d. Click **Next**. The **Encryption Policy Settings** tab opens.
e. Select **None**.

Figure 67 *Encryption Policy Settings*



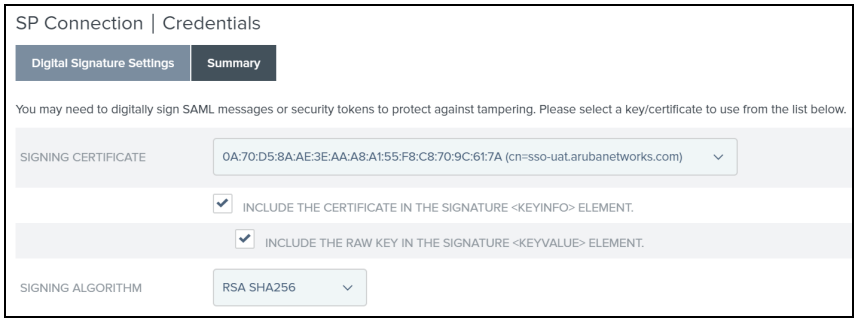
f. Click **Next**. Review the protocol setting.
g. Click **Done**.

Step 3:Configure Credentials

1. On the SP Connections page in the PingFederate administrative console, click **Credentials**.
2. Click **Configure Credentials**.
3. Click **Digital Signature Settings**.

4. Select the certificate to use for digital signature in SAML messages.

Figure 68 *Digital Signature Settings*



Step 4:Review Configuration

To review the configuration, click the **Activation & Summary** tab.

Step 5:SAML Authorization Profile in Aruba Central

For information on how to configure a SAML authorization profile, see Configuring SAML Authorization Profiles in Aruba Central.

Configuring Service Provider Metadata in ArubaClearPass Policy Manager

This procedure describes the configuration steps required for setting up ArubaClearPass Policy Manager as an IdP.

NOTE

ClearPass must be synced to NTP along with any other SAML SPs and IdPs. If clocks are out of sync, SAML will not function.

Before you Begin

- Go through the SAML SSO feature description to understand how SAML framework works in the context of Aruba Central.
- Ensure that you have access to the ClearPass Policy Manager instance.
- Ensure that you have downloaded the SAML metadata from Aruba Central.

Steps to Configure ClearPass Policy Manager as an IdP

To configure ClearPass as an IdP for providing SAML authentication and authorization services to Aruba Central, complete the following steps:

- Step 1:Configuring Enforcement Profile and Policies
- Step 2:Adding Roles
- Step 3:Mapping Roles to Enforcement Policies
- Step 4:Configuring an IdP Service
- Step 5:Uploading SP Metadata
- Step 6:Adding Local Users
- Step 7:Configuring SAML Authorization Profile in Aruba Central

Step 1:Configuring Enforcement Profile and Policies

To configure an enforcement profile:

1. Go to **Configuration > Enforcement > Profiles**.
2. Click **Add** to add a new enforcement profile. The **Enforcement Profiles** page is displayed.
3. In the **Profile** tab, select the template as **Generic Application Enforcement** from the **Template** drop-down list.
4. Enter a name and description for the profile in the **Name** and **Description** fields.
5. In the **Action** field, click and select **Accept** from the given options.
6. Click **Next**. The **Attributes** tab is displayed.
7. Click to add the attributes name and attributes value in the **Attributes Name** and **Attributes Value** fields. Ensure that you add Aruba-defined attributes and values. To know more about Aruba defined attributes, see Configuring Service Provider Metadata in IdP.
8. Click **Next**. The **Summary** tab is displayed.
9. In the **Summary** tab, check the information entered in the **Profile** and **Attributes** field and click **Save** to save the enforcement profile.

To configure an enforcement policy, complete the following steps:

1. Go to **Configuration > Enforcement > Policies**.
2. Click **Add** to add a new enforcement policy. The **Enforcement Policies** page is displayed.
3. Enter a name and description for the policies in the **Name** and **Description** fields.
4. In the **Enforcement Type** field, click and select **Application**.
5. From the **Default Profile** drop-down list, select the profile which you created.
6. Click **Next**. The **Rules** tab is displayed.
7. For configuring the rules, follow the steps mentioned in Step 3 below.
8. Click **Next**. The **Summary** tab is displayed.
9. In the **Summary** tab, check and validate the information and click **Save** to save the enforcement policy.

Step 2:Adding Roles

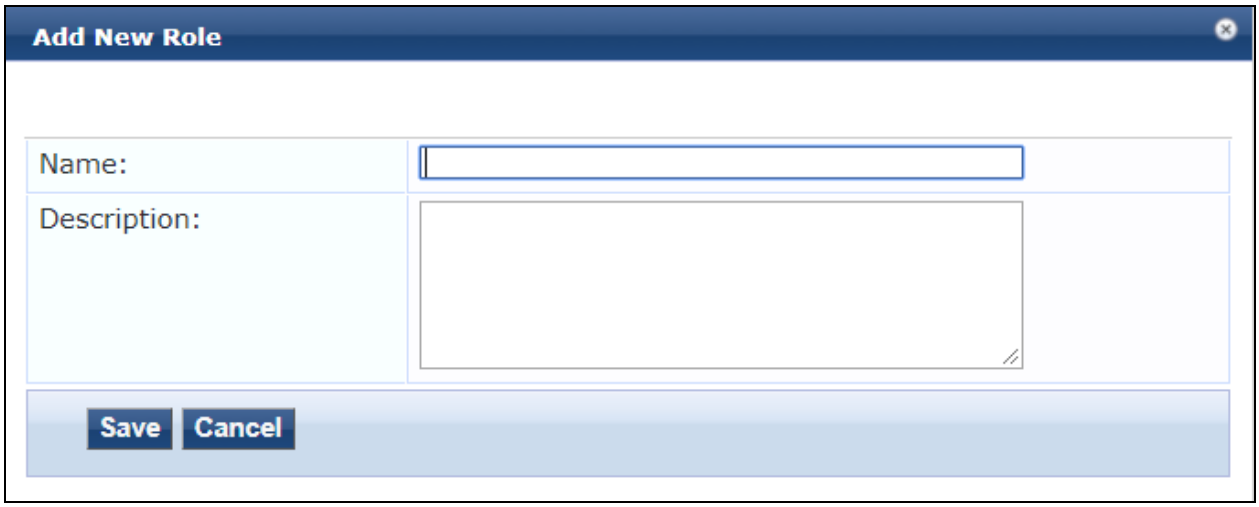
To add a user role:

1. Go to **Configuration > Identity > Roles**. The **Roles** page is displayed.
2. To add a new role, click **Add** in the **Roles** page.

Figure 69 *Configuring Roles*

3. Enter the role name and description in the **Name** and **Description** fields and click **Save** to save the role.

Figure 70 *Adding Role Information*

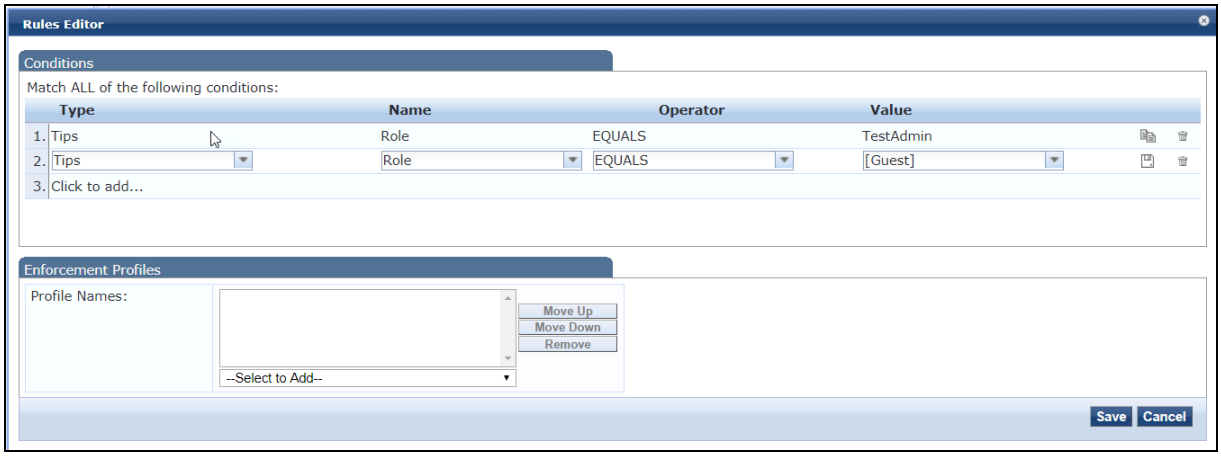


Step 3:Mapping Roles to Enforcement Policies

To map roles to enforcement policies:

1. Go to **Configuration > Enforcement > Policies**. The **Enforcement Policies** page is displayed.
2. Click and select the policy that you created.
3. Click the **Rules** tab and select **Add rule** to map a rule to the policy.
4. In the **Rules Editor** page, fill in the **Type**, **Name**, **Operator**, and **Values** as shown in the below example figure.

Figure 71 *Rules Editor Page*



5. In the **Profile Names** under **Enforcement Profiles**, select the profile that you created and click **Save**.
6. Click **Save**.

Step 4:Configuring an IdP Service

To configure an IdP service, complete the following steps:

1. Go to **Configuration > Services**. The **Services** Page is displayed.
2. From the **Services** page, click **Add** to add a new service.

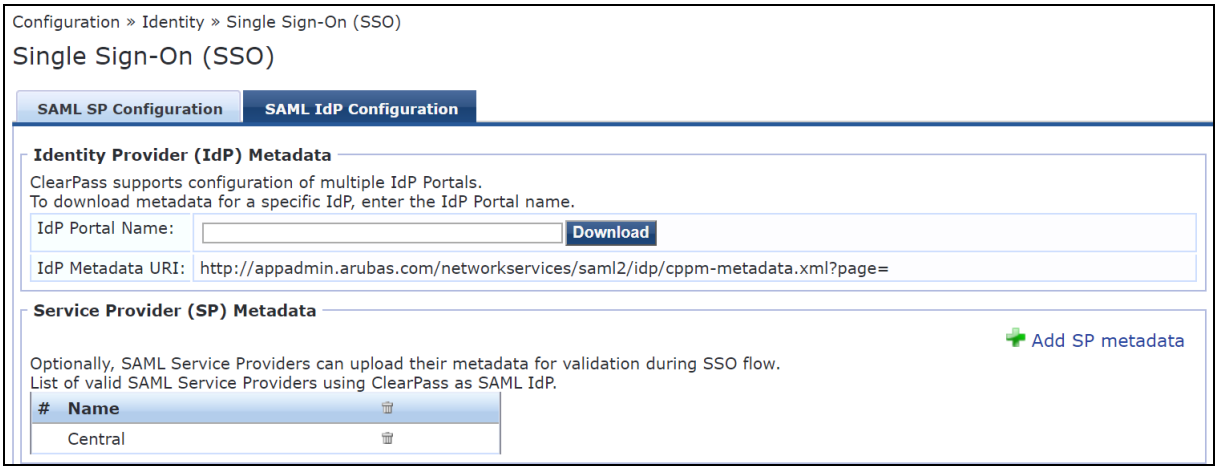
3. In the **Service** tab, select **Aruba Application Authentication** as a type of authentication from the **Type** drop-down list.
4. Enter a name Prefix and description for the services in the **Name** and **Description** fields respectively. This prefix is used to name all of the services and enforcement policies/profiles created by the wizard.
5. Optionally, you can enable the monitor mode and more options by clicking the **Monitor Mode** and **More Options** check boxes. By default, both the check boxes are not selected.
6. From the **Service Rule** option, select **ANY** or **All of the following conditions** to match the conditions.
7. You can define Type, Name, Operator, and Values for the condition by clicking and selecting from the respective drop-down lists.
8. Click **Next**. The **Authentication** tab is displayed.
9. Select **[Local User Repository] [Local SQL DB]** as an authentication source from **Authentication Sources** drop-down list.
10. Click **Next**. The **Roles** tab is displayed.
11. Keep the **Roles** tab to default values.
12. Click **Next**. The **Enforcement** tab is displayed.
13. Add an enforcement policy from the **Enforcement Policy** drop-down list.
14. Click **Next**. The **Summary** tab is displayed.
15. In the **Summary** tab, check if all the information in **Service**, **Authentication**, **Roles** , and **Enforcement** fields are correct and click **Save** to save the service.

Step 5:Uploading SP Metadata

To upload SP metadata, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Single Sign On**. The **Single Sign On** page is displayed.
2. Select the SAML authorization profile configured for the ClearPass IdP service, click **Show Metadata**, and download the metadata.
3. To upload SP metadata, go to **Configuration > Identity > Single Sign-On (SSO)**.
4. Click **SAML IdP Configuration** tab, and click **Add SP metadata**.
5. Set the SP name as Aruba Central and select the metadata file and click **Upload**.

Figure 72 *SAML IdP Configuration*

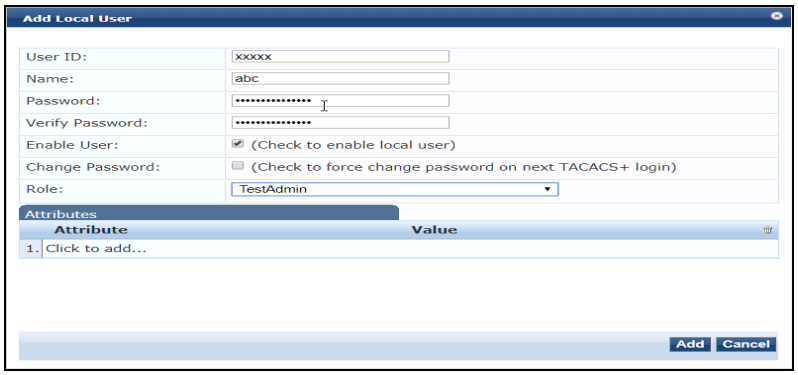


Step 6:Adding Local Users

To add local users, complete the following steps:

1. Go to **Configuration > Identity > Local Users**. The **Local Users** page is displayed.
2. In the **Local User**s page, click **Add**. The **Add Local User** page is displayed.
3. Enter the user id, name, and password in their respective fields.
4. Enter the password again to verify password in the **Verify Password** field.
5. By default, the **Enable User** check box is selected.
6. Select the **Change Password** check box if you want to force change the password on next user login. By default, the check box is not selected.
7. Select the role from the **Role** drop-down list and click **Add** to add the user. Below is an example figure for adding user:

Figure 73 *Adding a Local User*



Step 7:Configuring SAML Authorization Profile in Aruba Central

For information on how to configure a SAML authorization profile, see Configuring SAML Authorization Profiles in Aruba Central.

Configuring Service Provider Metadata in G Suite

This procedure describes the configuration steps required for setting up service provider metadata in G Suite.

Before you Begin

- Go through the SAML SSO feature description to understand how SAML framework works in the context of Aruba Central.
- Ensure that you have a domain and administrator privileges access to the G Suite. For more information, see G Suite Admin Help.
- Ensure that you have a verified user in Aruba Central.
- Ensure that you have downloaded the SAML metadata from Aruba Central.

Steps to Configure Service Provider Metadata in Google Admin Console.

To configure Google Admin Console for providing SAML authentication and authorization services to Aruba Central, complete the following steps:

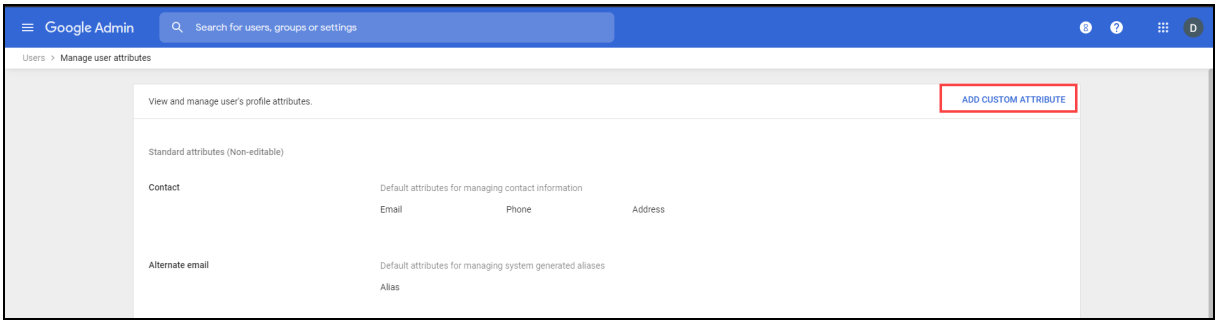
- Step 1:Add Custom Attributes
- Step 2:Add new user
- Step 3:Add values to custom attributes
- Step 4:Set up Custom SAML app
- Step 5:Turn on SSO to your new SAML app

Step 1:Add Custom Attributes

To add custom attributes in Google Admin:

1. In the **Google Admin console**, go to **Users > More > Manage custom attributes**. The Manage user attributes page is displayed.
2. At the top right corner, click **Add Custom Attribute**.

Figure 74 *Manage User Attributes*



3. In the **Add custom fields** pop-up window, configure the parameters as per the following table:

Parameter	Description
Category	Enter a name for the category you want to add.
Description	Optionally, enter a description for the category.
Custom fields	Configure the custom fields as per the following: ■ **Name**— Enter the label you want to display on the user's account page. ■ **Info type**— Select one of the following from the drop-down list: ◦ Text ◦ Whole Number ◦ Yes or No ◦ Decimal number ◦ Phone ◦ Email ◦ Date ■ **Visibility**— Select one of the following from the drop-down list: ◦ Visible to user and admin ◦ Visible to organization ■ **No. of values**— Select one of the following from the drop-down list: ◦ Multi-Value ◦ Single-value **NOTE:** ■ You cannot edit the **info type** and **No. of values** once you have created the custom attribute. ■ You can add multiple numbers of custom attributes in the **Custom fields**. Make sure that you add the Aruba supported attributes in the **Name** field. For more information on Aruba supported attributes, see Configuring Service Provider Metadata in IdP.

4. Click **Add** to finish adding the custom attributes.

Step 2:Add new user

To add a new user in the Google Admin console, complete the following steps:

1. In the **Google Admin console**, go to **Users > Add new user**. The **Add new user** page is displayed.
2. To add an image for the user, click **Add photo** and select the image file from the storage. You can also add the image later if you do not have it ready.
3. Fill the account information as per the following table:

Parameter	Description
First name	Enter the first name of the user.
Last name	Enter the last name of the user.
Primary email	Enter the primary email of the user.

Parameter	Description
Organization unit	The field gets auto populated.
Secondary email	Optionally, enter the secondary email of the user
Phone number	Optionally, enter the phone number of the user.

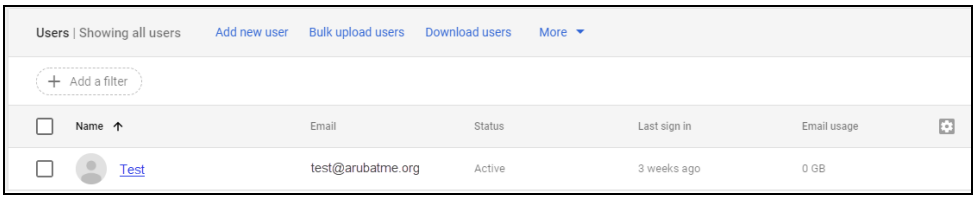
4. You can either generate the password automatically by turning on the toggle button or enter the password manually. By default, you have to enter the password manually. While creating the password, make sure that the password is of at least 8 characters.
5. Optionally, turn on the toggle to ask the user to change the password at the next sign-in.
6. Click **Add New User**.

Step 3:Add values to custom attributes

You can add or update values for custom attributes on the **User information page** for an user. To add values to custom attributes:

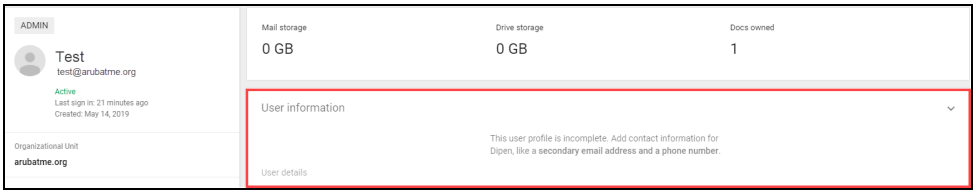
1. In the **Google Admin console**, click **Users**. The user page is displayed.

   Figure 75 *Users Page*



2. From the users list, find the user by using a filter or Search bar. For more information on how to find the user, see Find a user account.
3. Click **User information**.

   Figure 76 *User Information*



4. Click the **Aruba-Attributes** section to edit.

5. Add or change values to custom attributes as shown in the following example figure:

Figure 77 *Editing Aruba-Attributes*

6. Click **Save**.

NOTE

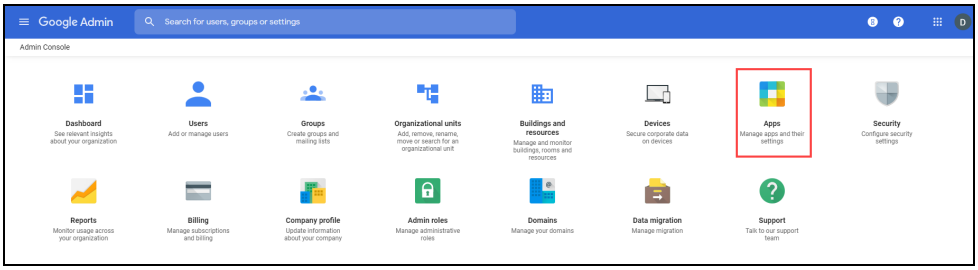
You can only assign roles to the user which are already existing and valid in Aruba Central.

Step 4:Set up Custom SAML app

To setup own custom SAML App:

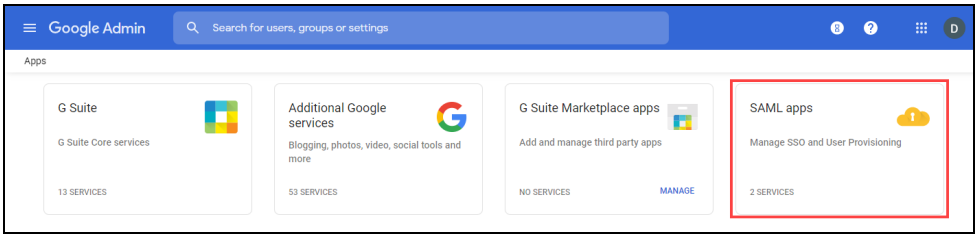
1. Log in to G Suite. The Admin console is displayed.

Figure 78 *Google Admin Console*



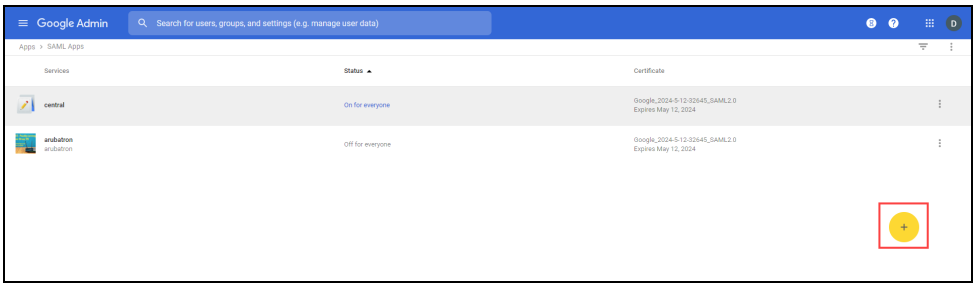
2. From the Admin Console main screen, click **Apps**. The **Apps** page is displayed.
3. From the **Apps** screen, click **SAML apps**. The **SAML apps** page is displayed.

Figure 79 *SAML Applications*



4. Click the **+** sign at the bottom of the screen to add a new SAML app (or, you can edit an existing one). The **Enable SSO for SAML Application** window page is displayed.

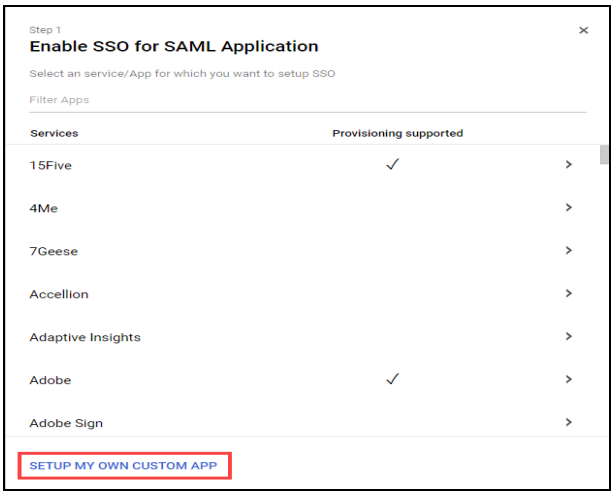
Figure 80 *Enable SSO for SAML Application*



5. Click **Setup My Own Custom App**.

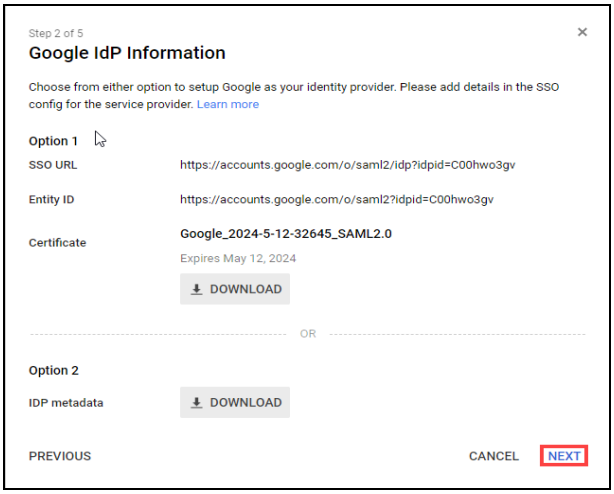
   The **Google IdP Information** window opens and the **SSO URL** and **Entity ID** fields automatically populate.

Figure 81 *Setup Custom Application*



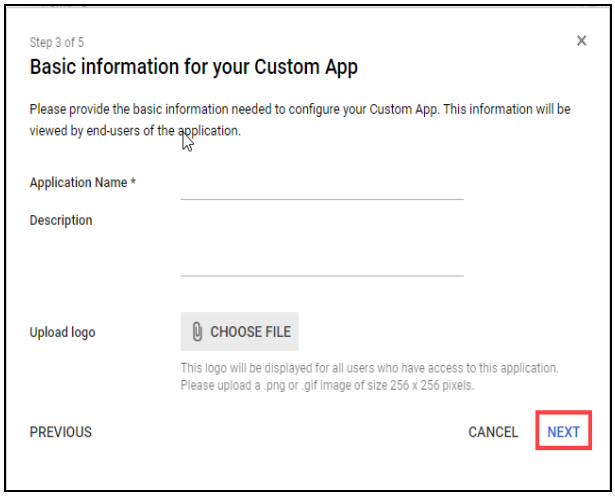
6. Get the setup information needed using one of these methods:
   a. Copy the **SSO URL** and **Entity ID** and download the Certificate.
   b. Download the **Idp metadata**.

Figure 82 *Google IdP Information*



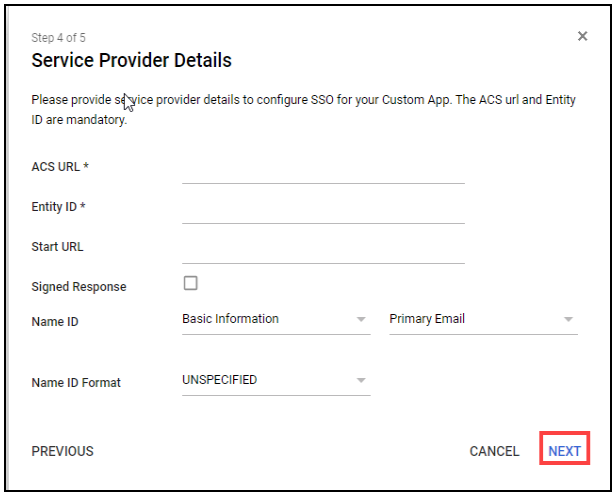
7. In a separate browser tab or window, sign in to Aruba Central and enter the information you copied in step 6 above into the appropriate SSO configuration page, then return to the Admin console. For information on how to configure a SAML authorization profile, see Configuring SAML Authorization Profiles in Aruba Central.
8. Click **Next**.
9. In the **Basic Information for Your Custom App** window, add an application name and description.
10. Optionally, upload a PNG or GIF file to serve as an icon for your custom app. The icon image should be of size 256 x 256 pixels.

Figure 83 *Configuring Basic Information*



11. Click **Next**.
12. In Aruba Central, select the SAML authorization profile configured for the domain, click **show meta data**, download the metadata, and return to the G Suite Admin console.
13. In the **Service Provider Details** window, enter an **ACS URL**, **Entity ID**, and **Start URL** (if needed) for your custom app. These values are all provided from the downloaded metadata.
14. By default, the **Signed Response** check box is not selected.
15. The **Name ID** and **Name ID Format** fields are automatically populated.

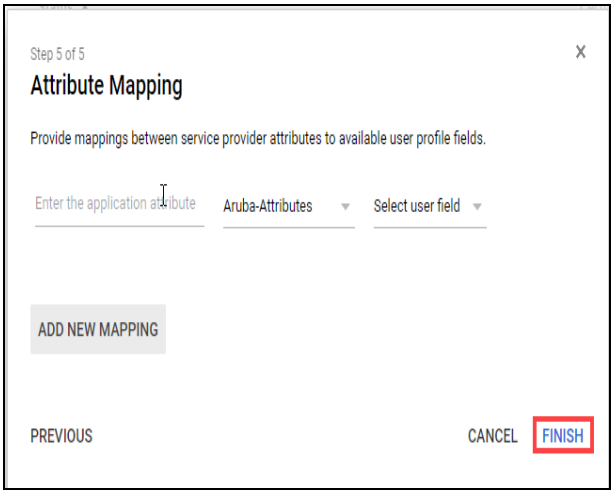
Figure 84 *Service Provider Details*



16. Click **Next**.

17. Optionally, click **Add New Mapping** and enter a new name for the attribute you want to map.
18. In the drop-down list, select the category and user attributes to map the attribute from the Google profile.

Figure 85 *Attribute Mapping*



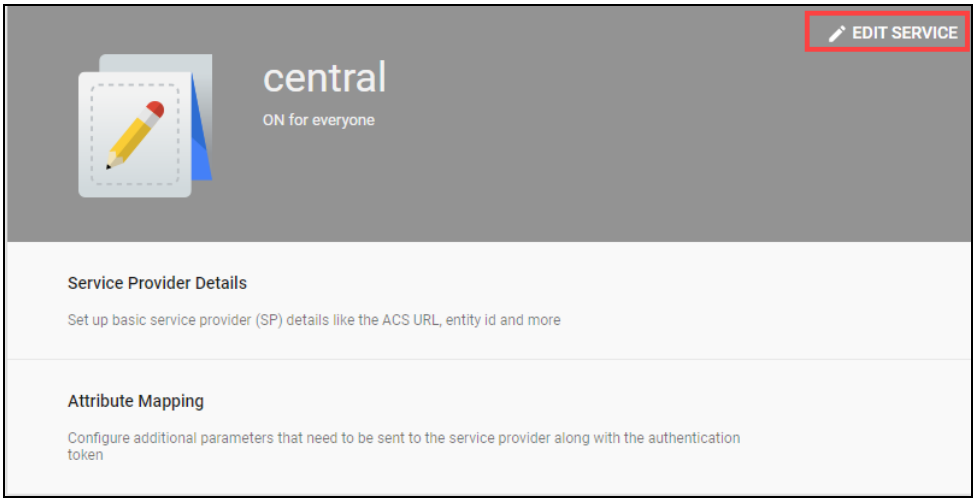
19. Click **Finish**.

Step 5:Turn on SSO to your new SAML app

To turn on SSO in your SAML app:

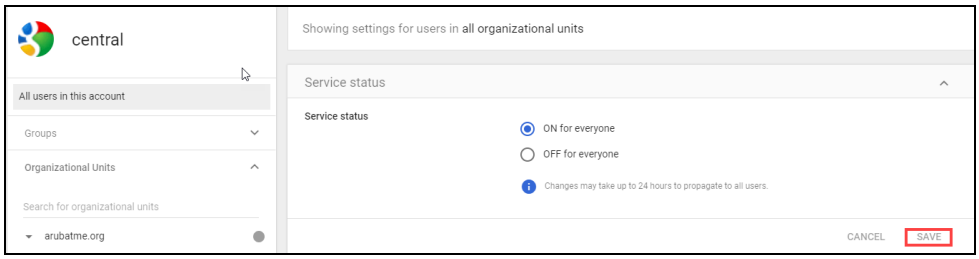
1. In the **Google Admin console**, go to **Apps > SAML apps** and select the SAML app that you created.
2. At the top right corner of the gray box, click **Edit Service**.

Figure 86 *Editing a Service*



3. To turn on or off a service for everyone in your organization, click **On for everyone** or **Off for everyone** from the Service status option, and click **Save**.

Figure 87 *Configuring All Organizational Units*



Viewing Federated Users in Aruba Central

If your Aruba Central account has SAML SSO users, Aruba Central displays these users as federated users.

To view a list of federated users in your account:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
   The **Users & Roles** page opens.
2. In the **Users** table, use the filter in **User Type** column to sort the table by federated users.

Viewing Audit Logs for Federated Users in Aruba Central

The federated or the SAML SSO user activity is logged in Aruba Central as audit trails.

To view the audit logs for federated users, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**.
   The **Audit Trail** page is displayed.
2. To filter audit logs by federated user activity, click the filter in the **Category** column and select **User Activity**.

NOTE

To view audit logs for the SAML authorization profiles, in the **Audit Trail** page, select **SAML Profile** from the **Classification** filter.

Converting System Users to Federated Users

The system users in Aruba Central use the standard authentication method, whereas the federated users sign in to Aruba Central using the SAML-based SSO authentication method.

If your business requires you to move system users from the standard authentication method to SAML-based authentication, follow the steps described in this page.

Before you Begin

Check if the user is accessing Aruba Central application using the web application, API Gateway, or the mobile app.

NOTE

Aruba does not support SAML-Based SSO logins for Aruba Central API Gateway, Aruba Installer, and Aruba Central mobile apps; Hence, it is recommended that you do not convert the API Gateway and mobile app user profiles to federated users.

Migrating Aruba Central Web Application Users to Federated User Profiles

To move system users of the Aruba Central web application users to SAML-based authentication method:

1. Back up the user profiles in the domain that is being migrated to SAML-based authentication framework. To view and create a backup of a list of existing user profiles, access the **[GET] /platform/rbac/v1/users** NB API.
2. Restore the current users in the system along with role and scope information defined for each user. To restore user profiles in bulk, use the **[POST] /platform/rbac/v1/bulk_users** API in the same domain.
3. Validate the configuration for one user.
4. If the migration is successful, remove the remaining system users in the domain, by using one of the following methods:
   - In the **Account Home** page, under **Global Settings**, click **Users & Roles**. page in the UI, select the user profile that you want to delete and click the delete icon.
   - Access the **[DELETE] /platform/rbac/v1/bulk_users** API and adding user account names in **Parameters** section.

   Example

   ```
   Param –
   [
   "user1@gmail.com","user2@gmail.com","user3@gmail.com"
   ]
   ```

5. Ensure that there is at least one system admin user in the domain that you are migrating to SAML-based SSO authentication framework.
6. Validate the SSO workflow for the users that you just migrated to the SAML-based SSO authentication method.

Enabling NB API Access for Federated Users

To enable NB API access for federated users:

1. Log in to Aruba Central web application using the SAML-based SSO authentication method.
2. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
3. Click **My Apps& Tokens**.
4. Click **+ Add Apps & Tokens** and generate an OAuth token.

For more information on generating tokens and API Gateway bootstrapping, see Aruba Central API Gateway Documentation.

Troubleshooting SAML SSO Authentication Issues

This section provides troubleshooting guidelines and tips to help Aruba Central administrators to diagnose and fix issues related to SAML SSO authentication.

Installing SAML Tracer on Web Browsers

To view SAML trace logs, you can install SAML Tracer on your web browsers. To install SAML Tracer:

- Mozilla FireFox— Go to https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/.
- Google Chrome—Go to https://chrome.google.com/webstore/category/extensions.

Viewing SAML Trace Logs

To view the SAML trace logs, open the SAML Tracer add-on in the web browser. SAML Tracer records all HTTP requests sent or received by your browser. If the HTTP request contains SAML, the **SAML** tab in the SAML Trace window records the trace logs.

For example, when the SAML user logs in, you can verify the SAML attributes that are recorded. Note the key elements in the SAML attributes output when diagnosing a SAML authentication error.

```
<Subject> <NameID>johnnyadmin1@adfsaruba.com</NameID> <SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<SubjectConfirmationData InResponseTo="ONELOGIN_
f937f6f66c3d29c4713eee99e09fd31e23ae6fec"
NotOnOrAfter="2019-06-14T11:57:47.883Z"
Recipient="https://portal-yodaacdc.arubathena.com/global_login/aaa_
saml/adfsaruba.com?acs"
/> </SubjectConfirmation> </Subject> <Conditions NotBefore="2019-06-
14T11:52:47.881Z"
NotOnOrAfter="2019-06-14T12:52:47.881Z"
> <AudienceRestriction> <Audience>https://portal-yodaacdc.arubathena.com/global_
login/aaa_saml/adfsaruba.com/metadata</Audience>
</AudienceRestriction> </Conditions> <AttributeStatement>
<Attribute Name="aruba_1_cid">
<AttributeValue>ab8eeb91a8434025a3ecbdad9b8af705</AttributeValue> </Attribute>
<Attribute Name="aruba_1_app_1"> <AttributeValue>central</AttributeValue>
</Attribute>
<Attribute Name="aruba_1_app_1_role_1"> <AttributeValue>admin</AttributeValue>
</Attribute>
<Attribute Name="aruba_1_app_1_role_1_tenant">
<AttributeValue>readonly</AttributeValue> </Attribute>
```

Troubleshooting Tips for Most Common Errors

Error 1—A blank page is displayed when the SAML user is redirected to the IdP server

- **Description**: When a SAML user is redirected to the IdP server for authentication, the IdP server does not return the SAML response and displays a blank page.
- **Cause**: This issue may occur when the Service Provider metadata for Aruba Central is not configured on the IdP server.
- **Resolution**: Configure Service Provider metadata for your Aruba Central account in the IdP server.

Error 2—The SAML user is logged out of Aruba Central after logging in to IdP

- **Description**: The SAML user gets logged out of Aruba Central after logging in to the IdP server and the following error code is displayed in the browser:

  error_code=INVALID+EXTERNAL+AUTH+REQUEST
- **Reason**: This issue may occur when the customer ID for the SAML user is not successfully retrieved from the IdP server.
- **Solution**: Verify the trace logs, check the IdP configuration for customer ID details, and ensure that the IdP sends the correct customer ID.

```
<NameID>johnnyadmin1@adfsaruba.com</NameID> <SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<SubjectConfirmationData InResponseTo="ONELOGIN_
```

```
c000669424a538ea0f4793ec38dab3b57a635efb"
NotOnOrAfter="2019-06-14T10:06:20.153Z"
Recipient="https://compass.arubathena.com/global_login/aaa_saml/adfsaruba.com?acs"/>
 </SubjectConfirmation> </Subject> <Conditions NotBefore="2019-06-14T10:01:20.151Z"
NotOnOrAfter="2019-06-14T11:01:20.151Z">
<AudienceRestriction>
<Audience>https://compass.arubathena.com/global_login/aaa_
saml/adfsaruba.com/metadata</Audience> </AudienceRestriction> </Conditions>
<AuthnStatement AuthnInstant="2019-06-14T10:01:19.749Z"
SessionIndex="_400366f7-75dc-4423-909c-2b3dc4e9fd9c"> <AuthnContext>
```

Error 3—The web browser displays an error message when a SAML user is redirected to Aruba Central after logging in to IdP

- **Description**: The web browser displays the following error message when the SAML user logs into IdP and is redirected to Aruba Central:

  ```
  error_code "FAILED EXTERNAL AUTH - SAML ACS PROCESSING"
  message "NameID not found in the assertion of the Response"
  ```

- **Cause**: This issue may occur when the **name-id** attribute is not configured in the IdP server.
- **Solution**: Verify the trace logs, check the IdP configuration, and ensure that the **name-id** attribute maps to the user's email address.

Error 4—The web browser displays a 404 error message when a SAML user is redirected to Aruba Central after logging into IdP

- **Description**: The web browser displays the following error message when a SAML user is redirected to Aruba Central after logging into IdP:

  ```
  The requested URL was not found on the server. If you entered the URL manually
  please check your spelling and try again.
  status_code 404
  ```

- **Cause**: This issue may occur due to one of the following reasons:
  - The **name-id** attribute does not contain user's email address.
  - The **app-id** attribute is not configured as **Central** in IdP.
  - The **role** attribute returned by the IdP is not configured in Aruba Central.
  - The **group** attribute in the IdP server is mapped to a group that is not available in your Aruba Central account.
  - IdP returns a tenant role for the SAML user of a standalone enterprise account.
- **Solution**: Verify the trace logs, check your Aruba Central deployment setup and the IdP configuration, and ensure that the correct values are configured for these attributes in the IdP server.

Error 5—Although the role attribute is not configured in IdP, the SAML user is assigned a readonly role

- **Description**: Although the role attribute is not configured in the IdP server, the SAML user is assigned a **readonly** role after logging in to Aruba Central.

- **Cause**: By default, Aruba Central assigns **readonly** role for SAML users if role attribute is not configured in IdP.
- **Solution**: If you want the SAML user to have a specific role assigned, configure the role attribute for the user in the IdP server.

Error 6—A SAML user was able to log in to Aruba Central earlier, but cannot access Aruba Central now

- **Description**: The SAML user who was able to log in to Aruba Central earlier gets the following message during login:

```
The requested URL was not found on the server. If you entered the URL manually
please check your spelling and try again.
status_code    404
```

  This issue is observed when the customer ID of a SAML user is changed from an MSP to its tenant or from a tenant to its MSP in the IdP server.
- **Cause**: This issue occurs when the Aruba Central user database already has a user entry for the SAML user who tries to log in to Aruba Central after the customer ID modification in the IdP server.
- **Solution**: In the **Account Home** page, under **Global Settings** click **Users & Roles** page and delete the SAML user in Aruba Central. Verify if the user entry is removed from the user database.

Error 7—The web browser displays SAML authentication error message when a SAML user tries to log in to Aruba Central

- **Description**: When a SAML user tries the log in to Aruba Central, the following error message is displayed:

```
FAILED EXTERNAL AUTH - SAML ACS PROCESSING
message 0 "invalid_response"
```

- **Cause**: This issue may occur due to certificate mismatch.
- **Solution**: Verify the SAML authorization profile configured in Aruba Central and ensure that the correct certificate is uploaded.

Error 8—The Aruba Central login page is displayed for the SAML user instead of the IdP login page

- **Description**: When a SAML user tries to access Aruba Central, the user is redirected to the Aruba Central login page instead of the IdP login page.
- **Cause**: This issue may occur when the SAML user is configured as a system user in Aruba Central.
- **Solution**: If a SAML user is added as a system user in Aruba Central, delete the system user entry for the user in Aruba Central.

Two-Factor Authentication

Aruba Central now supports two-factor authentication for both computers and mobile phones to offer a second layer of security to your login, in addition to password. When two-factor authentication is enabled on a user account, the users can sign in to their Aruba Central account either through the mobile app or the

web application, only after providing their password and the six-digit verification code displayed on their trusted devices.

When two-factor authentication is enabled at the customer account level, all the users belonging to the customer account are required to complete the authentication procedure when logging in to Aruba Central. If a user account is associated with multiple customer accounts and if two-factor authentication is enabled on one of these accounts, the user must complete the two-factor authentication during the login procedure.

If two-factor authentication is enabled on your accounts, you must install the Google Authenticator app on your devices such as mobile phones to access the Aruba Central application. When the users attempt to log in to Aruba Central with their credentials, the Google Authenticator app provides a six-digit verification code to complete the login procedure.

Installing the Google Authenticator App

For two-factor authentication, ensure that the Google Authenticator app is installed on your mobile device.

During the registration process, the Aruba Central application shares a secret key with the mobile device of the user over a secure channel when the user logs in to Aruba Central. The key is stored in the Google Authenticator app and used for future logins to the application. This prevents unauthorized access to a user account as this authentication procedure involves two-levels for secure transaction.

When you register your mobile device successfully, the Google Authenticator app generates a six-digit token for the second level authentication. The token is generated every thirty seconds.

Enabling Two-factor Authentication for User Accounts

To enable two-factor authentication, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
   The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Two-Factor Authentication (2FA)** toggle button to the right. The two-factor authentication is enabled for all the users associated with the account.

Two-factor Authentication for Aruba Central Web Application

When two-factor authentication is enabled for a customer account, the users associated with that customer account are prompted for two-factor authentication when they log in to Aruba Central.

To complete two-factor authentication, perform the following actions:

1. Access the Aruba Central website.
2. Log in with your credentials. If two-factor authentication is enforced on your account, the two-factor authentication page opens.
3. Install the Google Authenticator app on your mobile device if not already installed.
4. Click **Next**.
5. If this is your first login since two-factor authentication is enforced on your account, open Google Authenticator on your mobile device.
6. Scan the QR Code. If you are unable to scan the QR code, perform the following actions:
   a. Click the **Problem in Reading QR Code** link. The secret key is displayed.
   b. Enter the secret key in the Google Authenticator app.
   c. Ensure that the **Time-Based** parameter is set. Aruba Central is added to the list of supported clients and a six-digit token is generated.
7. Click **Next**.

8. Enter the six-digit token.
9. Select the **Remember 2FA for 30 Days** check box if you want the authentication to expire only after 30 days.
10. Click **Finish**.

Two-factor Authentication for the Aruba Central Mobile App

Two-factor authentication must first be enabled for your account. If two-factor authentication is not enabled, you log in to the application directly after a successful SSO authentication.

To log in to Aruba Central app on your mobile device, perform the following actions:

1. Open the Aruba Central app on your mobile device.
2. Enter your username and password and click **Log in**. If the registration process is pending, an error message is displayed:

   Please register for two-factor authentication in our web app to ensure secured authentication.
3. Enter the token. On successful authentication, the Aruba Central app opens.

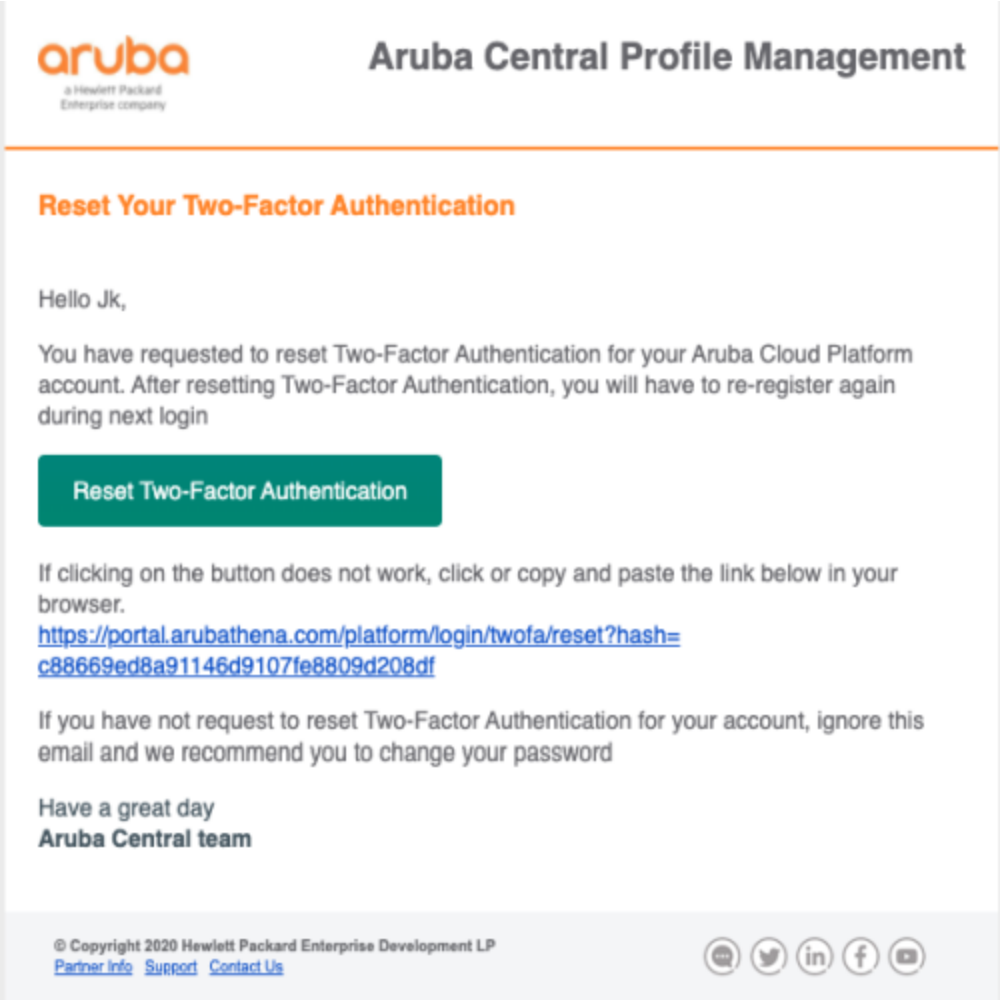
Registering a New Mobile Device

If you have changed your mobile device, you need to install Google Authenticator app on your new device and register again using a web browser on your Desktop for two-factor authentication.

To register your new mobile device, complete the following steps:

1. Log in to Aruba Central web application. The two-factor authentication page is displayed.
2. Click the **Changed Your Mobile Device?** link.
3. To register your new device and receive a reset email with instructions, click **Send 2FA Reset Email**. A reset email with instructions will be sent to your registered email address:

Figure 88 *Reset Tow-Factor Authentication Email*



4. Follow the instructions in the email and complete the registration.

Support Access

Aruba technical support may ask you to enable **Support Access** to debug issues. After you enable **Support Access**, the Aruba support team can access your Aruba Central account remotely. Only users with administrator role can enable **Support Access**.

Enabling Support Access

To enable **Support Access**, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
   The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Support Access** toggle button to the right.
3. Set password expiry by selecting the number of days and click **Get Password**. A new password is generated.
4. Copy the password and share it with the Aruba technical support representative.

Disabling Support Access

After the remote support session is complete, do the following to disable **Support Access**:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
   The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Support Access** toggle button to the left.

Managing License Keys

A license key is an alphanumeric string with 9 to 14 characters; for example, PQREWD6ADWERAS. Aruba Central can manage a device only if the corresponding license key of the device is added to Aruba Central. License keys can either be evaluation license keys that map to evaluation licenses or paid license keys that map to paid licenses. The evaluation license key is valid for 90 days.

To use Aruba Central for managing, profiling, analyzing, and monitoring your devices, you must ensure that you have a valid license key and that the license key is listed in the **Account Home** > **Global Settings** > **Key Management** page.

Evaluation License Key

The evaluation license key is enabled for trial users by default. It allows you to add up to a total of 60 devices. For an evaluation user, a set of evaluation keys is generated.

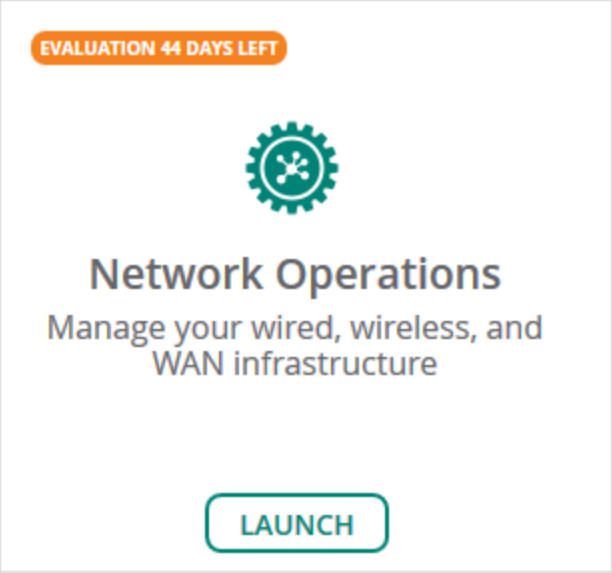
The **Account Home** > **Global Settings** > **Key Management** page displays the license expiration date in the **Key Management** table. You will receive license expiry notifications through email 30, 15, and 1 day before the license expiry and on day 1 after the license actually expires. The number of days left for license expiry is also displayed in the respective app under the **Apps** section of the **Account Home** page.

Upgrading to a Paid Account

If you have purchased a license for an AP, a switch, or a gateway, then upgrade your account by completing the following steps:

1. On the **Account Home** page, in the **Network Operation** app, click the link that shows the number of days left for the evaluation to expire.

   Figure 89 *Network Operations Evaluation Account*



The **Add a New License** window is displayed.

2. Enter the new license key that you purchased from Aruba.
3. Click **Add License**.

After you upgrade your account, you can add more devices, enable services, and continue using Aruba Central.

Paid License Key

If you have purchased a license key, you must ensure that your license key is added to Aruba Central. If you are logging in for the first time, Aruba Central prompts you to add your license key to activate your account. Ensure that you add the license key before on-boarding devices to Aruba Central.

The **Account Home** > **Global Settings** > **Key Management** page displays the license expiration date. You receive the license expiry notifications through email 90, 60, 30, 15, and 1 day before expiry and two notifications each day on day 1 and day 2 after the license expires.

When you upgrade or renew your license, or purchase another license key, you must add the key details in the **Account Home** > **Global Settings** > **Key Management** page to avail the benefits of the new license.

Adding a License Key

1. On the **Account Home** page, under **Global Settings**, click **Key Management**.

   The **Key Management** page is displayed.
2. Enter your license key.
3. Click **Add Key**.

   The license key is added to Aruba Central and the contents of the license key are displayed in the **Manage Keys** table. Review the license details.

   If you add a **Device Management** token, the key is listed in the **Convert Deprecated Licenses** page. For more information, see Converting Legacy Tokens to New Licenses.

Viewing License Key Details

To view the license key details, navigate to **Account Home** > **Global Settings** > **Key Management**.

The **Key Management** page provides information about license keys available for the devices and their details such as license tier, expiration date, and quantity of licenses. The **Key Management** sections are described in the next topics.

License Summary

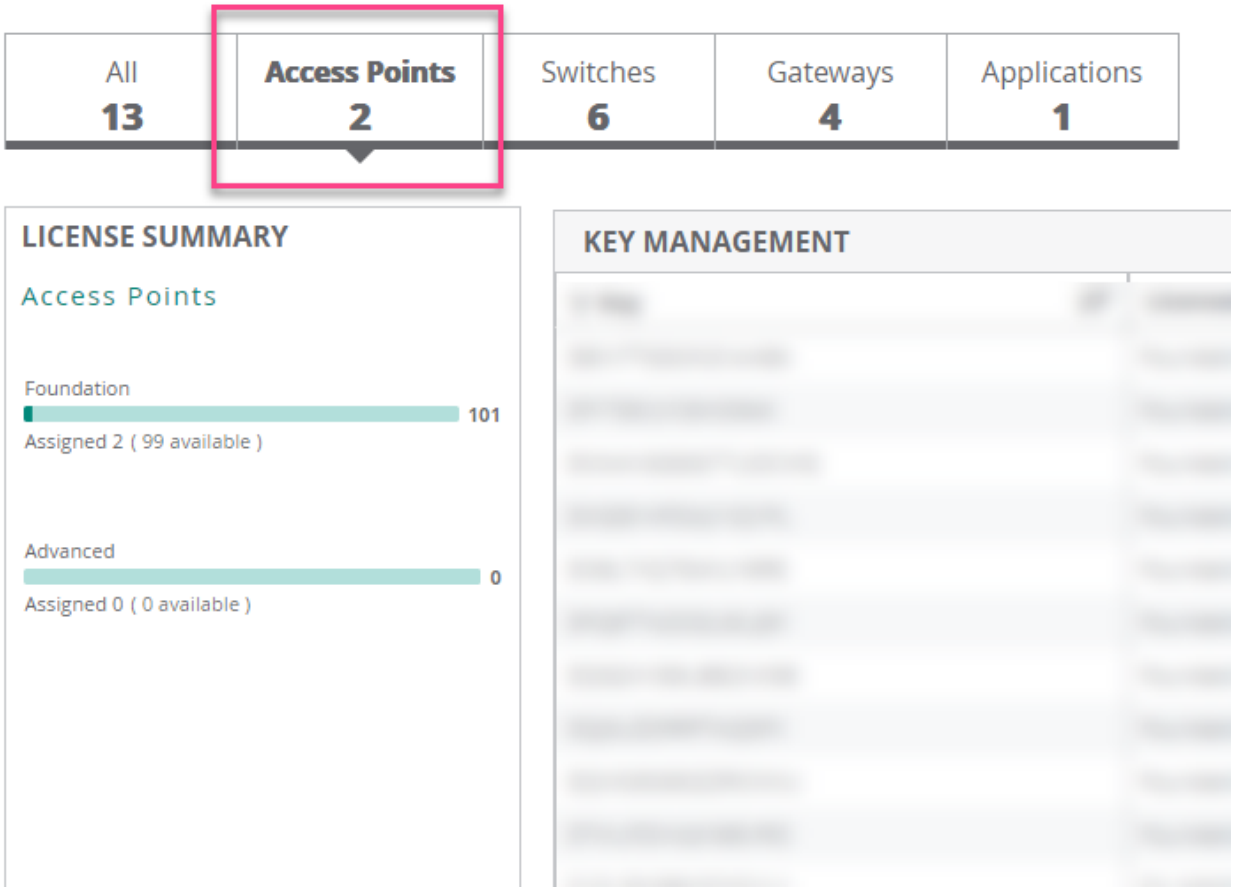
For the selected device type or app, or for all devices, the **License Summary** section lists down all the available licenses, the total number of licenses, the number of assigned licenses, and the number of unassigned licenses.

The available devices are APs, switches, and gateways.

The **Applications** tab currently lists the license keys for the Network Operations app and the Clear Pass Device Insight app (where applicable).

Click a single or multiple licenses in the **License Summary** section to display the details of the license type in the **Key Management** table. To unselect the license, click the selected license type again.

Figure 90 *License Summary Details for APs*



The preceding screenshot shows the following details:

- Total number of AP Foundation Licenses = 101
- Assigned AP Foundation Licenses = 2
- Unassigned AP Foundation Licenses = 99
- Total number of AP Advanced Licenses = 0

Key Management Table Details

The following table describes the contents of the **Key Management** table:

Table 49: *License Key Details*

Data Pane Item	Description
Key	License key number.
License Tier Type	Type of the license. Aruba Central supports the following types of licenses: ■ Foundation ■ Advanced The Foundation and Advanced licenses for APs, switches, and SD-WAN gateways are different from each other and cannot be used interchangeably.
Expiration	Expiration date for the license key.

Data Pane Item	Description
License Quantity	Number of licenses available.

To arrange the rows in ascending or descending order, use the sorting icon ( ) in the table header rows.

You can also use the row header indicated by the filter icon ( ) to type in search queries to refine the search.

License Expiry Date

The **Key Management** table displays the expiration date for each license.

As the licenses expiration date approaches, users receive expiry notifications. The users with evaluation license receive license expiry notifications through email 30, 15, and 1 day before the license expiry and on day 1 after the license actually expires.

The users with paid licenses receive license expiry notifications through email 90, 60, 30, 15, and 1 day before expiry and two notifications per day on day 1 and day 2 after the license expires.

If a license for the particular device expires, Aruba Central no longer manages that device. Currently, Aruba Central does not give an option to remove the expired licenses from the UI. The expired licenses are displayed in the **Key Management** table with the expired date.

Converting Legacy Tokens to New Licenses

The conversion of unassigned Device Management tokens to Foundation Licenses for APs, switches, and gateways is a one-time operation for the selected Device Management tokens. The Device Management token can either be an evaluation token or a purchased token.

The Service Management tokens are not converted into the Aruba Central Licenses.

If you do not convert the unassigned Device Management tokens by 31 December 2021, all the tokens are automatically converted to AP Foundation Licenses. If you wish to revert a conversion, you must contact Aruba Technical Support.

To complete the license conversion:

1. On the **Account Home** page, go to **Global Settings** > **Key Management**.
   The **Key Management** page is displayed.
2. Click **Click here to complete license conversion**.
   The **Convert Deprecated Licenses** page is displayed.
3. Select the key that you want to convert and click **Convert** on the row.
   The **Convert Deprecated Licenses** window is displayed.
4. Select the option to which you want to convert the unassigned device license for the key.
5. Click **Convert**.
   The **Convert** button is available only when all the licenses are assigned for the selected key.
6. View **Global Settings** > **License Assignment** page.
   A list of new licenses assigned for the deprecated keys is displayed.

Download Conversion Logs

This option provides information about how legacy Device Management and Services subscription keys are converted to Aruba Central Licenses either using automatic or manual license assignment.

The information can be downloaded as a PDF document. The document contains a table which provides following information:

- **Conversion Time**—Date and time when the legacy keys are converted to Aruba Central Licenses.
- **SKU Type**—Legacy key type as Device Management or Service subscription.
- **Subscription Key**—Legacy subscription key details.
- **Start Date**—Start date of the legacy subscription.
- **End Date**—End date of the legacy subscription.
- **Remaining Unassigned Quantity**—Number of Aruba Central Licenses that are not yet assigned (after the legacy subscription keys are converted).
- **Converted Subscriptions**—Information about the Aruba Central Licenses to which the legacy keys are converted.

Managing License Assignments

Aruba offers two tiers of device licenses as part of the Aruba Central Licenses. The two tiers are Foundation and Advanced Licenses. The devices in Aruba Central that offer Foundation and Advanced Licenses include the following:

- APs
- Switches
- SD-Branch Gateways

The value-added services that previously required service subscriptions are now packaged as part of either a Foundation or an Advanced License. To know more about the different types of licenses available for the devices, and the services packaged with each license, see Overview of Aruba Central Foundation and Advanced Licenses.

Before proceeding with the license assignment, ensure that all the license keys are available in Aruba Central. For more information on how to add license keys to Aruba Central, see Managing License Keys.

For more information about MSP Licenses, see Managing MSP Licenses.

Licensing Workflow in the Initial Setup Wizard

To enable automatic assignment of licenses from the Initial Setup Wizard:

1. Verify that you have valid license key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the **Assign License** tab, turn on the **Auto Assign License** toggle switch.

Licensing Workflow for a New User

If you are a new user in Aruba Central, you can avail of either the evaluation license or a paid license.

For an evaluation user, see the workflow at Starting Your Free Trial.

For a paid user, see the workflow at Setting up Your Aruba Central Instance.

If you are a new user in Aruba Central and have purchased one or several licenses, ensure that all of your license keys are added to Aruba Central.

For license assignment to devices, you can avail of one of the following options:

- Use the **Auto-Assign Licenses** option
- Manually assign, update, or unassign licenses

Enabling the Auto-Assign Licenses Option

The **Auto-Assign Licenses** option in Aruba Central enables automatic assignment of available licenses to all of the devices available in the inventory. When you enable this option, you must specify the preferred license type as either Foundation or Advanced. You cannot manually assign licenses to devices if the **Auto-Assign Licenses** option is enabled.

The licenses for APs, switches, and gateways cannot be used interchangeably. For example, you cannot use an AP Foundation License on a gateway. Similarly, if an Aruba 25xx Switch is in the inventory but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch. Before enabling the Auto-Assign License option for a specific device type, ensure that there are sufficient available licenses for the specific device type.

To enable automatic assignment of licenses from the License Assignment page:

1. On the **Account Home** page, under **Global Settings**, click **License Assignment**.

   The **License Assignment** page is displayed.
2. Select the device type to assign the license.

   The available tabs are Access Points, Switches, and Gateways. The total number of devices for each device type is displayed for each of the tabs.
3. On the device tab, slide the **Auto-Assign Licenses** toggle switch to the On position.

   The **Manage License Assignment (Auto)** window is displayed.
4. Select the appropriate license type, **Foundation** or **Advanced**, from the drop-down menu, and then click **Update**.

   All the unassigned devices of the selected type in the inventory are enabled for automatic assignment of license.

Manually Assigning, Updating, or Unassigning Licenses

The License Assignment page enables you to assign, update, or even unassign a license from a device.

Aruba Central monitors devices with a valid license only.

The licenses for APs, switches, and gateways cannot be used interchangeably. For example, you cannot use an AP Foundation License on a gateway. Similarly, if an Aruba 25xx Switch is in the inventory but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch.

To manually assign licenses to devices or to change the existing license assignment:

1. On the **Account Home** page, under **Global Settings**, click **License Assignment**.

   The **License Assignment** page is displayed.

2. Select a device type tab.

   The available tabs are **Access Points**, **Switches**, and **Gateways**. The total number of devices for each device type is displayed for each of the tabs.
3. Under **License Summary**, ensure that the **Auto-Assign Licenses** option is disabled.

   You cannot manually assign licenses if the Auto-Assign Licenses option is enabled.
4. Select the device for which you want to assign or update the license.

   Clicking on a device type displays two additional sub-tabs: **Licensed** and **Unlicensed**.

To manually assign or update licenses for all devices of a type, click **Select All**. You can also select devices at random.

5. Click **Manage**.

   The **Manage License Assignment (Manual)** window is displayed.
6. Do one of the following:
   a. To update or assign a license: Select the appropriate license from the drop-down menu and click **Update**.
   b. To unassign a license: Select **Unassign** to remove the existing license from that device.

Migration Workflow for an Existing User

Whether you are an evaluation user or a user with purchased licenses, the following is the migration workflow to the new Aruba Central Licenses:

Any existing rules set about Service Management tokens through APIs are discarded during the migration.

1. For all existing APs and switches that are already assigned licenses in the legacy system, the licenses are automatically converted to device-specific Foundation Licenses in the new model. The gateway licenses remain unchanged.
2. To check how the migration was done, and to learn more about the new license keys and corresponding licenses, in the **Account Home** page, go to **Global Settings** > **Key Management**.

   For more information about the **Key Management** page, see Managing License Keys.
3. To check how the legacy licenses were converted, navigate to **Account Home** > **Global Settings** > **Key Management** page, and click the **Download Conversion Logs** link.
4. If there are unassigned evaluation or purchased Device Management tokens, you can convert the legacy tokens to license keys for the new Aruba Central Licenses.

Service Management tokens are not converted. Instead, the AP licenses are pre-packaged with additional services.

   To know more about converting unassigned Device Management tokens, see Converting Legacy Tokens to New Licenses.
5. If you had the auto-licensing option enabled before migration, in the new licensing model the **Auto-Assign Licenses** option is automatically enabled for APs, switches, and gateways. The **Auto-Assign Licenses** option for APs and switches is set with the corresponding device-specific Foundation Licenses.

NOTE

The **Auto-Assign Licenses** option for gateways is not enabled during the migration.

For more information about the **Auto-Assign Licenses** option, see Enabling the Auto-Assign Licenses Option.

6. If you had the auto-licensing option disabled before migration, this option is also disabled in the new licensing system.

Viewing the License Assignment Details

The License Assignment page consists of three sections for the type of device selected from the tabs. The device can be **Access Points**, **Switches**, or **Gateways**,

License Summary

A summary about the type of licenses available for the selected device type, the number of licenses available, and number of licenses assigned.

The available devices for Aruba Central include APs, switches, and gateways. Clicking on a device type displays two additional sub-tabs: **Licensed** and **Unlicensed**.

Clicking on one or more license type in the License Summary section displays the details of the license type in the License Management section. To deselect the license, click the selected license type again.

License Assignment

The **License Assignment** section provides detailed information about all the devices in the inventory and license status for each of the device. This table provides following information about each device in the inventory:

- Type
- Serial Number
- MAC address
- Model
- Customer
- Assigned License

Use the sorting icon ( ) in the table header row to arrange the rows in ascending or descending order. You can also use the row header indicated by the filter icon ( ) to type in search queries to refine the search.

Renewing License Assignments

To renew your license, contact your Aruba Sales team.

Automatic License Assignment Workflow

The **Auto-Assign Licenses** option can be set to either **Foundation** or **Advanced**. This option enables Aruba Central to automatically assign licenses to all the available APs, switches, and gateways. This section explains how the **Auto-Assign Licenses** option works with the help of a sample Aruba Central account.

Sample Aruba Central Account Details

Assume an Aruba Central account with the following devices:

- APs - 10
- Aruba 90xx Series Gateway and 1 Aruba 70xx Series Gateway - 1
- Aruba 29xx Series Switches - 2

Now assume that you have the following licenses:

- AP Foundation Licenses - 5
- AP Advanced Licenses - 10
- Gateway Foundation Base Licenses - 5
- Gateway Advanced with Security Licenses - 5
- Switch Foundation Licenses for 6200/29xx - 5

Here are the available scenarios for the **Auto-Assign Licenses** option. Note that only one can be chosen during actual installation.

- Auto-Assign Licenses Option Set to Foundation
- Auto-Assign Licenses Option Set to Advanced

If you have an Aruba Central account with legacy Device Management tokens, the tokens are utilized during the automatic license assignment workflow if and when there is no availability of licenses. The legacy tokens are converted to Foundation Licenses of the required type and assigned to the devices that did not have any licenses mapped. For more information, see Using Legacy Device Management Tokens.

Auto-Assign Licenses Option Set to Foundation

If you enable the **Auto-Assign Licenses** option and set the preference to **Foundation**, this is how the device-to-license mappings are done:

- **For APs**—First, the Foundation Licenses for APs are used. Since there are five AP Foundation License, five APs are assigned with the Foundation Licenses. For the remaining five APs, the Advanced License pool for APs is used and the five remaining APs are assigned Advanced Licenses.
- **For Gateways**—First, the Foundation Base Licenses for gateways are used. Since there are only two gateways and the Foundation Base Gateway Licenses are applicable to both the Aruba 70xx Series and 90xx Series Gateways, two Foundation Base Licenses for gateways are assigned.
- **For Switches—**First, the Foundation Licenses for switches are used. Since there are only two 29xx Series Switches and two Foundation Licenses for 29xx Series Switches are available, these are assigned.

The following is the final device-to-license mapping:

- APs (10) - Five AP Foundation Licenses and five AP Advanced Licenses
- Gateways (2) - Two Gateway Foundation Base Licenses
- Switches (2) - Two Switch Foundation Licenses for 6200/29xx

Auto-Assign Licenses Option Set to Advanced

If you enable the **Auto-Assign Licenses** option and set the preference to **Advanced**, this is how the device-to-license mappings are done:

- **For APs**—First, the Advanced Licenses for APs are used. Since there are five AP Advanced Licenses, five APs are assigned with the Advanced License. For the remaining five APs, the Foundation License pool for APs is used and the five remaining APs are assigned Foundation Licenses.

- **For Gateways**—First, the Advanced with Security Licenses for gateways are used. Since there are only two gateways and the Advanced with Security Licenses are applicable to both the Aruba 70xx Series and 90xx Series Gateways, two Advanced with Security Licenses for gateways are assigned.
- **For Switches**—There are no Advanced Licenses for switches available. Hence, the Foundation Switch Licenses for 6200/29xx are used. Since there are only two switches, two Foundation Licenses for switches are assigned.

The following is the final device-to-license mapping:

- APs (10) - Five AP Advanced Licenses and five AP Foundation Licenses
- Gateways (2) - Two Gateway Advanced with Security Licenses
- Switches (2) - Two Switch Foundation Licenses

Using Legacy Device Management Tokens

When you enable the **Auto-Assign Licenses** option, and there are no available Foundation or Advanced Licenses left to assign, Aruba Central has the option of checking if legacy Device Management tokens are available and use those tokens instead. The legacy tokens are converted to Foundation Licenses of the required type and assigned to the devices that did not have any licenses mapped.

Assume that you have the following devices:

- APs - 20
- Gateways - 2
- Switches - 2

For the sake of simplicity, the gateway and switch model types are omitted from this example.

Now assume that you have the following licenses:

- AP Foundation Licenses - 5
- AP Advanced Licenses - 10
- Legacy Device Management Tokens - 20

If you enable the **Auto-Assign Licenses** option and set the preference to **Foundation Licenses**, this is how the device to license mappings are done:

- **For APs**—First, the Foundation Licenses for APs are used. Since there are five AP Foundation License, five APs are assigned with the Foundation Licenses. Next, the 10 AP Advanced Licenses are assigned. For the remaining five APs, there are no licenses available. Aruba Central then converts five legacy Device Management tokens to five AP Foundation Licenses and assigns them to the remaining five APs. There are now 15 legacy Device Management tokens available.
- **For Gateways**—There are no available gateway licenses. Aruba Central converts two legacy Device Management tokens to two Gateway Foundation Licenses and assigns them to the two gateways. There are now 13 legacy Device Management tokens available.
- **For Switches**—There are no available switch licenses. Aruba Centralconverts two legacy Device Management tokens to two Switch Foundation Licenses and assigns them to the two switches. There are now 11 legacy Device Management tokens available.

The following is the final device to license mapping:

- APs (20) - 10 AP Foundation Licenses, five AP Advanced Licenses
- Gateways (2) - Two Gateway Foundation Licenses
- Switches (2) - Two Switch Foundation Licenses
- Legacy Device Management Tokens left - 11

Aruba Central Licenses Feature Details

This section provides a description about the different configuration and monitoring options available for Aruba Central features tied to Foundation and Advanced Licenses.

Configuration

AP Configuration

License Applicability: AP configuration is available for AP Foundation License.

Network administrators can manage APs through the Aruba Instant UI, Aruba Central, or AirWave management system. Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AP deployments.

For template-based provisioning, APs must be assigned to a group with template-based configuration method enabled.

AOS-Switch Configuration

License Applicability: AOS-Switch configuration is available for Switch Foundation License.

Network administrators can manage AOS-Switches through the Aruba Central UI menu options. Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AOS-Switch deployments.

AOS-CX Configuration

License Applicability: AOS-CX configuration is available for Switch Foundation License.

Network administrators can manage AOS-CX switches through the Aruba Central UI menu options and the MultiEdit mode. The MultiEdit mode in Aruba Central provides a single window for viewing and editing the configuration for one or more AOS-CX switches. In this mode, viewing and editing the configuration is performed using the CLI syntax.

Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AOS-CX deployments.

Auto-Commit

License Applicability: Auto-Commit is available for Foundation and Advanced Licenses for APs, switches, and gateways.

Aruba Central supports a two-staged configuration commit workflow for Instant APs. When the auto-commit state is enabled for a group, the configuration changes are instantly applied to all devices where the auto-commit state is enabled.

Configuration Audit

License Applicability: Configuration Audit is available for Foundation and Advanced Licenses for APs, switches, and gateways.

In Aruba Central, the Configuration Audit page provides an audit dashboard for reviewing configuration changes of the devices provisioned in the UI and template groups. The Configuration Audit page allows you to view configuration push errors, template synchronization errors, configuration sync, and device-level configuration overrides.

Gateway Configuration

License Applicability: Gateway configuration is available for Gateway Foundation and Foundation Base Licenses.

Aruba Central supports the following methods to configure Gateway groups and Gateways in SD-Branch deployments:

- Guided Setup—You can use the Guided Setup to quickly configure basic and essential parameters on Aruba Gateways for deploying the SD-WAN solution. The Guided Setup provides a wizard-based workflow for provisioning Gateways.
- Basic Mode—Allows you to configure your Gateways in a non-linear fashion. This mode allows you to make configuration changes after you provision your gateways for the first time using a Guided setup.
- Advanced Mode—Allows you to configure advanced features for SD-WAN deployments.

Template groups in Aruba Central allow network administrators to create a common configuration output by using a combination of CLI commands and variables, and apply this configuration to the other Gateway devices provisioned in that group.

Monitoring and Reporting

Access, Spectrum, Monitor Mode of Radio Operations

License Applicability: The Access, Spectrum, and Monitor modes of the radios of an access point are available for AP Foundation and Advanced Licenses.

In the Access mode, the Instant AP serves clients, while also monitoring for rogue Instant APs in the background. In the Monitor mode, the Instant AP acts as a dedicated monitor, scanning all channels for rogue Instant APs and clients. In the Spectrum mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring Instant APs or from non Wi-Fi devices such as microwaves and cordless phones.

Alerts and Events

License Applicability: Alerts and events for APs, Gateways, and switches is part of Foundation License and does not require any extra configuration. This tab shows data for all devices irrespective of device license type.

The **Alerts and Events** dashboard displays a list of alerts and events generated for events pertaining to device provisioning, configuration, and user management. You can view the alerts and events in the **List** view and **Summary** view. **Configuration** view is used to configure alerts and is available only at the **Global** context.

Application Visibility

License Applicability: The Application Visibility feature is a part of a Foundation License. However, as API streaming is available for Advanced Licenses only, the Application Visibility streaming service is supported only for APs with an Advanced License.

Application Visibility is a custom-built Layer-7 firewall capability in Aruba Central that allows you to create firewall policies based on the types of applications in IAPs. Application Visibility provides features like deep packet inspection, application monitoring, and AirSlice Policy.

Audit Trail

License Applicability: Audit Trail logs for APs, gateways, and switches, is part of Foundation License and does not require any extra configuration. This tab shows data for all devices irrespective of device license type.

The **Audit Trail** page in Aruba Central shows the total number of logs generated for all device management, configuration, and user management events triggered in the network.

Client List and Details

License Applicability: Clients monitoring is available for the Foundation License of AP, switch, and gateway.

The **Clients** page is also called the unified clients list and it provides a list of all clients that are connected to access points, switches, or gateways in the network. The List and Summary views under the Clients tab serve as dashboards. It displays details about the network performance, client connection status, instantaneous client refresh, Go Live (only AP), and other information required for monitoring the clients.

Floorplans

License Applicability: Floorplans is available for AP and gateway Foundation Licenses. Floorplans allow you to plan sites, create and manage floorplans, and provision access points. Floorplans provide a real-time picture of the radio environment of your wireless network and the ability to plan the wireless coverage of new sites.

Reports

License Applicability: Reports is available for the Foundation License.

The Reports feature enables you to generate reports for the Clients, Infrastructure, Security Compliance, and Applications categories. The **Reports** feature is present under the **Analyze** section of the **Network Operations** app. The functionalities present are creating a report, generating a report, scheduling the report generation, previewing a report, and downloading a report in PDF and CSV formats. The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days in Aruba Central 2.5.3.

Topology

License Applicability: Topology is available for Foundation and Advanced Licenses for APs, switches, and gateways.

In Aruba Central, the Topology tab in the site dashboard provides a graphical representation of the site, including the network layout, details of the devices deployed, and the health of the WAN uplinks and tunnels. The topology map provides information about third-party devices and devices that are not managed by Aruba. It also provides information about orphan and offline third-party devices, and the VLANs configured on switches running AOS-Switch and AOS-CX software.

Web Content Classification (WebCC)

License Applicability: The WebCC feature is available for Foundation Licenses for APs and gateways.

The WebCC allows you to classify website content based on reputation and take measures to block malicious sites. It fetches information about website content classification and geolocation of IPs. The IP reputation database contains known IP addresses associated with various malicious activities or threats such as botnet, DOS, and spam sources. The geolocation IP database contains the geographical location of

the IP address from where the traffic is received or to which the traffic is sent. This provides geolocation and reputation filtering as part of the security suite.

The table below lists the features supported for AP and gateway licenses:

AP Foundation	Gateway Foundation and Foundation Base
WebCC Firewall rules, visualization by reputation and category	WebCC Firewall rules, visualization by reputation and category

Wi-Fi Connectivity

License Applicability: The Wi-Fi Connectivity dashboard for APs is part of Foundation License and does not require any extra configuration.

The **Wi-Fi Connectivity** page displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase. The connection phases include the following:

- **All**—Displays the aggregated success percentage of Association, Authentication, and DHCP for all clients connected to the network.
- **Association**—Displays the percentage of successful attempts made by a client to connect to the network.
- **Authentication**—Displays the percentage of successful attempts of client authentication.
- **DHCP**—Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client.
- **DNS**—Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network.

AI Operations

AI Insights

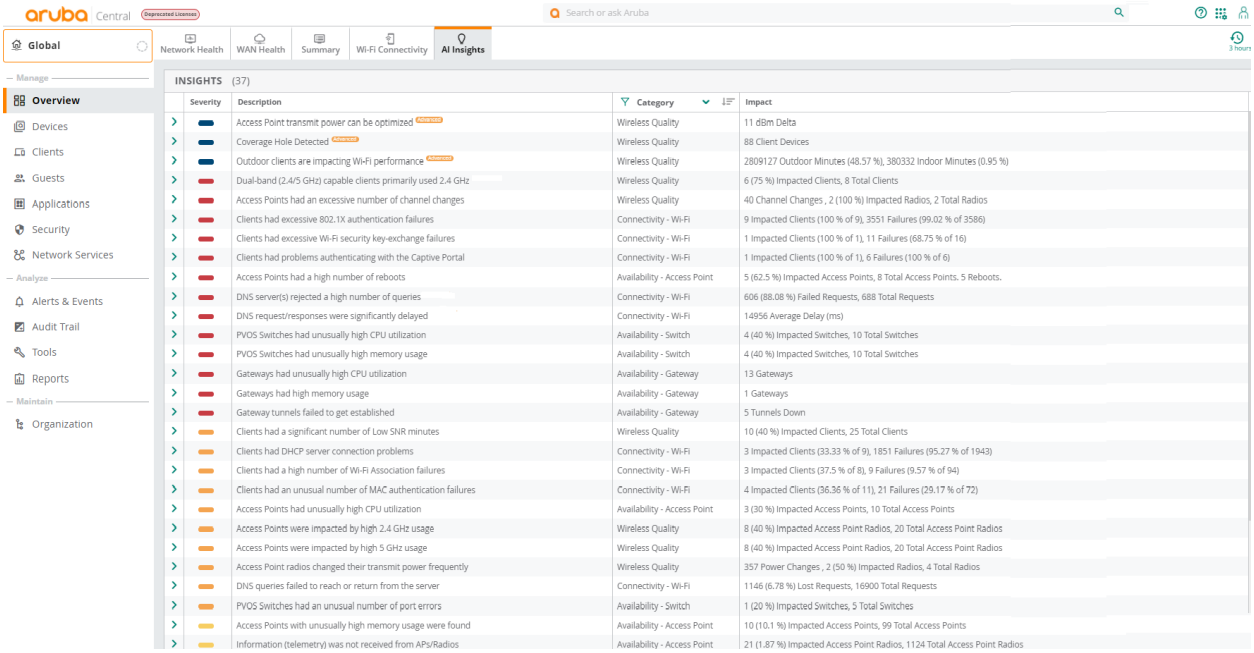
License Applicability: AI Insights is available for Foundation and Advanced Licenses for APs, switches, and gateways. The Insights that require an Advanced License are marked as Advanced in the UI.

The AI Insights dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level for the selected time range. Each insight provides specific details on the occurrences of these events for easy debugging.

Different types of insights are generated by Aruba Central and they can be accessed from different contexts such as Global, Site, Clients, and Device. Some of the insights are part of an Advanced License only and they are marked as Advanced in the user interface.

The following figure displays various AI Insights available and some are marked as Advanced.

Figure 91 *AI Insights List*



The table below lists the features supported for AP, switch, and gateway licenses:

AP Foundation License	AP Advanced License	Switch Foundation	Gateway Foundation, Foundation Base, and VGW
▪ Connectivity—Wi-Fi ▪ Wireless Quality ▪ Availability—Access Points ▪ Class and Company Baselines	▪ Wireless Quality ◦ Outdoor clients impacting Wi-Fi performance ◦ Coverage Hole Detection ◦ Transmit power optimization	▪ Availability—Switch ▪ Class and Company Baselines	▪ Availability—Gateways ▪ Class and Company Baselines

NOTE

In this release, all AI Insights are available irrespective of the user role or Aruba Central subscription. In the upcoming Aruba Central release, AI Insights marked as **Advanced** in the user interface would require an advanced subscription.

AI Search

License Applicability: AI Search feature is available for Foundation License for AP, switch, and gateway.

The AI search feature in Aruba Central enables you to search for clients, devices, and infrastructure connected to the network. Using the search results, you can navigate to the configuration and troubleshooting pages. The search also retrieves relevant documentation to help you efficiently operate your networks. The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant search results.

Dynamic Logs

License Applicability: Dynamic Log is available for both Foundation and Advanced Licenses for APs and gateways.

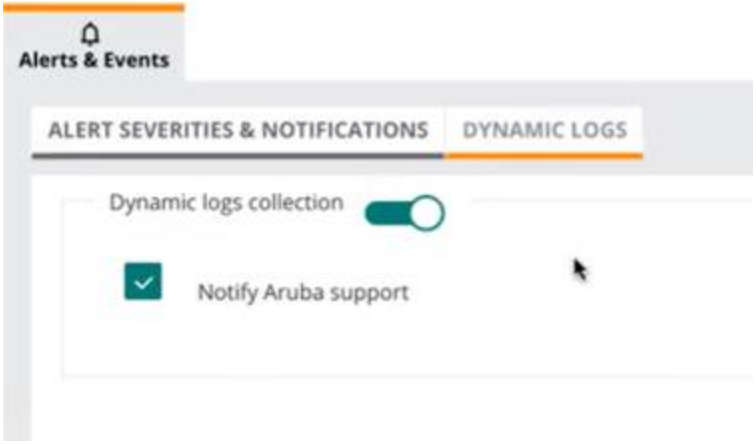
The Dynamic Logs feature enables Aruba Central to dynamically run CLI show commands on APs and gateways, and collect the output as logs. You can also enable Aruba support notification option to notify TAC support regarding the logs generated. These logs can be used to troubleshoot the APs and gateways.

NOTE

Dynamic Logs is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

The following figure displays the available options for Dynamic Logs.

Figure 92 *Dynamic Logs Option*



For devices assigned with the Foundation License, the Dynamic Logs feature only supports the log collection activity. Even if you enable the **Notify Aruba Support** option, the option is not activated for devices licensed with Foundation License.

For devices assigned with Advanced Licenses, Dynamic Logs support both log collection and the Aruba support notification option.

For example, assume an Aruba Central account with Dynamic Logs enabled, where you configure a group of three Access Points (APs), AP1, AP2, and AP3. AP1 has a Foundation License while AP2 and AP3 have Advanced Licenses. For this group, both **Dynamic logs collection** and **Notify Aruba Support** options are enabled. However, the Aruba support notification option is only applicable for AP2 and AP3, which have Advanced Licenses.

Troubleshooting

Live Events

Licensing Applicability: Live Events for clients, APs and switches is part of Foundation License and does not require any extra configuration.

The clients **Live Events** page shows information required to troubleshoot issues related to a client or a site in real time for detailed analysis. Aruba Central also allows to troubleshoot issues related to access points. The AP Live Events feature is similar to client live troubleshooting, but in this case we can enable Live Events at the AP level. Currently, users can subscribe to Radio, VPN, and Spectrum events.

Live Packet Capture (PCAP)

Licensing Applicability: Live PCAP for APs and switches is part of Foundation License and does not require any extra configuration.

Aruba Central allows users to interact and launch a targeted packet capture on a client connected to a specific AP or a switch. When the user starts packet capture from the UI, Aruba Central notifies the AP and the switch. The default packet capture duration is 15 minutes.

Troubleshooting Tools

License Applicability: Troubleshooting for APs, gateways, and switches is part of Foundation License and does not require any extra configuration.

The **Tools** menu option allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central.

The **Tools** page is divided into the following tabs:

- **Network Check**—Allows you to run diagnostic checks on networks and troubleshoot client connectivity issues.
- **Device Check**—Allows you to run diagnostic checks and troubleshoot switches.
- **Commands**—Allows you to perform network health check on devices at an advanced level using command categories.

Services

AirGroup

License Applicability: AirGroup is available for both AP Foundation and Advanced Licenses.

AirGroup is a zero–configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. AirGroup supports both wired and wireless devices.

AirGroup is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

In InstantOS-based APs, the service is hosted on the IAP Virtual controller and all services are supported.

AirMatch

License Applicability: AirMatch is available for AP Foundation License.

AirMatch channel planning evens out channel distributions in any size of network and in any subset of the contiguous network. AirMatch also minimizes channel coupling where adjacent radios are assigned to the same channel.

AirSlice

License Applicability: The AirSlice feature is available for only AP Advanced Licenses.

The AirSlice feature allows network operators to build virtual networks suitable for specific application requirements. It allows network operators to monitor applications used by clients and supports multiple services such as gaming, IoT, voice, video, and so on.

NOTE

AirSlice is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

For devices that have Advanced Licenses, the AirSlice feature supports unlimited applications and provides prioritization of custom-applications with visibility and configuration.

The table below lists the features supported for AP licenses:

Advanced
▪ Visibility and prioritization of applications ▪ Maximum number of applications as supported by the Aruba Central platform

ClientMatch

License Applicability: ClientMatch is available for AP Foundation License.

ClientMatch continually monitors the RF neighborhood for each client to provide ongoing client band steering, load balancing, and enhanced AP reassignment for roaming mobile clients.

Presence Analytics

License Applicability: Presence Analytics is available for Foundation AP License.

Presence Analytics enables businesses to collect and analyze user presence data in public venues, enterprise environments, and retail hubs. Presence Analytics also enables businesses to collect real-time data on user footprints within the wireless network range.

SaaS Express

License Applicability: SaaS Express is available for Advanced Gateway License and Advanced with Security Gateway License only.

The SaaS Express feature, on SD-WAN Gateways, enables discovery of the SaaS application servers, monitors application performance, and steers traffic to the best-available servers, and thus provides an improved user experience.

Unified Communications

License Applicability: Unified Communications is available for AP Advanced Licenses.

The Unified Communications feature enables a seamless user experience for voice calls, video calls, and application-sharing when using communication and collaboration tools. It allows you to actively monitor voice, video, and application-sharing sessions, provide traffic visibility, prioritize the required sessions, and provide rich visual metrics for analytical purposes.

NOTE

Unified Communications is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

Security

Cloud Guest

License Applicability: Cloud Guest is available for the AP Foundation License.

The Cloud Guest access enables the guest users to connect to the network. This is provided through the splash page profile that is created by the administrators for the guest users in the **Guests** tab under

Manage. The **Summary** page in the **Manage > Guest Access** application is the monitoring dashboard that displays the number of guests, guest SSID, client count, type of clients, and guest connection. Cloud Guest deals with the AP, so the license that is assigned to the AP is also applicable to Cloud Guest. By default, the Foundation License is applicable. The Advanced License features will also be available if the Cloud Guest is assigned to it.

ClearPass Device Insight-Based Clients Profile

License Applicability: ClearPass Device Insight (CPDI) based Clients Profile is available for Foundation License for APs and gateways..

The CPDI-based Clients Profile enables network and security administrators to discover, monitor, and automatically classify new and existing devices that connect to a network. You can identify devices that include IoT devices, medical devices, printers, smart devices, laptops, VoIP phones, computers, gaming consoles, routers, servers, switches, and so on.

CPDI-based Clients Profile is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

The table below lists the features supported for AP and gateway licenses:

Foundation	Advanced
▪ Basic client MAC Classification based on telemetry data ▪ Client Family, Client Category, Client OS ▪ Cloud Auth Integration	▪ Access to Collector support in Central (not including physical collector costs) ▪ ML-based client classification ▪ Advanced Security Features (Risk / Posture / Vulnerability) ▪ Security baseline of device behavior with Firewall recommendation

Intrusion Detection and Prevention (IDS or IPS)

License Applicability: IDS and IPS is available for Foundation with Security Gateway License, Foundation Base with Security Gateway License, and Advanced with Security Gateway License.

The IDS and IPS monitors, detects, and prevents threats in the inbound and outbound traffic. Aruba IDS or IPS adds an extra layer of security that focuses on users, applications, network connections, and can be integrated with the Aruba SD-Branch solution.

RAPIDS

License Applicability: RAPIDS is available for Foundation and Advanced Licenses for APs.

The RAPIDS feature enables Aruba Central to quickly identify and act on interfering APs in the network that can be later considered for investigation, restrictive action, or both. Once the interfering APs are discovered, Aruba Central sends alerts for security events to the network administrators about the possible threat and provides essential information needed to locate and manage the threat.

RAPIDS is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

This feature is part of the AP Foundation License. However, as API streaming is available for Advanced License only, Aruba Central would not stream any security events for APs with Foundation License. For APs

with Advanced License, API streaming of security events is available for further diagnosis and threat management.

API

Streaming APIs

License Applicability: The Streaming API service requires that devices such as IAPs and gateways are assigned with Advanced License.

The Streaming API feature enables you to subscribe to a select set of services, instead of polling the NB API to get an aggregated state, or statistics of the events, pertinent to the monitoring activities of Aruba Central. With Streaming API, you can write value-added applications based on the aggregated context.

For example, with Streaming API, you are notified about the following types of events:

- The UP and DOWN status of the devices
- Change in location of stations

The Streaming API feature in Aruba Central is enabled only when any one of the devices in the account has an Advanced License. If the account has devices with only Foundation License, the Steaming API tab is not displayed in Aruba Central.

If the Streaming API feature is enabled, and the account has a mix of Foundation License and Advanced License for devices, the devices that are assigned with Foundation License do not stream any data for any topics.

SD-Branch

Application-based Policy

License Applicability: The application-based policy configuration is available for Foundation License for Branch Gateways.

The Application-based policy configuration helps in deep packet inspection of application usage by clients. Using this configuration, you can define applications, security, and service aliases. You can configure Access Control Lists (ACLs) to restrict user access to an application or application category.

Dynamic Path Steering

License Applicability: Dynamic Path Steering is available for Gateway Foundation and Foundation Base License.

In the **Path Steering** tab, you can view traffic path steering details for the Dynamic Path Steering policies configured on the Branch Gateway. This tab also displays the number of policies that are compliant along with the total number of policies configured on the Branch Gateway.

Full SD-LAN Control

License Applicability: SD-LAN monitoring is available for Foundation License for Branch Gateways.

The LAN Summary page displays a graphical representation of the LAN link availability of a Branch Gateway. It also provides a summary of all the LAN interfaces and port details.

IPsec VPN

License Applicability: IPsec VPN is available for Gateway Foundation and Foundation Base License.

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the controller secures corporate data. You can configure an IPsec tunnel from virtual controller using Aruba Central.

Role-based Access Policy

License Applicability: Role-based Access Policy configuration is available for Foundation License for Branch Gateways.

The Role-based Access Policy determines client access based on the user roles assigned to a client. Each user or device connected to the branch network is associated with a user role. Once the role is assigned, traffic and security policies are applied to devices based on the role.

SD-WAN Overlay

License Applicability: SD-WAN Overlay monitoring is available for Gateway Foundation License.

The SD-WAN Overlay is an orchestrator service for branch deployments, which is done by setting up IPsec tunnels between the Branch Gateways and VPN Concentrators. This is achieved through **Tunnel** and **Route** orchestration. The tunnel configuration between the branch and hub sites is automatic and the route configuration is done by redistributing the routing information learnt from the branch in a dynamic way. The **Map** and **Grid** views of the **Tunnel** and **Route** tabs under **SD-WAN Overlay** serve as dashboards for monitoring purpose, providing information about the tunnels and routes configured for an individual Branch Gateway.

Stateful Firewalls

License Applicability: Stateful Firewalls is available for Gateway Foundation and Foundation Base License.

Aruba Gateways support stateful firewall for stateful inspection of packets. Stateful firewalls provide an additional layer of security by tracking the state of network connections and using the state information from previous communications to monitor and control new communication attempts. To protect your network from external attacks and unauthorized communication attempts, you can configure match conditions and packet filtering criteria for the Aruba Gateways.

Web Content Filtering

License Applicability: Website content filtering is available for Foundation License for Branch Gateways. Aruba Gateways enhance branch security by providing real-time web content and reputation filtering. The Website Content Classification feature on Branch Gateways allows you to classify website content based on reputation and take measures to block malicious sites.

Managing Your Device Inventory

After you add the paid subscription key(s) to your Aruba Central account, device(s) purchased by you are automatically added to the device inventory in the respective Aruba Central account. For more information about subscription keys, see Managing License Keys.

If the device you purchased does not show up in the inventory, you can manually add it. Aruba Central allows you to add up to 32 devices manually by entering the valid MAC and serial number combination for each device.

Users having roles with **Modify** permission can add devices. Users having roles with **View Only** permission can only view the Device Inventory module.

Viewing Devices

The devices provisioned in your account are listed in the **Account Home > Global Settings > Device Inventory** page. A dashboard lists the total number of devices and the number of access points, switches, and gateways in the inventory.

The following table describes the columns in the **Devices** table.

Table 50: *Device Details*

Parameter	Description
Serial Number	Serial number of the device.
MAC Address	MAC address of the device.
Type	Type of the device, for example Instant AP, switch, or gateway.
Model	Hardware model of the device.
Part Number	Part number of the device.
IMEI	The International Mobile Equipment Identity (IMEI) number of the gateway device. This field is applicable only for 9004-LTE gateways. Click the ellipsis icon in the table to select this column. It is not displayed by default.
IP Address	IP address of the device.
Name	Name of the device.
Group	Group assigned to the device.
Assigned License	License assigned to the device.

Adding Devices to Inventory

For information on adding devices, see Onboarding Devices.

Onboarding Devices

Aruba Central supports the following options for adding devices:

- If you are an evaluating user, you must manually add the serial number and MAC address of the devices that you want to manage from Aruba Central.

This section includes the following topics:

- Adding Devices (Evaluation Account)
- Adding Devices (Paid Subscription)
- Manually Adding Devices

Adding Devices (Evaluation Account)

Use one of the following methods to add devices to Aruba Central:

- Using the Initial Setup Wizard
- Using the Device Inventory Page

Using the Initial Setup Wizard

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number and MAC address of your devices.

   You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
3. Click **Done**.
4. Review the devices in your inventory.

Using the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.

   The **Device Inventory** page is displayed.
2. Click **Add Devices**.

   The **Add Devices** pop-up window is displayed.
3. Enter the serial number and the MAC address of each device.

   You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
4. Click **Done**.
5. Review the devices in your inventory.

Adding Devices (Paid Subscription)

If your devices are not added to your inventory, set up a device sync by adding one device from your purchase order.

To set up device sync, use one of the following methods:

- In the Initial Setup Wizard
- From the Device Inventory Page

In the Initial Setup Wizard

1. Ensure that you have added a license key and click **Next**.
2. In the **Add Devices** tab, enter the serial number and MAC address of any one device from your purchase order.

   Most Aruba devices have the serial number and MAC address on the front or back of the hardware.
3. Click **Add Device**. Aruba Central imports all other devices mapped to your purchase order.
4. Review the devices in your inventory.
5. Perform the following options:
   - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
   - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
   - **Contact support**—Contact Aruba Technical Support.

From the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The **Device Inventory** page is displayed.

Aruba Central imports only devices associated with your account from Activate.

2. Do any one of the following:
   - Click **Sync Devices**. Enter the serial number and MAC address and click **Add Device**.
   - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
   - If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.

Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home** > **Audit Trail** page.

3. Review the devices in your inventory.
4. Perform the following options:
   - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
   - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
   - **Contact support**—Contact Aruba Technical Support.

Manually Adding Devices

Aruba Central allows you to set up only manual sync of devices from Activate database using one of the following methods:

- Adding Devices Using MAC address and Serial Number
- Adding Devices Using Activate Account
- Adding Devices Using Cloud Activation Key

You can only set up only a manual sync for Aruba Central-managed folders such as the default, licensed, and non-licensed folders.

Adding Devices Using MAC address and Serial Number

You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.

To add devices using MAC address and serial number, use any one of the following methods:

- In the Initial Setup Wizard
- From the Device Inventory Page

In the Initial Setup Wizard

If you are using the Initial Setup wizard:

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number or the MAC address of your device.

3. Click **Done**.
4. Review the list of devices.

From the Device Inventory Page

To add devices from the **Device Inventory** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The **Device Inventory** page is displayed.
2. Perform one of the following:
   - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
   - If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.

Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home** > **Audit Trail** page.

3. Click **Done**.
4. Review the devices added to the inventory.

When you add the serial number and MAC address of one AP from a cluster or a switch stack member, Aruba Central imports all devices associated in the AP cluster and switch stack respectively.

Adding Devices Using Activate Account

- Use this device addition method only when you want to migrate your inventory from Aruba AirWave or a standalone AP deployment to the Aruba Central management framework.
- Use this option with caution as it imports all devices from your Activate account to the Aruba Central device inventory.
- You can use this option only once. After the devices are added, Aruba Central does not allow you to modify or re-import the devices using your Aruba Activate credentials.

To add devices from your Activate account:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The **Device Inventory** page is displayed.
2. Click **Advanced** and select **Using Activate**.
3. Enter the username and password of your Activate account.
4. Click **Add**.
5. Review the devices added to the inventory.

Adding Devices Using Cloud Activation Key

When you import devices using the Cloud Activation Key, all your devices from the same purchase order are added to your Aruba Central inventory.

Before adding devices using cloud activation key, ensure that you have noted the cloud activation key and MAC address of the devices to add.

Locating Cloud Activation Key and MAC Address

To know the cloud activation key:

- For APs:
  1. Log in to the WebUI or CLI.
     - If using the WebUI, go to the **Maintenance** > **About**.
     - If using the CLI, execute the **show about** command.
  2. Note the cloud activation key and MAC address.

- For Aruba Switches:
  1. Log in to the switch CLI.
  2. Execute the **show system | in Base** and **show system | in Serial** commands.
  3. Note the cloud activation key and MAC address in the command output.

- For Mobility Access Switches
  1. Log in to the Mobility Access Switch UI or CLI.
     - If using the UI, go to the **Maintenance** > **About**.
     - If using the CLI, execute the **show inventory | include HW** and **show version** commands.
  2. Note the cloud activation key and MAC address. The activation key is enabled only if the switch has access to the Internet.

Adding Devices Using Cloud Activation Key

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The **Device Inventory** page is displayed.
2. Click **Advanced** and select **With Cloud Activation Key**. The **Cloud Activation Key** pop-up window opens.
3. Enter the cloud activation key and MAC address of the device.
4. Click **Add**.

If a device belongs to another customer account or is used by another service, Aruba Central displays it as a blocked device. As Aruba Central does not support managing and monitoring blocked devices, you may have to release the blocked devices before proceeding with the next steps.

Archiving Devices in Aruba Central

Aruba Central supports archiving devices that are not in use or devices that are yet to be installed. Archiving feature helps network administrators to hide devices in the Device Inventory page, to keep the device inventory organized. The archived devices are moved to the **Archived** tab on the Device Inventory page, and these can be unarchived and used whenever required.

Network administrators and users with a custom role and the **Modify** permission for the Device Inventory page can archive and unarchive devices in Aruba Central.

NOTE

The virtual gateway devices cannot be archived.

Archiving Devices

Complete the following steps to archive devices in Aruba Central:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The **Device Inventory** page is displayed.
2. Click the **All** tab.
3. Select the devices to be archived.
4. Click the **Archive** button.
   The **Confirm Action** window is displayed.
   If you click **Yes** and the selected devices are licensed, then the licenses applied to the devices are removed automatically, and devices are disconnected from the Aruba Central. The disconnected devices are moved to the **Archived** tab.

NOTE

For an MSP account, if a device of a tenant is archived, the device gets unlicensed and is moved back to the MSP account and then archived.

Unarchiving Devices

Complete the following steps to unarchive devices in Aruba Central:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The **Device Inventory** page is displayed.
2. Click the **Archived** tab.
3. Select the devices to be unarchived.
4. Click the **Unarchive** button.
   The **Confirm Action** window is displayed.

   If you click **Yes**, the devices are moved out of the **Archived** tab, and if auto-licensing is enabled, then the devices get licensed automatically.
5. To see the unarchived devices, click the **All** tab .

NOTE

For an MSP account, if a device is unarchived, the device is moved back to the MSP account. The device continues to stay unlicensed with the MSP and does not move to the tenant.

Data Collectors

Data collectors host applications that process network data.

Data collectors are available as a physical appliance or a virtual appliance. To create a data collector, set up and install on-premises at your organization the physical appliance or virtual appliance and then install an Aruba application.

Managing Data Collectors High-Level Process Flow

The following is a high-level process flow for managing data collectors:

1. Set up on-premises the physical or virtual appliance that will become the data collector. For more information, see Setting Up Appliances.
2. Create the data collector by installing an Aruba application on the physical or virtual appliance. For more information, see Creating Data Collectors.
3. Verify the status of the data collector. The status is **Running** if the data collector was created successfully. For more information, see Viewing Data Collectors.
4. Repeat Step 1 through 3 until you have created all of the data collectors that you require.
5. Set the auto-update preference for the data collectors. For more information, see Updating Data Collectors.
6. Monitor the status and performance of the different data collectors. For more information, see Viewing Data Collectors.
7. (Optional) Manually update one or all of the data collectors as required. This overrides the global auto-update preference you have set for all data collectors. For more information, see Updating Data Collectors.
8. (Optional) Delete the installed Aruba application from the data collector. This enables the appliance to be available to become a data collector again in the future for the same Aruba application or for a different Aruba application. For more information, see Deleting Data Collectors.

About Data Collectors Page

The **Data Collectors** page enables you to manage the data collectors for your organization. Using this page you can:

- Create a registration token required for setting up a physical or virtual appliance.
- Download the virtual appliance required for setting up a virtual appliance.
- Create data collectors by installing an Aruba application on a physical or virtual appliance.
- View data collectors (both managed and unmanaged).
- Set the data collectors update preference and update data collectors.
- Uninstall the Aruba application running on a data collector. When you uninstall the application, the appliance is freed up and can be used for creating another data collector in the future.

This page contains the following four cards, which can be used to perform different data collector functions:

- **Managed Collectors**
- **Other Collectors**
- **Create Collector**
- **Configure Appliance**

Managed Collectors Card

You can view and update the managed data collectors that you have created in the **Managed Collectors** card. The **Managed Collectors** card provides a **Dashboard** and a **List** view of the data collectors. Click the grid view icon ( ) in the upper right hand corner of the card to open the **List** view.

Dashboard

The **Dashboard** displays a donut chart showing the data collectors by status, by applications, or by update. By default, the data collectors by status are displayed in the chart. To change the display option for the chart, click the down arrow in the heading of the card and select another display option. Display options are: **By Status, By Apps,** and **By Update.**

By Status

The donut chart shows the data collectors by status. Next to the chart is a legend indicating the different data collector statuses. Statuses are: **Starting** (grey), **Online** (green), **Offline** (red), and **Warning** (yellow). Hover over the different color sections of the donut chart and a tool tip is displayed indicating the number of data collectors for each status. The total number of data collectors is displayed in the center of the chart.

By Apps (Applications)

The donut chart displays the data collectors by applications. Next to the chart is a legend indicating the different Aruba applications. Aruba applications include: **ClearPass Device Insight**. Each application is displayed in a different color. Hover over the different color sections of the donut chart and a tool tip is displayed indicating the number of data collectors for each Aruba application. The total number of data collectors is displayed in the center of the chart.

By Update

The donut chart shows the data collectors by update status. Next to the chart is a legend indicating the different update statuses. Statuses are: **Up to date** (yellow), **Update in progress** (red), and **Update available** (green). Hover over the different color sections of the donut chart and a tool tip is displayed indicating the number of data collectors for each update status. The total number of data collectors is displayed in the center of the chart.

The **Auto-Update** field is displayed in the lower right corner of the card when you select this display option. By default, **As soon as available** is displayed in this field. When you click this field, the **Collector Update** dialog opens. Use the **Collector Update** dialog to set when you want updates to be installed for all data collectors.

For more information about setting the data collectors global update preference, see Updating Data Collectors.

List View

The **List** view displays all of the data collectors in a grid format. The **List** view lists the data collectors that are currently represented in the **Dashboard**. At the top of the **List** view are the following buttons:

- **Update All**

  Click this button to update all of the data collectors at once. To update a specific data collector, you can expand a row in the grid and click the **Update Now** button for that specific data collector.

  For more information, see Updating Data Collectors.
- **Create Collector**

Opens the **Create Collector** dialog where you can create a data collector.

For more information, see Creating Data Collectors.

The following table describes the information that is displayed in the **List** view:

Table 51: *List View*

Field	Description
Name	Data collector name.
Status	Status of the data collector. Statuses are: **Starting, Online, Offline** and **Warning**.
Applications	Aruba application installed on the data collector.
Desired Update Time	Desired update time for that specific collector. For more information, see Updating Data Collectors.
Update Status	Update status for the data collector. Statuses are: ■ **Up to date** ■ **Update in progress** ■ **Update available**

When you hover over a row in the grid, the following icons are displayed in the row of the grid:

- **Delete** icon is displayed to the right of **Applications**. Click the **Delete** icon to uninstall the Aruba application running on that data collector. When you uninstall the application, the appliance is freed up and can be used for creating another data collector in the future.

  For more information, see Deleting Data Collectors.

Additional details for a data collector can be viewed by expanding a row in the grid. Click the plus icon next to a row in the grid to expand a row. When you expand the row, the row expands and the additional details for the data collector are displayed.

Additional Details

In the expanded row, additional overview details for the data collector are displayed. In the **Collector Details** area, the data collector name, status, creation date, and the Aruba application installed on the data collector are displayed.

To the right in the expanded row, the **Appliance In Collector** table is displayed. The following table describes the information displayed in the table:

Table 52: *Appliance In Collector Table*

Field	Description
Name	Appliance name.
IP Address	IP address of the appliance.
Model	Appliance model name. **VMware Virtual Platform** is displayed for virtual appliances.

At the bottom of the expanded row, the **Update Now** button is either available or unavailable depending on whether there is an update available for the data collector. If there is no update available, the **Update Now** button is unavailable and **No update available** is displayed in the **Version** field. If there is an update available, the **Update Now** button is available and the update version is displayed in the **Version** field.

Click the **Update Now** button to update that specific data collector. To update all data collectors, you can click the **Update All** button at the top of the **List** view.

For more information, see Updating Data Collectors.

Other Collectors Card

The **Other Collectors** card displays an overview of the number of unmanaged data collectors that are connected and not connected. The counts that are displayed in this card are:

- **Connected** (Number of unmanaged data collectors that are connected)
- **Not Connected** (Number of unmanaged data collectors that are not connected)

The following actions can be performed within the card:

- Click the **Connected** number to open the **Other Collectors** dialog where you can view the data collectors that are connected.
- Click the **Not Connected** number to open the **Other Collectors** dialog where you can view the data collectors that are not connected.

For more information, see Viewing Data Collectors.

Create Collector Card

The **Create Collector** card displays the number of appliances that are available to be used for creating a data collector. The appliance number is updated after you have successfully set up a physical appliance or virtual appliance.

For more information about setting up appliances, see Setting Up Appliances.

Click the **Create Collector** button to open the **Create Collector** dialog where you can create a data collector.

For more information, see Creating Data Collectors.

Configure Appliance Card

The **Configure Appliance** card contains a **Download Virtual Appliance** link and a **Registration Token** button.

Click the **Registration Token** button to create a registration token. The registration token is required when setting up a physical appliance or virtual appliance.

Click the **Download Virtual Appliance** link to open the **Download Virtual Appliance** dialog where you can download either the small virtual appliance file (.ova file) or medium virtual appliance file (.ova file) that is required when setting up a virtual appliance.

For more information about setting up appliances, see Setting Up Appliances.

Setting Up Appliances

Data collectors are available as physical appliances or virtual appliances. Appliances must be set up before you can create a data collector. This section contains:

- Creating Registration Tokens
- Downloading Virtual Appliances
- Setting Up Physical Appliances
- Setting Up Virtual Appliances
- Using Command Line Interface Options

Creating Registration Tokens

A registration token is required when setting up a physical appliance or a virtual appliance.

To create a registration token:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. If no data collectors have been created, the **Get Started** dialog is displayed. Otherwise, the **Data Collectors** page is displayed.
3. Click **Registration Token** in the **Get Started** dialog or the **Configure Appliance** card of the **Data Collectors** page. The registration token is created. The **Registration Token** dialog opens with the token that was created displayed. The date and time the registration token expires is displayed at the bottom of the dialog.
4. Click **Copy Token.** You can now enter this registration token when setting up a physical appliance or virtual appliance during the registration of the appliance (Option 3 (register)) on the **Collector CLI**. For more information about setting up appliances, see Setting Up Appliances.
5. Click **Close**.

Downloading Virtual Appliances

The virtual appliance file (.ova file) is required for setting up a virtual appliance.

To download a virtual appliance:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. If no data collectors have been created, the **Get Started** dialog is displayed. Otherwise, the **Data Collectors** page is displayed.
3. Click **get a virtual appliance** in the **Getting Started** dialog or the **Download Virtual Appliance** link in the **Configure Appliance** card of the **Data Collectors** page. The **Download Virtual Appliance** dialog opens displaying a **Small** virtual appliance card and a **Medium** virtual appliance card. The small virtual appliance requires: 8 Core CPU, 16 GB Memory, and 256 GB disk. The medium virtual appliance requires: 24 Core CPU, 64 GB Memory, and 480 GB disk. Download the virtual appliance by performing the following:
   a. Hover over the **Small** card or the **Medium** card. The **Download File** link is displayed in the card.
   b. Click the **Download File** link in the **Small** card or **Medium** card. The virtual appliance file (.ova) is downloaded. When setting up a virtual appliance using VMWare, you will browse for and select this virtual appliance file (.ova file). For more information about setting up virtual appliances, see Setting Up Appliances.
4. Click **Close.**

Setting Up Physical Appliances

Data collectors are available as physical appliances or virtual appliances. Before you can use an Aruba application that uses data collectors, you need to set up appliances.

To set up a physical appliance, you use several command line options from the **Collector CLI** on the appliance after it is installed. On the **Collector CLI** there are seven options that are available for selection. The options available are listed below:

```
Options:
1. Configure Hostname    4. Configure Proxy      7. Advanced Options
2. Configure Network     5. Change Timezone/NTP  0. Exit
3. Register              6. Test Connectivity
```

You use options 1 through 6 to set up a physical appliance. Perform the options in the order in which they are displayed.

For more information about the advanced options, see Using Command Line Interface Options.

Before You Begin

Before you begin to set up a physical appliance, you need to create a **Registration Token.**

For more information, see Creating Registration Tokens.

About the Physical Appliance

Aruba provides one physical appliance for Aruba ClearPass Device Insight, the Aruba Central Data Collector physical appliance.

Table 53: *Physical Appliance Specifications*

Model	vCPU	Memory	Disk	NICs
DC2000 (Medium)	24	64 GB	480 GB	8 (2 mgmt, 6 data)

Setting Up Physical Appliances

This section discusses how to set up a physical appliance.

NOTE

If you are using a proxy, configure the proxy prior to doing the registration. Additionally, it is recommended that you configure the time zone and NTP prior to registration if you plan on changing them.

To set up a physical appliance:

1. Install on-premises the physical appliance.
2. Power on the appliance and log in to the appliance using these credentials:
   - **Username** = **aruba**
   - **Password** = **aruba**
3. Configure the hostname for the appliance using **Option 1 (Configure Hostname)** on the **Collector CLI.**
4. Configure the network interfaces for the appliance using **Option 2 (Configure Network)** on the **Collector CLI:**
   - Configure the eth0 Ethernet interface.
   - (Optional) Configure the eth1 Ethernet interface.
5. Configure Domain Name System (DNS) for the appliance using **Option 2 (Configure Network)** on the **Collector CLI.**
6. Configure routes for the appliance using **Option 2 (Configure Network)** on the **Collector CLI.**

NOTE

You only need to configure routes if you have configured the eth1 Ethernet interface.

7. Test the connectivity of the appliance to the Cloud URL discovery server using **Option 6 (Test Connectivity)** on the **Collector CLI.**
8. Register the appliance using **Option 3 (Register)** on the **Collector CLI.**
9. Test the connectivity of the appliance to the Aruba cloud using **Option 6 (Test Connectivity)** on the **Collector CLI.**

10. Configure the proxy server using **Option 4 (Configure Proxy)** on the **Collector CLI.**
11. Change the time zone for the appliance using **Option 5 (Change Timezone/NTP)** on the **Collector CLI.**
12. Configure the Network Time Protocol (NTP) server for the appliance using **Option 5 (Change Timezone/NTP)** on the **Collector CLI.**

For more information about the different command line options, see Using Command Line Interface Options.

Setting Up Virtual Appliances

Data collectors are available as virtual appliances or physical appliances. Before you can use an Aruba application that uses data collectors you need to set up appliances.

You can set up virtual appliances using two different methods. You can set up a virtual appliance using the VMware ESXi Host Web Client or the VMware vSphere Desktop Client for Windows. Using either of these methods, you create the virtual machine and then you complete the setup using several command line options from the **Collector CLI** from the virtual machine. On the **Collector CLI** there are seven options that are available for selection. The options available are listed below:

```
Options:
1. Configure Hostname    4. Configure Proxy      7. Advanced Options
2. Configure Network     5. Change Timezone/NTP  0. Exit
3. Register              6. Test Connectivity
```

You use options 1 through 6 to set up a virtual appliance. Perform the options in the order in which they are displayed.

For more information about the advanced options, see Using Command Line Interface Options.

You perform the same command line options when setting up a virtual appliance as you would when setting up a physical appliance.

Before You Begin

Before you begin to set up a virtual appliance you need the following:

- VMware ESXi server
- A VMware ESXi server is required to set up a virtual appliance. You must know the ESXi server host name and IP address when setting up a virtual appliance.
- **Registration Token**
- A registration token is required to set up a virtual appliance.
- For more information, see Creating Registration Tokens.
- Virtual appliance file (**.ova file**)
- A virtual appliance file (.ova file) is required to set up a virtual appliance using VMware.
- For more information, see Downloading Virtual Appliances.

About Aruba Virtual Appliances

Aruba provides two virtual appliances for Aruba ClearPass Device Insight:

- Aruba Central Data Collector virtual appliance (small)
- Aruba Central Data Collector virtual appliance (medium)

Table 54: *Virtual Appliance Specifications*

Model	vCPU	Memory	Disk	NICs
DC1000V (Small)	8	16 GB	256 GB	4 ports (1 G management, DPI up to 100 Mbps)
DC2000V (Medium)	24	64 GB	480 GB	4 ports (1 G management, DPI up to 1 Gbps)

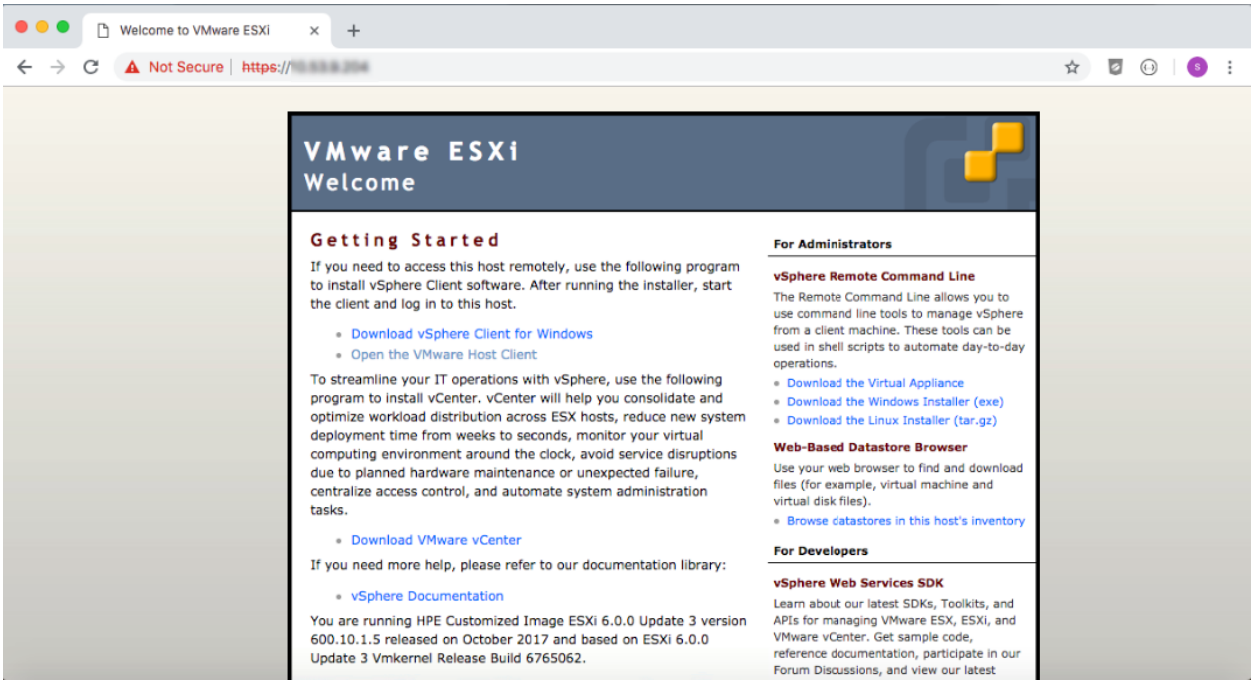
Setting Up Virtual Appliances Using the VMware ESXi Host Web Client

NOTE

If you are using a proxy, configure the proxy prior to doing the registration. Additionally, it is recommended that you configure the time zone and network time protocol (NTP) prior to registration if you plan on changing them.

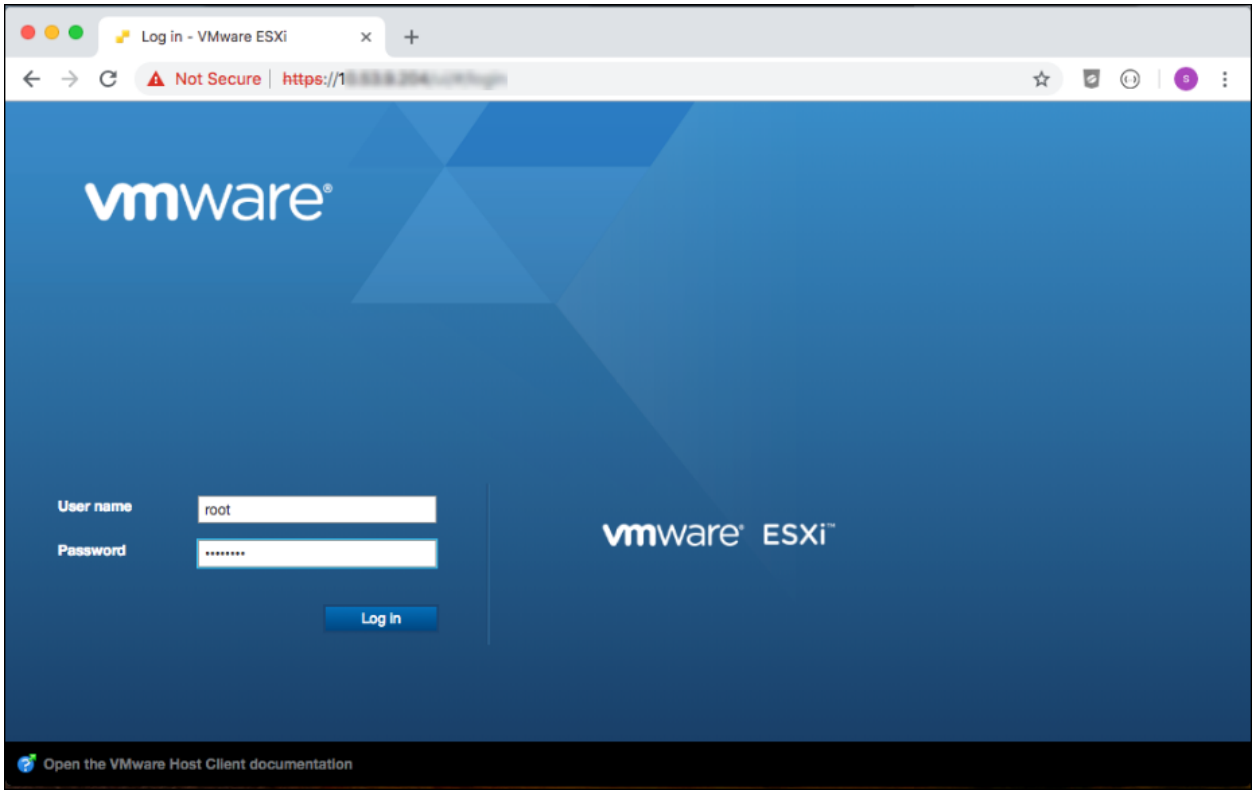
To set up a virtual appliance using the VMware ESXi Host Web Client:

1. Go to a web browser and enter the IP address for the VMware ESXi server.
2. Press **Enter.** The **VMware ESXi Welcome** window appears.

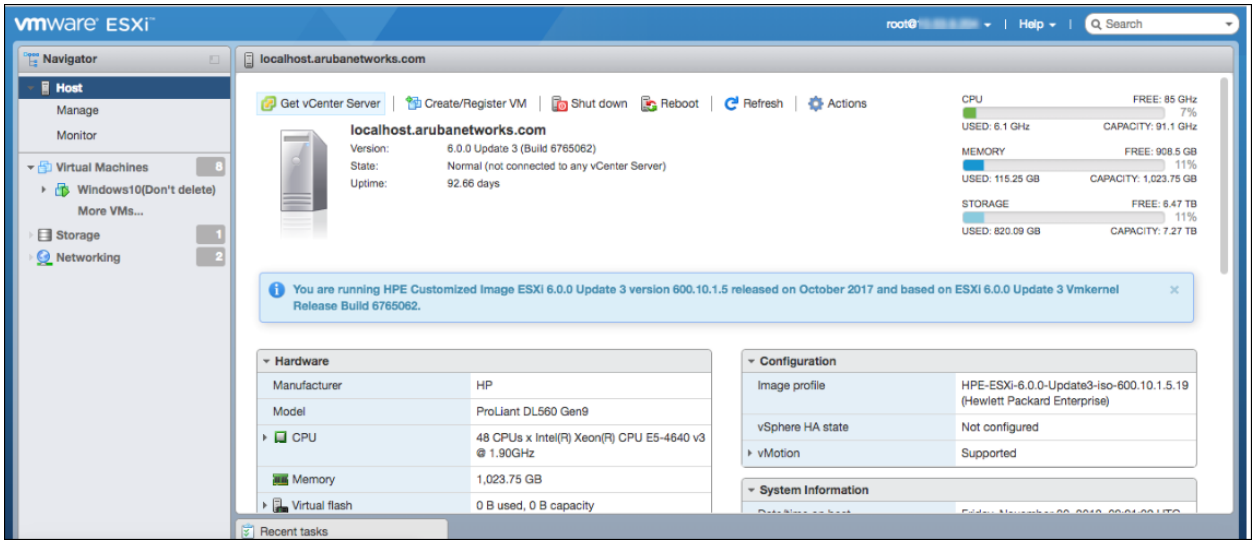


3. Click the **Open the VMware Host Client** link under **Getting Started.** The **VMware ESXi Host Client Log In** window appears.

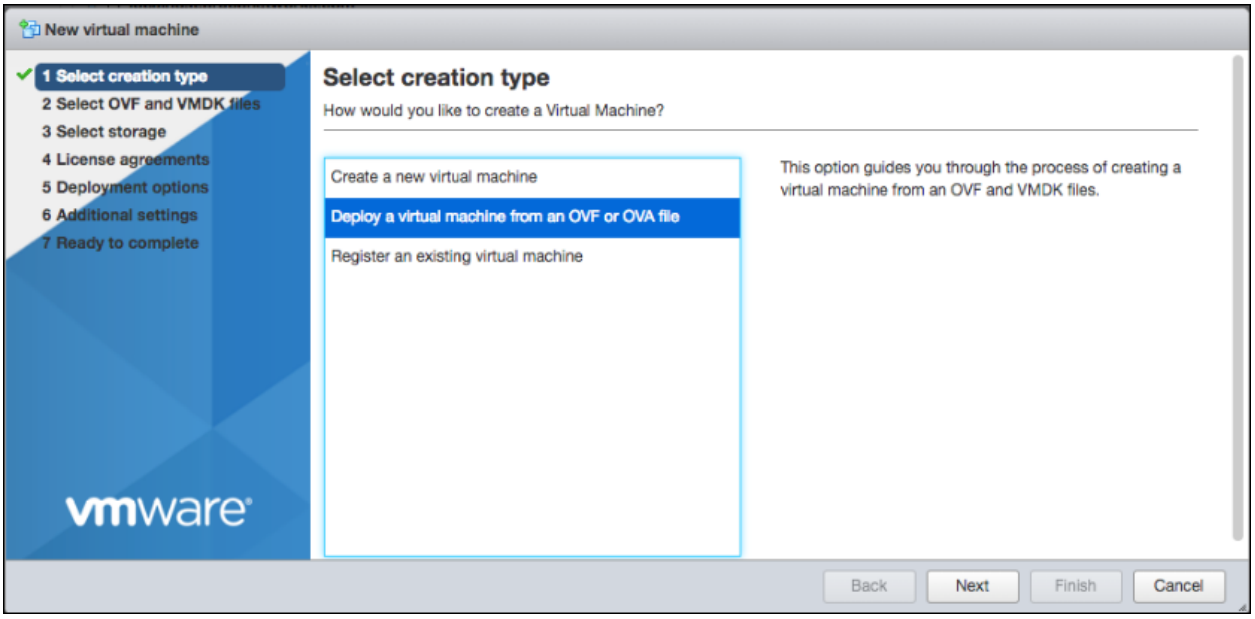
4. Enter the **User name** and **Password** for the ESXi host server.



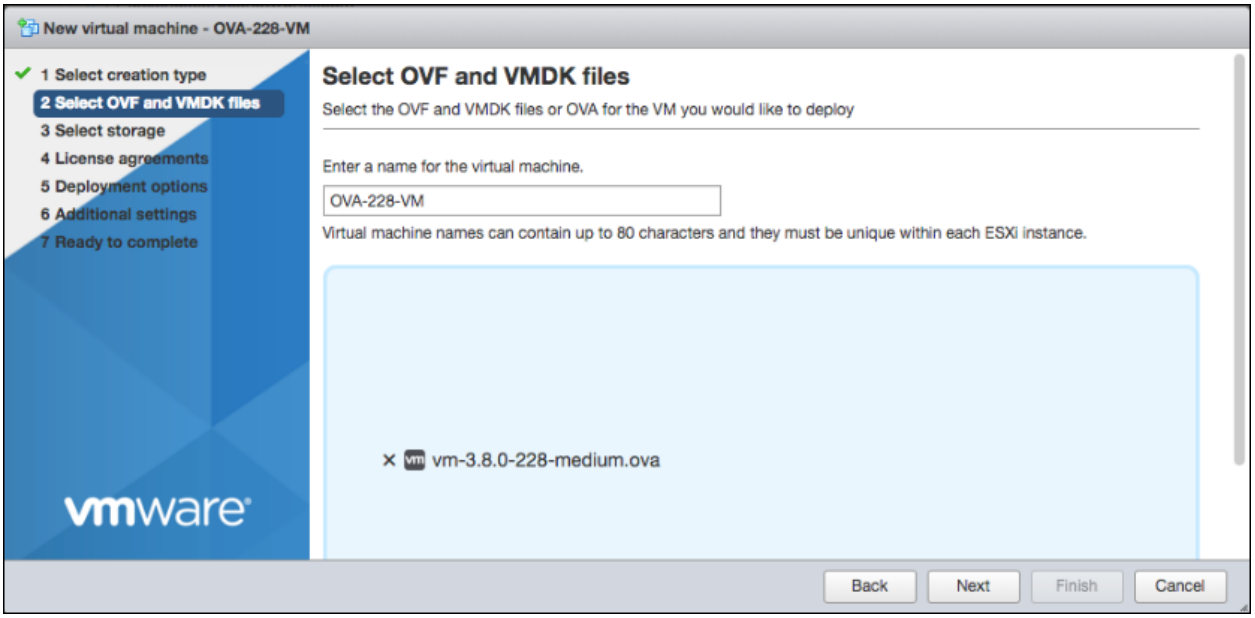
5. Click **Log In.**



6. Click **Create/Register VM** icon. The **New virtual machine- Select creation type** window appears.

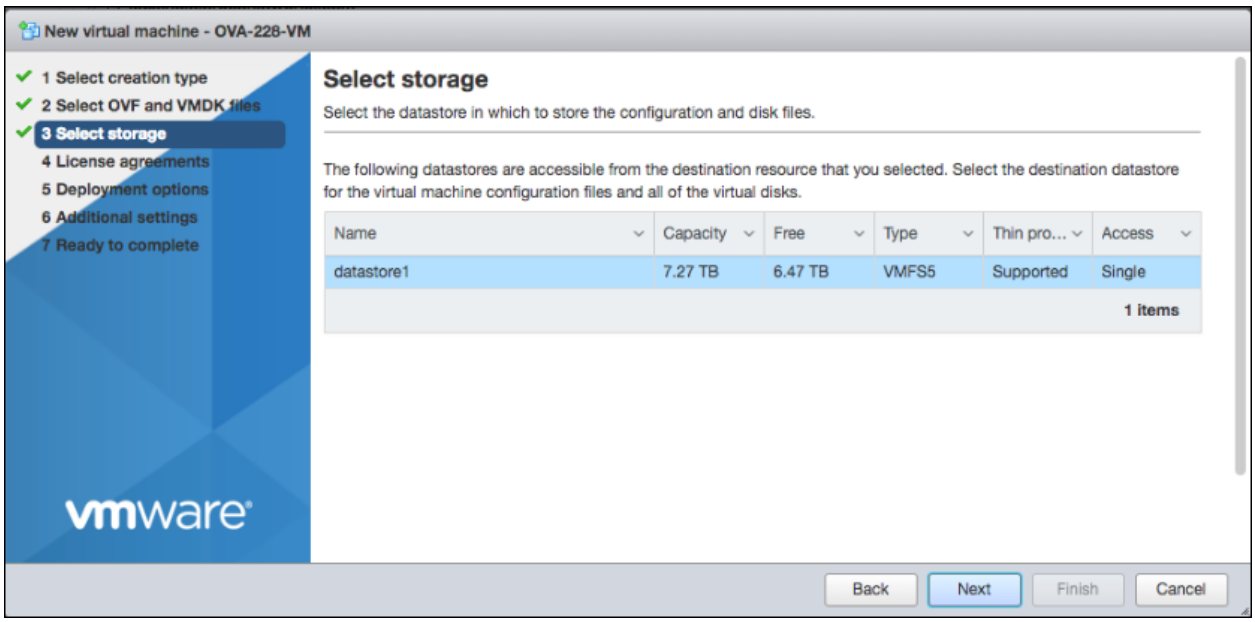


7. Select **Deploy a virtual machine from an OVF or OVA file** for creation type.
8. Click **Next.** The **New virtual machine- Select OVF and VMDK files** window appears.
9. Enter the following:
   a. Enter a name for the virtual machine.
   b. Browse for the ova file and select it.



10. Click **Next.** The **New virtual machine - Select storage** window appears.

11. Select the datastore.



12. Click **Next.** The **New virtual machine - Deployment options** window appears.
13. Enter the following:

NOTE

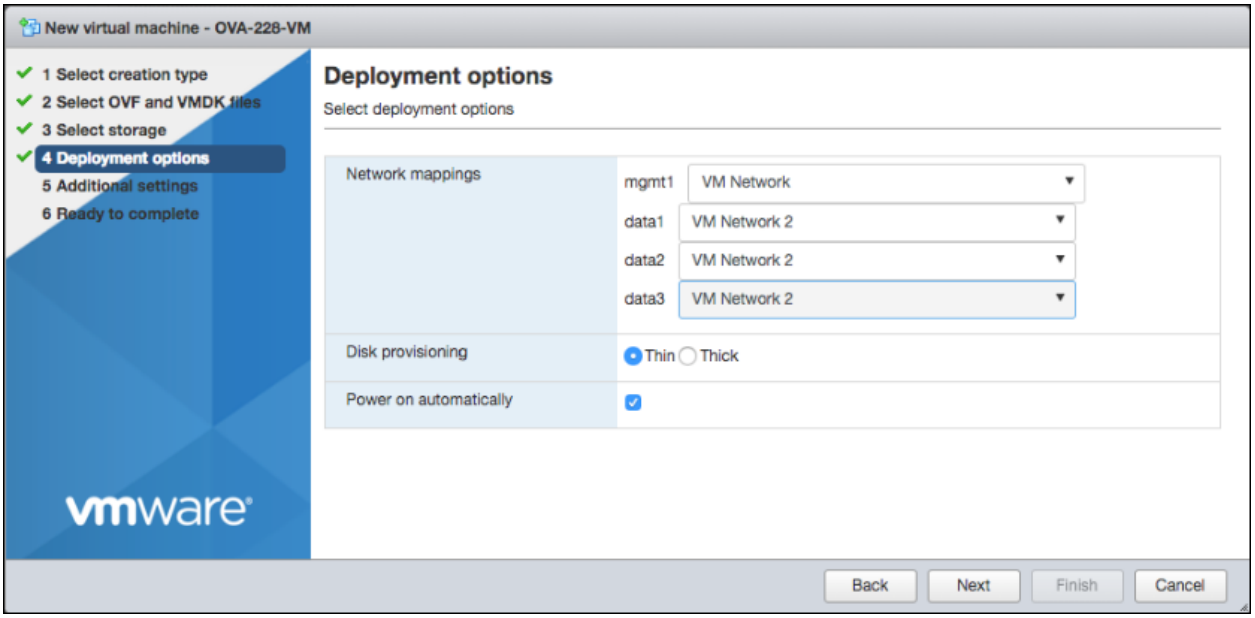
You need to assign a management network and optionally a data network to the virtual machines network adaptors. A virtual machine has network adaptors 1 through 4 to which you can assign the management network, data network, and SPAN networks. You need to identify the network adaptor with the lowest MAC address and assign the management network to this network adaptor. If you have a separate data network, the network adaptor with the second lowest MAC address must be assigned to the data network. You can assign the rest of the network adaptors to the SPAN networks.

a. Select the **Network mapping** for **mgmt1.**
b. Select the **Network mappings** for **data1, data2,** and **data3**.

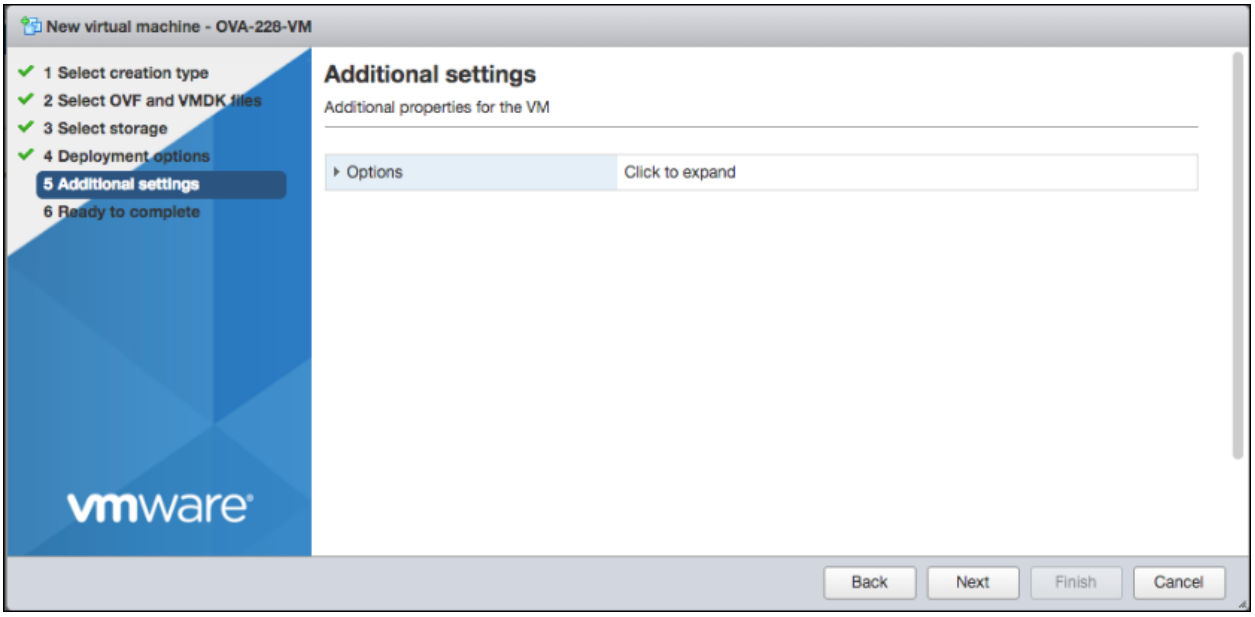
NOTE

Currently, Aruba ClearPass Device Insight supports one management network mapping and one data network mapping.

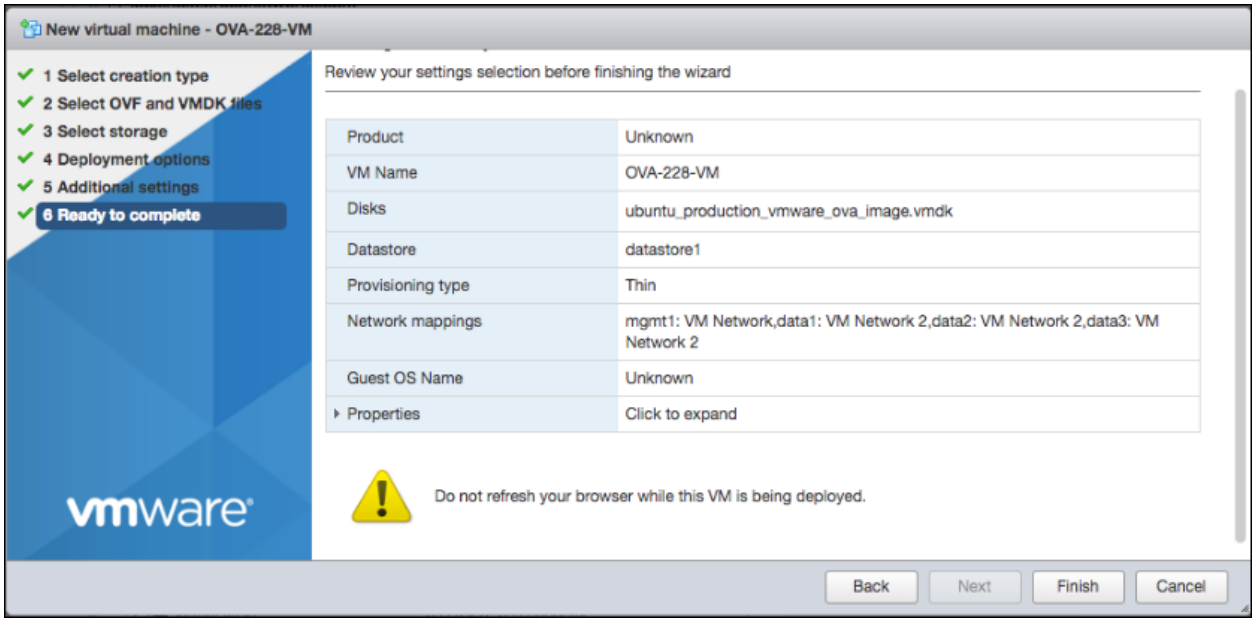
c. Select the **Disk provisioning** option. Options are **Thin** or **Thick. Thin** appears by default.
d. Click the **Power on automatically** check box to have the machine automatically power on. This check box appears selected by default.



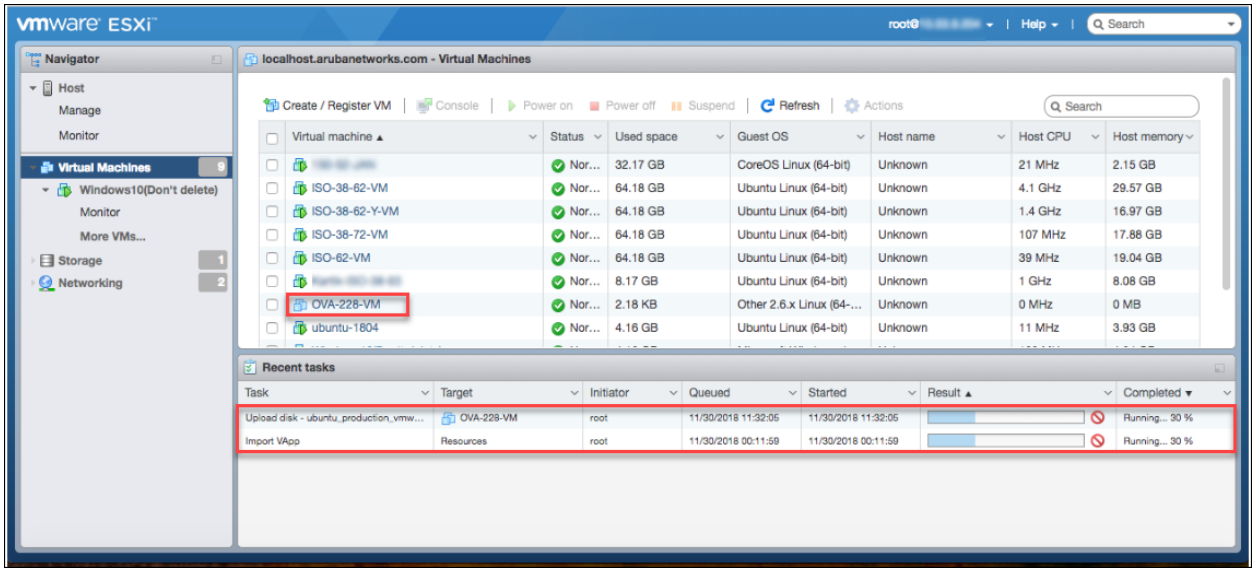
14. Click **Next.** The **New virtual machine - Additional settings** window appears.



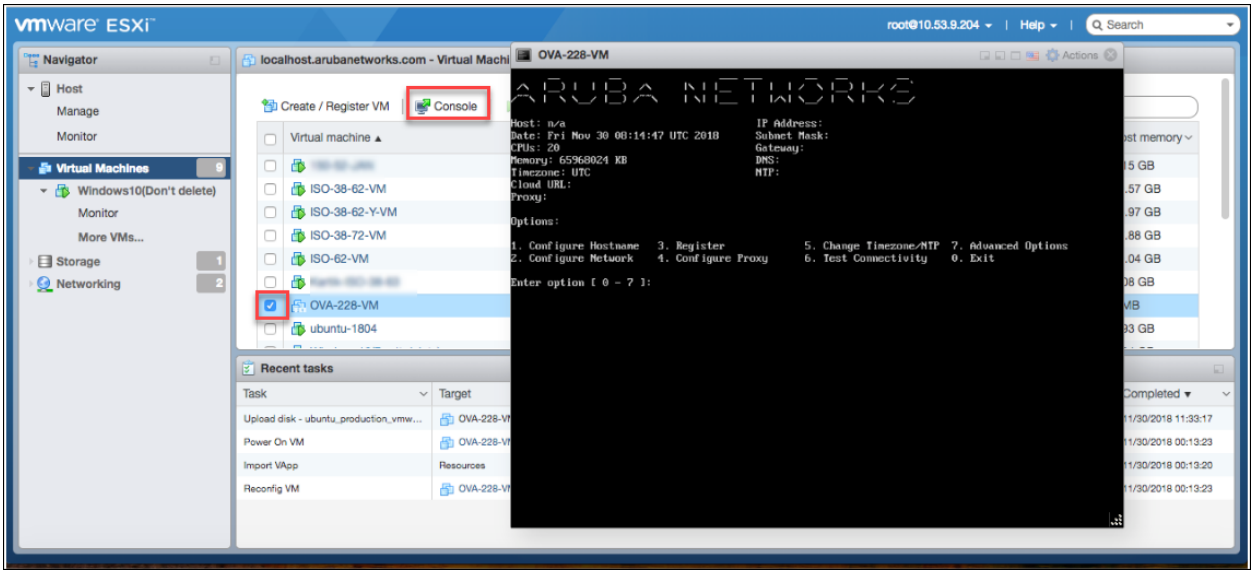
15. Click **Next.** The **New virtual machine - Ready to complete** window appears displaying the selections you made in the previous windows.



16. Click **Finish.** The creation of the virtual machine is initiated. Under **Recent tasks** you can view the results of the new virtual machine tasks by monitoring the **Result** field status bar for each task. Wait until the **Result** field displays **Completed successfully** for each task. When this occurs you have created the virtual machine.



17. Select the new virtual machine that you just created in the upper region of the window and click the **Console** icon. The **Collector CLI** appears.



18. Configure the hostname for the appliance using **Option 1 (Configure Hostname)** on the **Collector CLI.**
19. Configure the network interfaces for the appliance using **Option 2 (Configure Network)** on the **Collector CLI:**
    - Configure the eth0 Ethernet interface.
    - (Optional) Configure the eth1 Ethernet interface.
20. Configure Domain Name System (DNS) for the appliance using **Option 2 (Configure Network)** on the **Collector CLI.**
21. Configure routes for the appliance using **Option 2 (Configure Network)** on the **Collector CLI.**

NOTE

You only need to configure routes if you have configured the eth1 Ethernet interface.

22. Test the connectivity of the appliance to the Cloud URL discovery server using **Option 6 (Test Connectivity)** on the **Collector CLI.**
23. Register the appliance using **Option 3 (Register)** on the **Collector CLI.**
24. Test the connectivity of the appliance to the Aruba cloud using **Option 6 (Test Connectivity)** on the **Collector CLI.**
25. Configure the proxy server using **Option 4 (Configure Proxy)** on the **Collector CLI.**
26. Change the time zone for the appliance using **Option 5 (Change Timezone/NTP)** on the **Collector CLI.**
27. Configure the Network Time Protocol (NTP) server for the appliance using **Option 5 (Change Timezone/NTP)** on the **Collector CLI.**

For more information about the different command line options, see Using Command Line Interface Options.

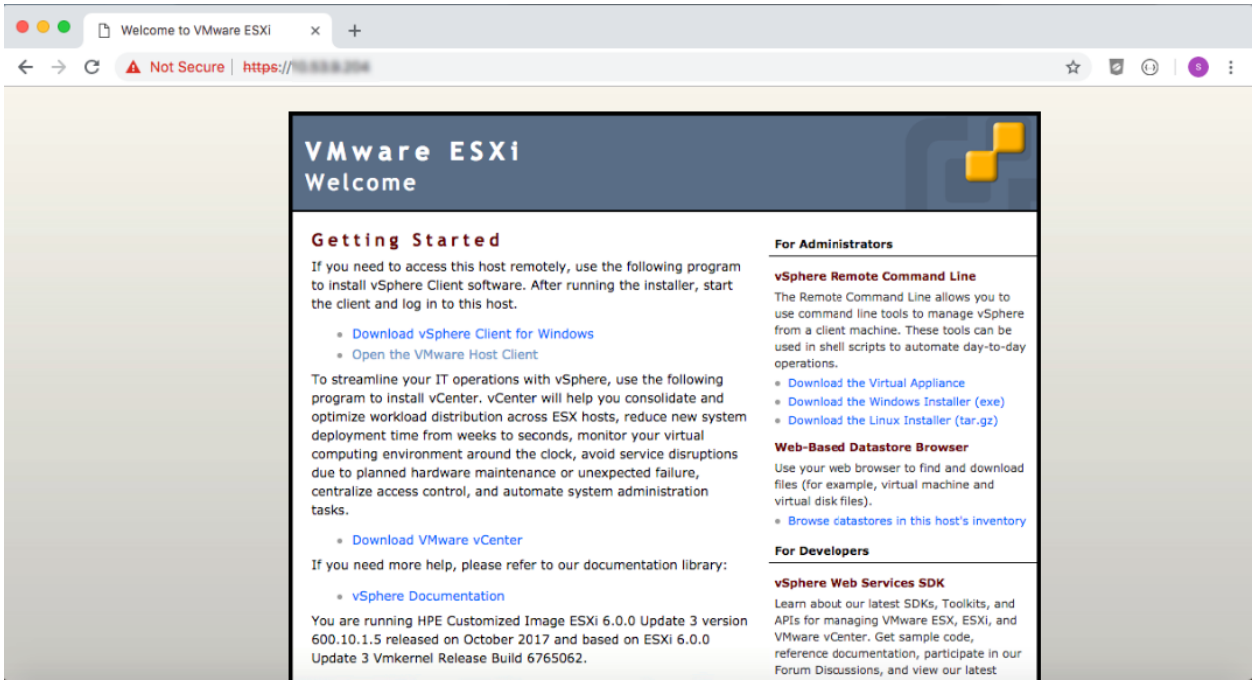
Setting Up Virtual Appliances Using the VMware vSphere Desktop Client for Windows

NOTE

If you are using a proxy, configure the proxy prior to doing the registration. Plus, it is recommended that you configure the time zone and network time protocol (NTP) prior to registration if you plan on changing them.

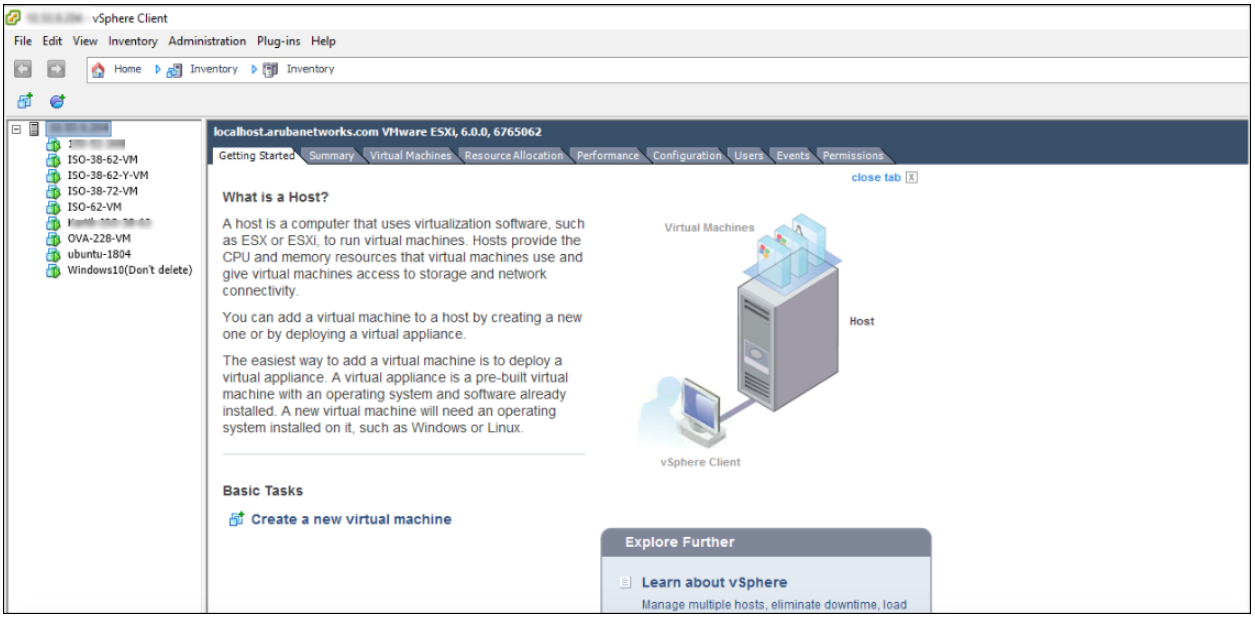
To set up a virtual appliance using the VMware vSphere Desktop Client for Windows:

1. Go to a web browser and enter the IP address for the VMware ESXi server.
2. Press **Enter.** The **VMware ESXi Welcome** window appears.



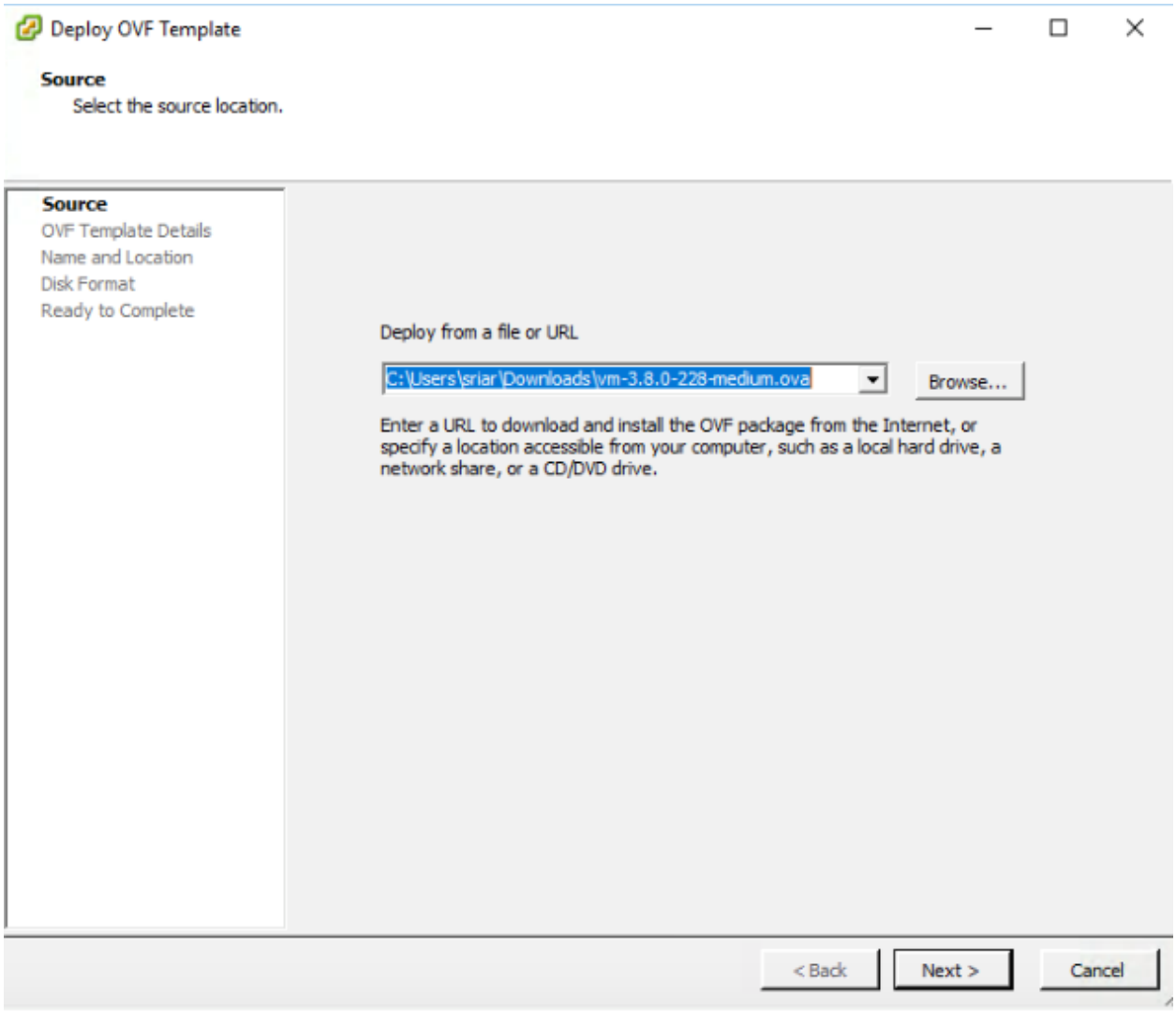
3. Click the **Download vSphere Client for Windows** link under **Getting Started.** The **VMware vSphere Client Log In** window appears.
4. Enter the **User name** and **Password** for the ESXi host server.

5. Click **Login.** The **ESXi Host Details window** appears.

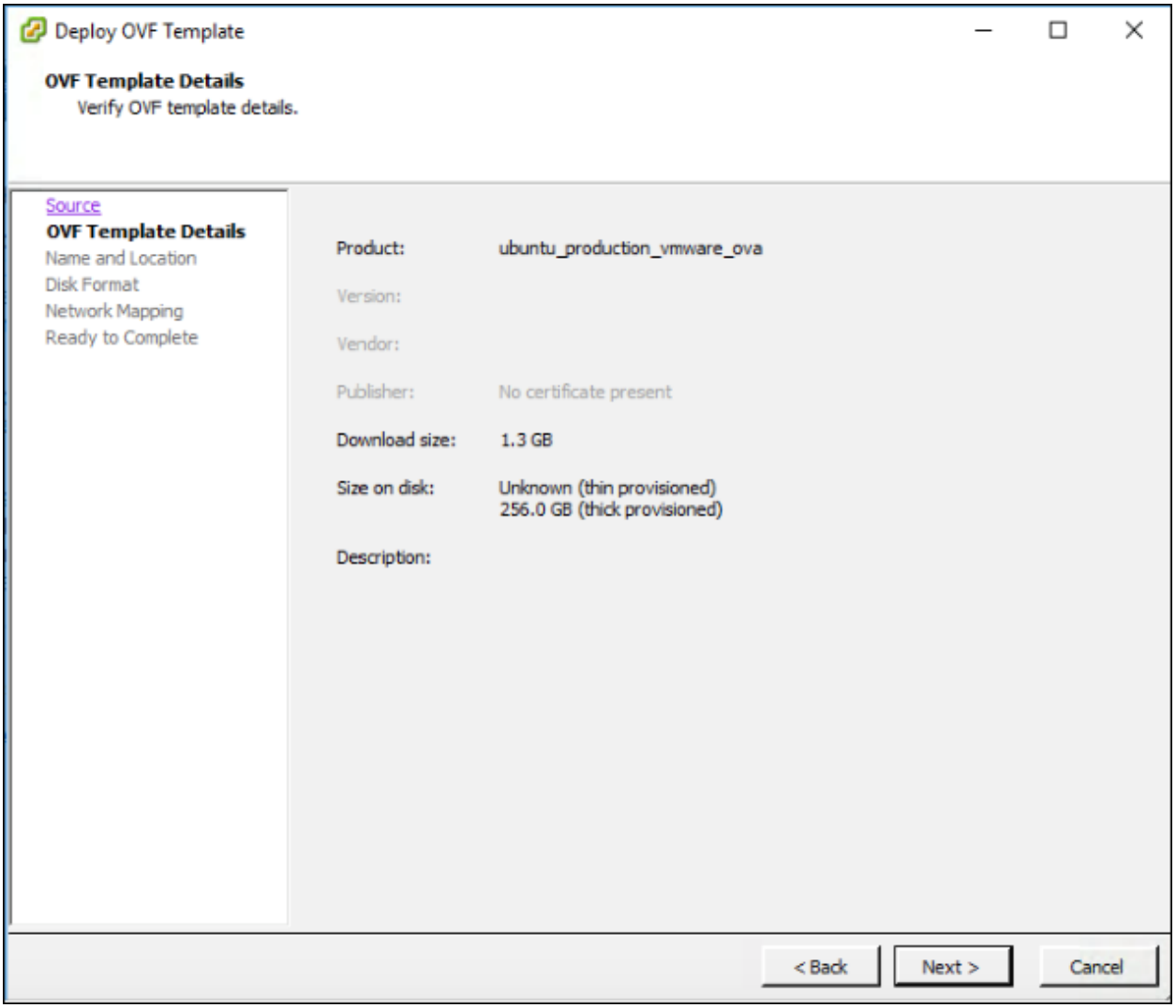


6. Go to **File > Deploy OVF Template.** The **Deploy OVF Template - Source** window appears.

7. Click **Browse** and browse for the ova file and select it.

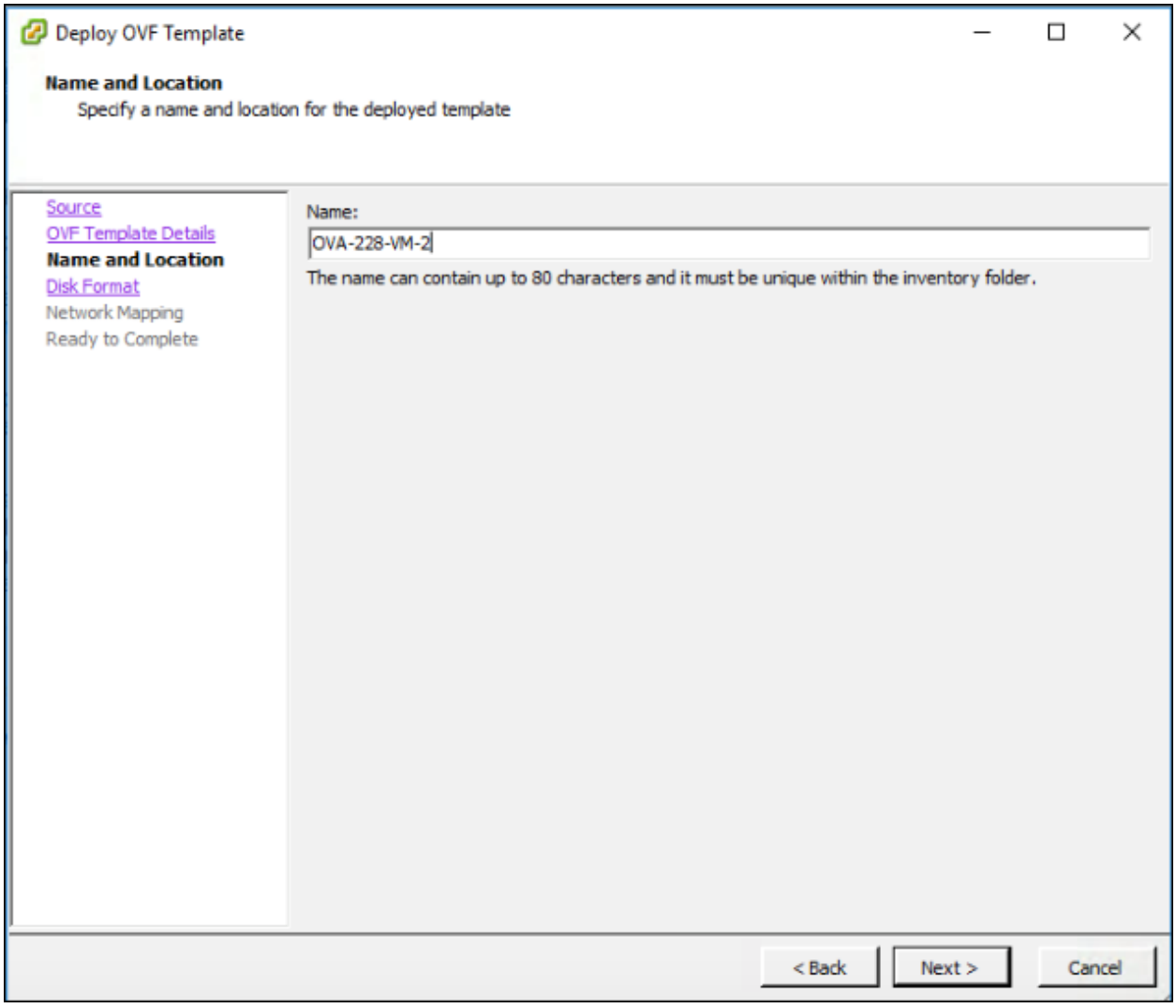


8. Click **Next.** The **Deploy OVF Template - OVF Template Details** window appears displaying the OVF template details.



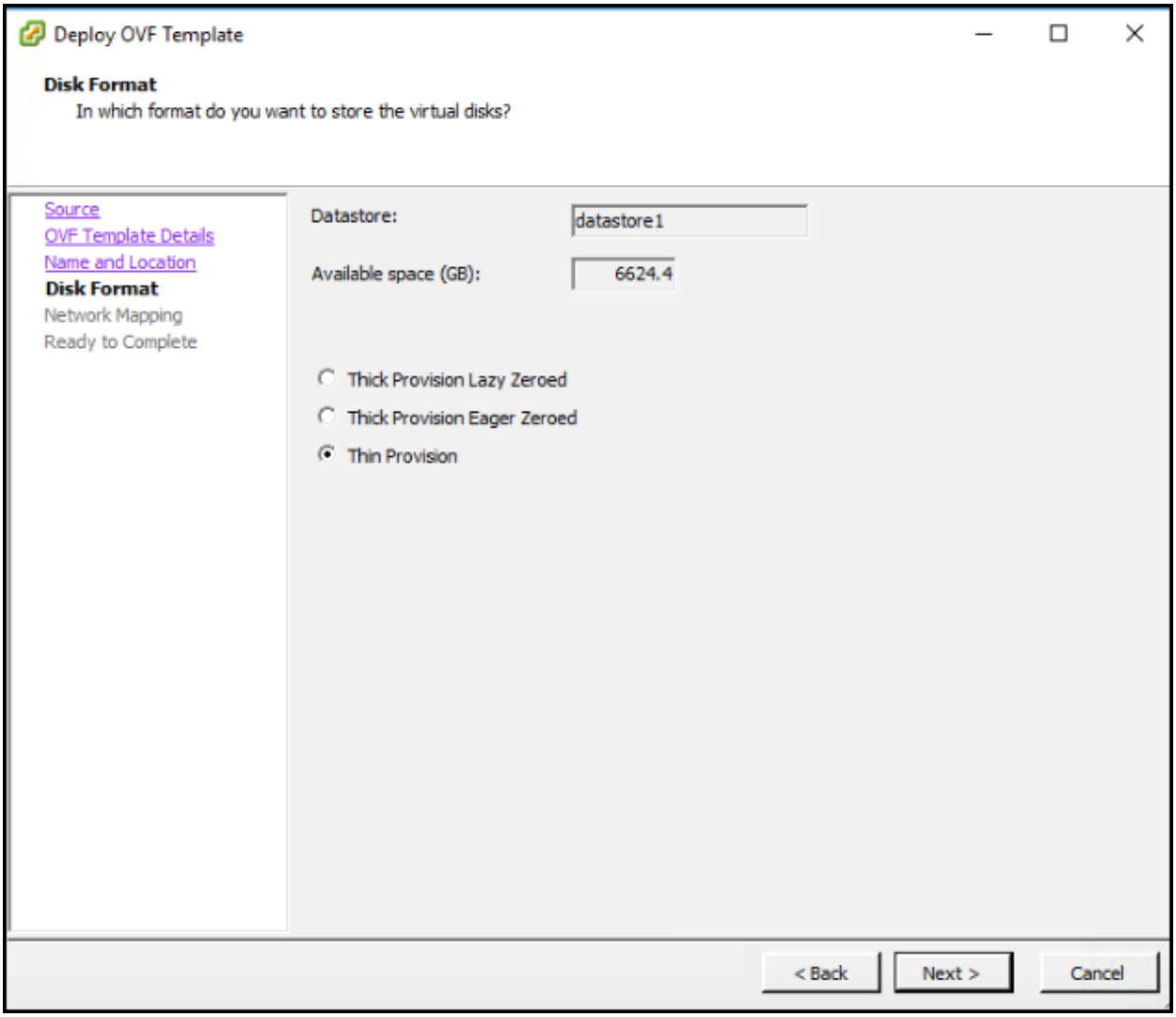
9. Click **Next.** The **Deploy OVF Template - Name and Location** window appears.

10. In the **Name** field enter the name for the virtual appliance.



11. Click **Next.** The **Deploy OVF Template - Disk Format** window appears.
12. Enter the following:
    a. In the **Datastore** field enter the datastore.
    b. Select the disk format. Options are: **Thick Provision Lazy Zeroed, Thick Provision Eager**

Zeroed, and **Thin Provision. Thin Provision** appears selected by default.



13. Click **Next.** The **Deploy OVF Template - Network Mapping** window appears.
14. Enter the following:

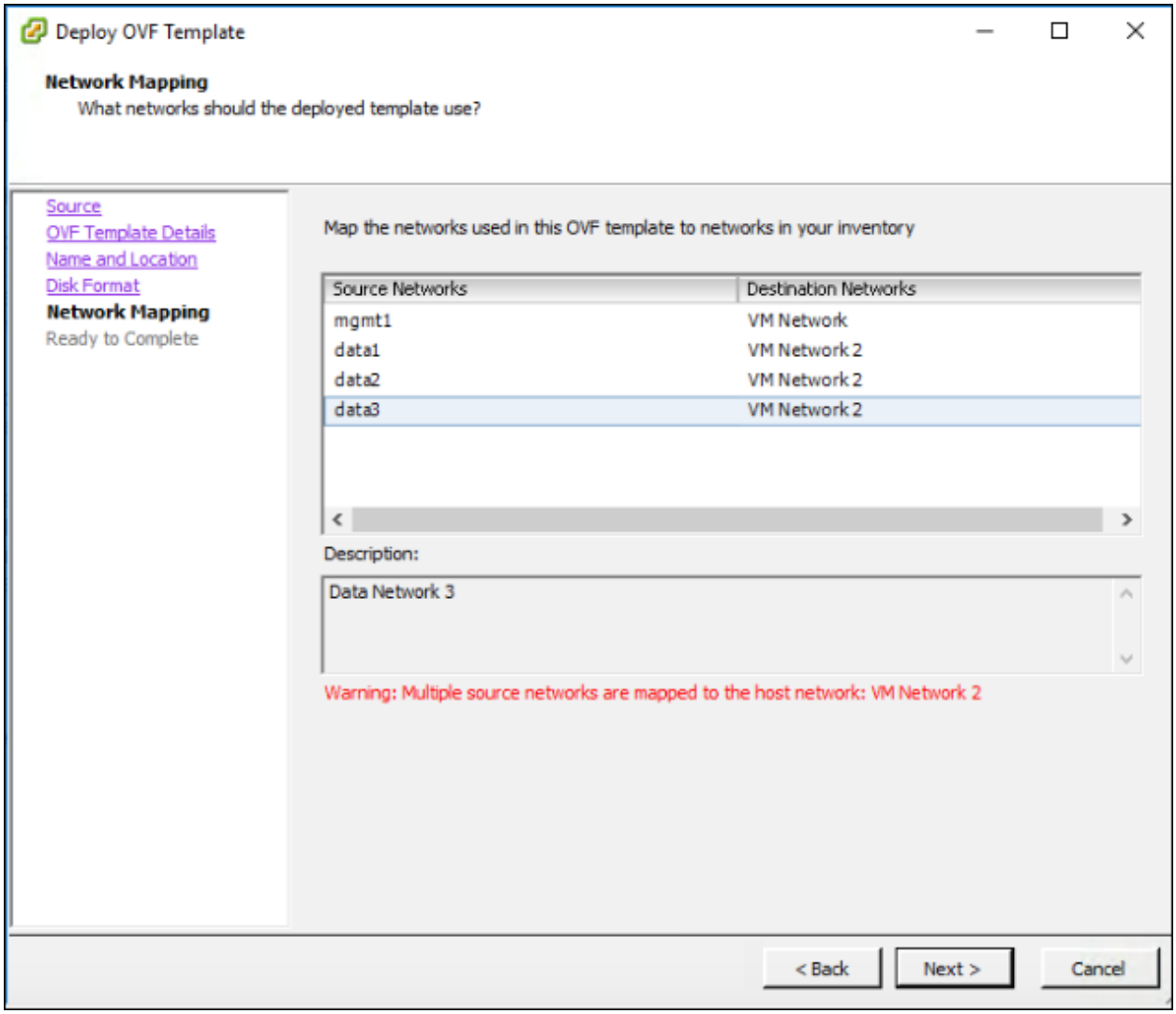
NOTE

You need to assign a management network and optionally a data network to the virtual machines network adaptors. A virtual machine has network adaptors 1 through 4 to which you can assign the management network, data network, and SPAN networks. You need to identify the network adaptor with the lowest MAC address and assign the management network to this network adaptor. If you have a separate data network, the network adaptor with the second lowest MAC address must be assigned to the data network. You can assign the rest of the network adaptors to the SPAN networks.

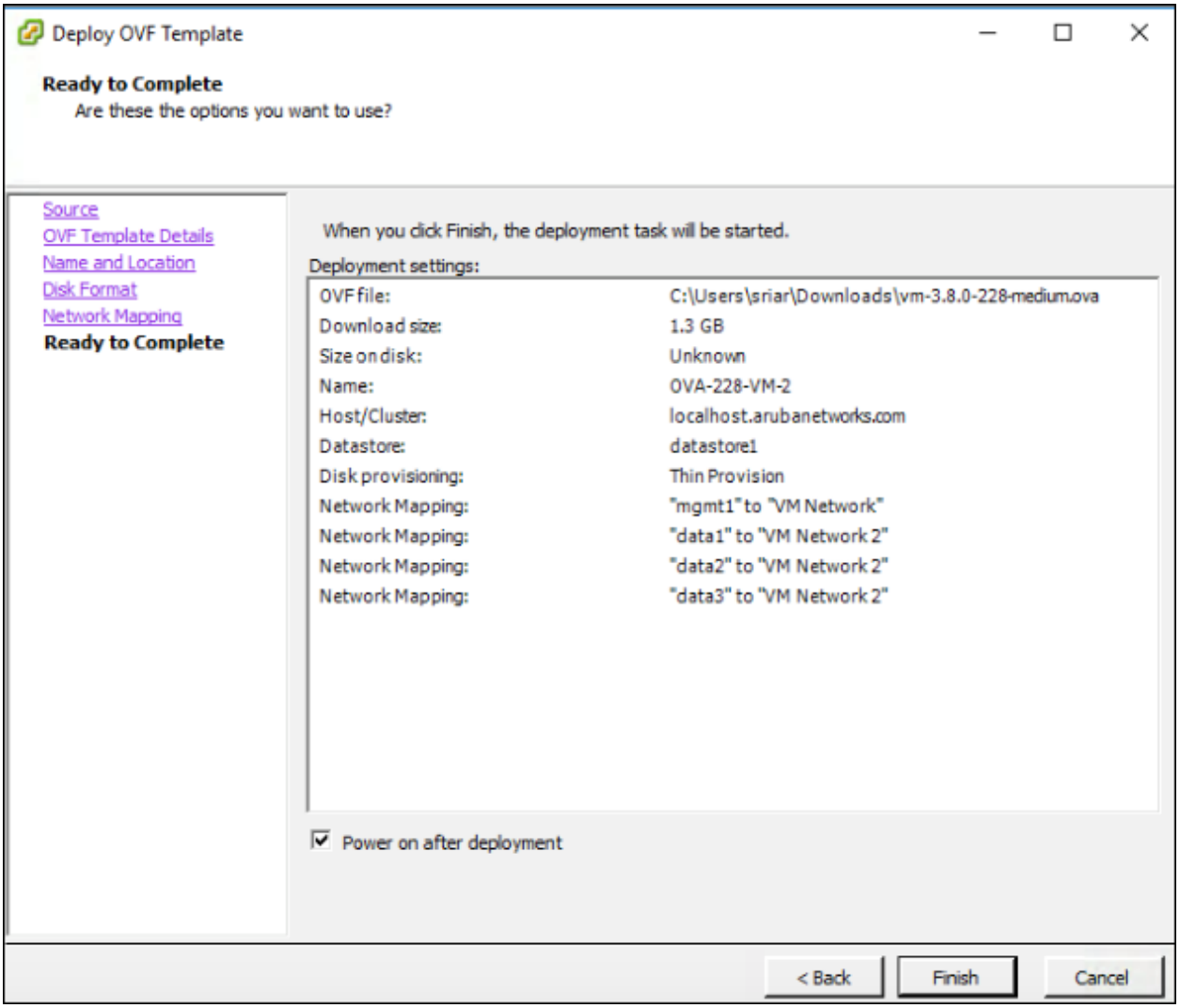
a. Select the **Destination Network** for **mgmt1.**
b. Select the **Destination Networks** for **data1, data2,** and **data3.**

NOTE

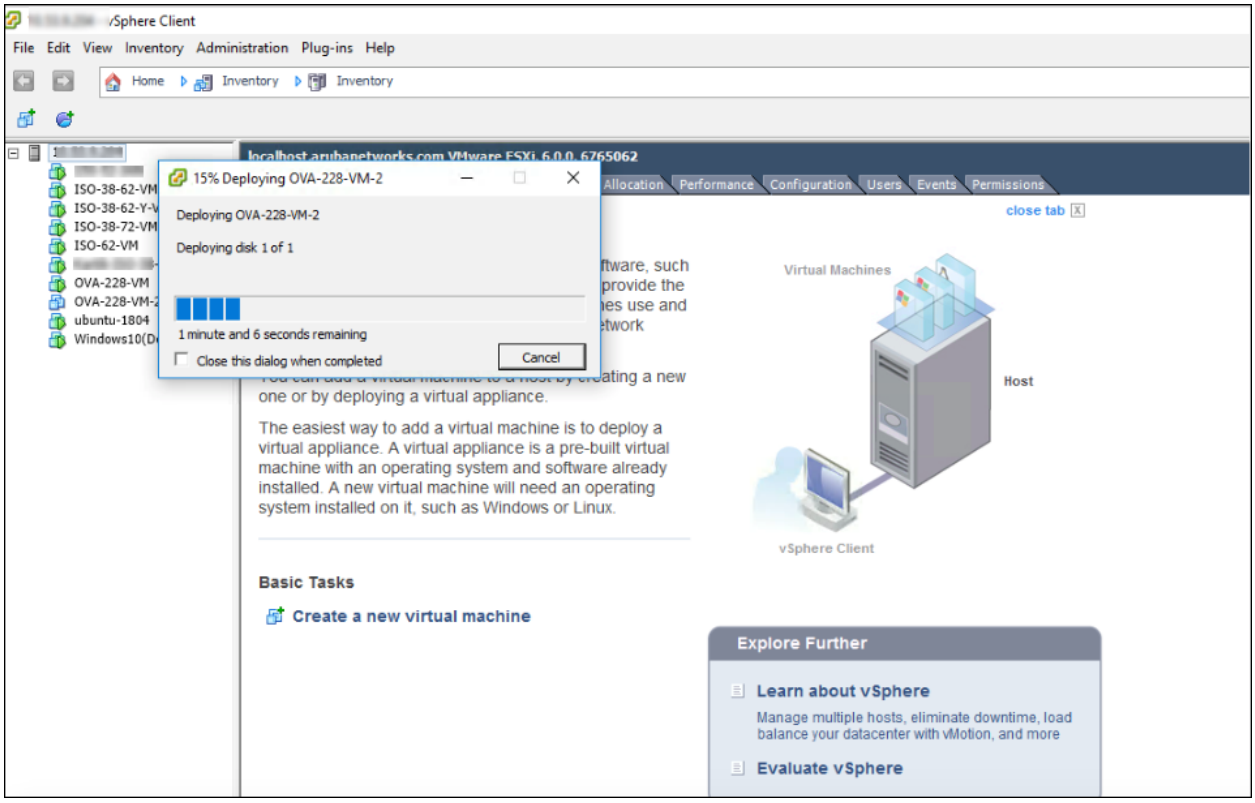
Currently, Aruba ClearPass Device Insight supports one management destination network and one data destination network.



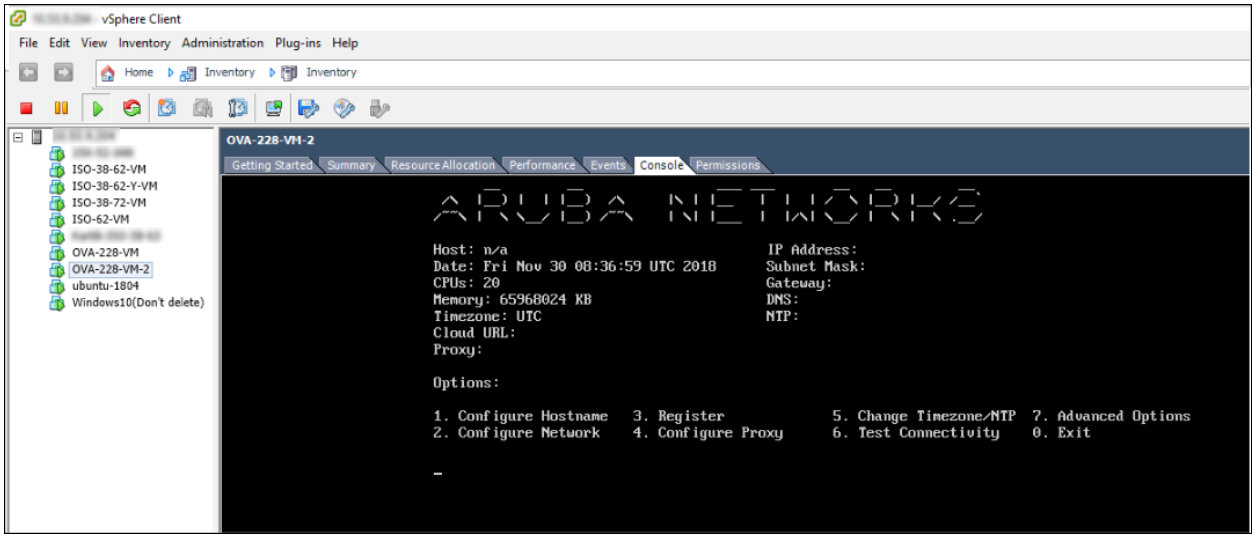
15. Click **Next.** The **Deploy OVF Template - Ready to Complete** window appears.
16. Review the settings and select the **Power on after deployment** check box to have the machine automatically power on. The **Power on after deployment** check box appears selected by default.



17. Click **Finish.** The creation of the virtual machine is initiated. A dialog box appears displaying the status of the virtual machine creation. After the virtual machine is created, it is listed in the **ESXi Host Details** window.



18. Select the virtual machine on the **ESXi Host Details** window and then select the **Console** tab. The **Collector CLI** appears.



19. Configure the hostname for the appliance using **Option 1 (Configure Hostname)** on the **Collector CLI.**
20. Configure the network interfaces for the appliance using **Option 2 (Configure Network)** on the **Collector CLI:**
    - Configure the eth0 Ethernet interface.
    - (Optional) Configure the eth1 Ethernet interface.
21. Configure Domain Name System (DNS) for the appliance using **Option 2 (Configure Network)** on the **Collector CLI.**

22. Configure routes for the appliance using **Option 2 (Configure Network)** on the **Collector CLI.**

You only need to configure routes if you have configured the eth1 Ethernet interface.

23. Test the connectivity of the appliance to the Cloud URL discovery server using **Option 6 (Test Connectivity)** on the **Collector CLI.**
24. Register the appliance using **Option 3 (Register)** on the **Collector CLI.**
25. Test the connectivity of the appliance to the Aruba cloud using **Option 6 (Test Connectivity)** on the **Collector CLI.**
26. Configure the proxy server using **Option 4 (Configure Proxy)** on the **Collector CLI.**
27. Change the time zone for the appliance using **Option 5 (Change Timezone/NTP)** on the **Collector CLI.**
28. Configure the Network Time Protocol (NTP) server for the appliance using **Option 5 (Change Timezone/NTP)** on the **Collector CLI.**

For more information about the different command line options, see Using Command Line Interface Options.

Using Command Line Interface Options

This section describes how to use the different command line interface (CLI) options for an appliance. Several of these options are used when setting up a physical appliance or a virtual appliance.

This section contains:

Configuring Hostname

This section describes how to configure hostname for an appliance and how to edit the hostname after it has been configured.

Configuring Hostname

To configure hostname:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **1** (Configure Hostname) and press **Enter.**
3. In the **New hostname** field, enter the hostname and press **Enter.** The hostname must start with a letter and can contain letters, numbers, and a hyphen "-". It can not contain any other special characters. A message is displayed stating that the hostname has been changed successfully.
4. Press **Enter.**

Editing Configured Hostname

This option is available only after you have configured the hostname.

To edit configured hostname:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **1** (Configure Hostname) and press **Enter.**
3. In the **Enter option** field, enter **1** (Edit Hostname) and press **Enter.**
4. In the **New hostname** field, enter the hostname and press **Enter.** The hostname must start with a letter and can contain letters, numbers, and a hyphen "-". It can not contain any other special characters. A message is displayed stating that the hostname has been changed successfully.
5. Press **Enter.**

Configuring Network

This section describes how to configure the network interfaces, domain system name, and routes for the appliance and how to show the interfaces information for the appliance.

Configuring Network Interfaces

To configure network interfaces:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **2** (Configure Network) and press **Enter.**
3. In the **Enter option** field, enter **1** (Configure Network Interfaces) and press **Enter.**
4. In the **Enter option** field, enter **0** (eth0) and press **Enter.**

You must configure the eth0 (management) Ethernet interface. Configuring the eth1 (data) Ethernet interface is optional. The MAC Address is displayed in brackets next to eth0 and eth1.

5. In the **Enter IP Address** field, enter the IP address for the appliance and press **Enter.**
6. In the **Enter Subnet mask** field, enter the subnet mask for the appliance and press **Enter.**
7. In the **Enter Gateway** field, enter the gateway address for the appliance and press **Enter.**
8. (Optional) Configure the second ethernet interface (eth1). Repeat steps 4 through 7 above except in step 4 enter **1** (eth1).
9. In the **Enter option** field, enter **b** (Back to Previous Menu) and press **Enter.**
10. Press **Enter.**
11. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Configuring DNS

To configure Domain Name System (DNS):

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **2** (Configure Network) and press **Enter.**
3. In the **Enter option** field, enter **2** (Configure DNS) and press **Enter.**
4. In the **Enter DNS** field, enter the DNS address for the appliance and press **Enter.**
5. (Optional) In the **Enter Secondary DNS** field, enter the secondary DNS address for the appliance and press **Enter.** Otherwise, press **Enter** to proceed without entering a secondary DNS address.
6. Press **Enter.**
7. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Configuring Routes

You only need to configure routes if you have configured ethernet interface eth1. Routes do not apply to ethernet interface eth0.

Listing All Routes

To list all routes:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **2** (Configure Network) and press **Enter.**
3. In the **Enter option** field, enter **3** (Configure Routes) and press **Enter.**
4. In the **Enter option** field, enter **1** (List all routes) and press **Enter.** All of the routes are displayed.
5. Enter **b** (Back to Previous Menu) and press **Enter.**
6. Press **Enter.**
7. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Adding a Route Via eth1

To add a route through eth1:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **2** (Configure Network) and press **Enter.**
3. In the **Enter option** field, enter **3** (Configure Routes) and press **Enter.**
4. In the **Enter option** field, enter **2** (Add a route via eth1) and press **Enter.**
5. In the **Enter destination IP Address** field, enter the IP address of the node that needs to connect to the eth1 interface and press **Enter.** The route is created. The system assigns a sequential index number to the route. You can view the index number assigned to the route by using Option 1 - List all routes.
6. Enter **b** (Back to Previous Menu) and press **Enter.**
7. Press **Enter.**
8. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Deleting a Route Via eth1

To delete a route through eth1:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **2** (Configure Network) and press **Enter.**
3. In the **Enter option** field, enter **3** (Configure Routes) and press **Enter.**
4. In the **Enter option** field, enter **3** (Delete a route via eth1) and press **Enter.**
5. In the **Enter index of route to be deleted** field, enter the index number associated with the route to be deleted and press **Enter.**
6. Enter **b** (Back to Previous Menu) and press **Enter.**
7. Press **Enter.**
8. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Showing Interfaces Information

To show interfaces information:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **2** (Configure Network) and press **Enter.**
3. In the **Enter option** field, enter **4** (Show Interfaces Info) and press **Enter.**
4. The information for both eth0 and eth1 network interfaces is displayed. The **IP address, Netmask, Gateway,** and **MAC Address** is displayed for each interface.
5. Press **Enter.**
6. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Registering the Appliance

To register the appliance:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **3** (Register) and press **Enter.**
3. In the **Registration code** field, enter the registration code and press **Enter.** The registration process is initiated. The registration process associates the appliance with your customer account. After the registration process completes, a message is displayed that the registration was successful. The appliance is now available to be formed into a data collector by installing an Aruba application on it. The appliance count that is displayed in the **Create Collector** card on the **Data Collectors** page is incremented by one. For information about creating a data collector, see Creating Data Collectors.
4. Press **Enter.**

Configuring Proxy Server

This section describes how to configure a proxy server, edit a proxy server configuration, and unconfigure a proxy server.

Configuring Proxy Server

To configure proxy server:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **4** (Configure Proxy) and press **Enter.**
3. In the **Proxy Server URL/IP** field, enter the URL or IP address for the proxy server and press **Enter.**
4. In the **Proxy Server Port** field, enter the port and press **Enter.** Otherwise, press **Enter** to accept the default port. **3128** appears as the default port.
5. In the **Username** field, enter the user name for the server and press **Enter.**
6. In the **Password** field, enter the password for the server and press **Enter.** A password can not contain any special characters. A message is displayed stating the proxy server has been configured.
7. Press **Enter.**

Editing Proxy Configuration

This option is available only after you have configured a proxy server.

To edit proxy configuration:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **4** (Configure Proxy) and press **Enter.**
3. In the Enter option field enter **1** (Edit Proxy Configuration) and press **Enter.**

4. In the **Proxy Server URL/IP** field, enter the URL or IP address for the proxy server and press **Enter.**
5. In the **Proxy Server Port** field, enter the port and press **Enter.** Otherwise, press **Enter** to accept the default port. **3128** appears as the default port.
6. In the **Username** field, enter the user name for the server and press **Enter.**
7. In the **Password** field, enter the password for the server and press **Enter.** A password can not contain any special characters. A message is displayed stating the proxy server has been configured.
8. Press **Enter.**

Unconfiguring Proxy Configuration

This option is available only after you have configured a proxy server.

To unconfigure proxy configuration:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **4** (Configure Proxy) and press **Enter.**
3. In the Enter option field, enter **2** (Unconfigure Proxy) and press **Enter.** A message is displayed stating the proxy server is being disabled.
4. Press **Enter.**

Changing Time Zone and Configuring NTP Server

This section describes how to change the time zone and how to configure the NTP server.

Changing Time Zone

To change the time zone:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **5** (Change Timezone/NTP) and press **Enter.**
3. In the **Enter option** field, enter **1** (Change Timezone) and press **Enter.** The following regions are displayed:
   - **1- Africa**
   - **2 - America**
   - **3 - Antarctica**
   - **4 - Arctic**
   - **5 - Asia**
   - **6 - Atlantic**
   - **7 - Australia**
   - **8 - Europe**
   - **9 - Indian**
   - **10 - Pacific**
   - **11 - UTC**
4. In the **Select region** field, enter the number for the region and press **Enter.** For example, to select the Pacific region enter **10.** The time zones for the region you selected are displayed.
5. In the **Select timezone** field, enter the number for the time zone and press **Enter.** A message is displayed that the time zone was configured. Press **Enter.**
6. In the **Enter option** field enter **m** (Main Menu) and press **Enter.**

Configuring NTP Server

To configure Network Time Protocol (NTP) server:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **5** (Change Timezone/NTP) and press **Enter.**
3. In the **Enter option** field, enter **2** (Configure NTP) and press **Enter.**
4. In the **NTP Server** field, enter the NTP server hostname and press **Enter.** A message is displayed that the NTP server has been configured.
5. Press **Enter.**
6. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Testing Appliance Connectivity

The section describes how to test the appliances connectivity to the Aruba cloud and to another host.

Testing Aruba Cloud Reachability

To test Aruba cloud reachability:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **6** (Test Connectivity) and press **Enter.**
3. In the **Enter option** field, enter **1** (Test Aruba Cloud reachability) and press **Enter.** This process performs two connectivity tests. The first test, tests the reachability of the appliance to the Cloud URL discovery server. This test you perform before you register the appliance. The second test, tests the reachability of the appliance to the Aruba cloud. This test you perform after you register the appliance. When you perform this process before registration, the following messages are displayed:

```
Testing reachability to Cloud URL discovery server ...

Cloud URL discovery server reachable

Aruba Cloud URL is not set. Please activate the node.

When you perform this process after registration, the following messages are
displayed:

Testing reachability to Cloud URL discovery server ...

Cloud URL discovery server reachable

Testing cloud reachability.....

Aruba cloud is reachable
```

4. Press **Enter.**

Testing Connectivity to Another Host

To test connectivity to another host:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **6** (Test Connectivity) and press **Enter.**
3. In the **Enter option** field, enter **2** (Test connectivity to another host (using PING)) and press **Enter.**

4. In the **Type host address** field, enter the host address you want to reach and press **Enter.** A message is displayed whether the host is reachable or not.
5. Press **Enter.**

Performing Advanced Options

This section describes how to complete advanced tasks for appliances such as changing the password, enabling support access, and resetting the factory settings.

Rebooting or Shutting Down

Rebooting

To reboot:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **7** (Advanced Options) and press **Enter.**
3. In the **Enter option** field, enter **1** (Reboot/Shutdown) and press **Enter.**
4. In the **Enter option** field, enter **1** (Reboot) and press **Enter.**
5. At the prompt, **Are you sure you want to reboot the node?** enter **y** and press **Enter.** The appliance is rebooted.

Shutting Down

To shutdown:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **7** (Advanced Options) and press **Enter.**
3. In the **Enter option** field, enter **1** (Reboot/Shutdown) and press **Enter.**
4. In the **Enter option** field, enter **2** (Shutdown) and press **Enter.**
5. At the prompt, **Are you sure you want to shutdown the node?** enter **y** and press **Enter.** The appliance is shutdown.

Changing Password

To change password:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **7** (Advanced Options) and press **Enter.**
3. In the **Enter option** field, enter **2** (Change password) and press **Enter.**
4. At the prompt, **Are you sure you want to change the password?** enter **y** and press **Enter.**
5. In the **Enter new UNIX password** field, enter the new password and press **Enter.**
6. In the **Retype new UNIX password** field, re-enter the new password and press **Enter.** A message is displayed that the password has been updated successfully.
7. Press **Enter.**
8. In the **Enter option** field, enter **m** (Main Menu) and press **Enter.**

Enabling Support Access

Enabling support access provides a way for Aruba customer support to access the collector remotely for any troubleshooting. This requires both enabling support access on the collector and providing consent in Aruba Central.

Enabling Support Access on the Collector

To enable support access on the collector:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **7** (Advanced Options) and press **Enter.**
3. In the **Enter option** field, enter **3** (Enable support access) and press **Enter.**
4. In the **Select an option** field, enter **1** (Enable support access) and press **Enter.**
5. In the **Allow access for user** field, enter the email address for the Aruba Technical Assistance Center (TAC) support contact you wish to enable access and press **Enter.** An **Access Token** is generated and is displayed.
6. Send that **Access Token** to the Aruba TAC support contact through email or when speaking with them over the phone. The TAC support contact takes that access token and generates a decoded password. From there they can access the appliance remotely using an application such as Webex or Remote Control Service (RCS).
7. Press **Enter.**
8. In the **Enter option** field, enter **m** (Main Menu) and press Enter.

Providing Consent in Aruba Central

To provide consent in Aruba Central:

1. Go to Aruba Central (if you are in the Analyzer portal, there is an option on the top right to switch to Aruba Central.
2. Go to **User Management.**
3. In the **Actions** drop down located in the top right, select **Enable Support Access.** A popup appears.
4. Toggle the **Enable Support Access** option and enable it.
5. Select **Get Password.** We do not need the password. It can be ignored for the purpose of accessing the collector.

Disabling Support Access

The support access, once enabled, remains until it is disabled. For security reasons it is recommended that you disable the access once it is no longer required by Aruba customer support.

To disable support access:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **7** (Advanced Options) and press **Enter.**
3. In the **Enter option** field, enter **3** (Enable support access) and press **Enter.**
4. In the **Select an option** field, enter **2** (Disable support access) and press **Enter.**
5. Press **Enter.**

Transferring Logs Through SCP

When troubleshooting an issue, you may want to transfer the logs that have been generated from the appliance. For this transfer to occur you need to have a Linux server that is Secure Shell (SSH) enabled.

To transfer logs through SCP:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **7** (Advanced Options) and press **Enter.**
3. In the **Enter option** field, enter **4** (Transfer logs through SCP) and press **Enter.**

4. In the **SCP server configuration** field, enter the hostname and IP address for the server and press **Enter.** Before the logs are transferred they are compressed. On the Collector CLI the status of the compression is displayed. 100% is displayed after compression is complete.
5. In the **server password** field, enter the password for the server and press **Enter.** A tar file is created for the logs. The date and time when the tar file was created is a part of the name of the file. For example, if a tar file is named (ISO-38-41-PH_logs_11021729.tar.gz) the date and time it was created is November, 2 at 17:29. The time zone reflected is the appliance time zone where the tar file was created.
6. Press **Enter.**

Resetting Factory Settings

This option applies only to physical appliances.

To reset factory settings:

1. Go to the **Collector CLI.**
2. In the **Enter option** field, enter **7** (Advanced Options) and press **Enter.**
3. In the **Enter option** field, enter **5** (Factory Reset) and press **Enter.**
4. At the prompt, **Are you sure you want to do a factory reset?** enter **y** and press **Enter.** The appliance is reset to the state it was when it came from the factory and then the appliance reboots. To use the appliance perform the appliance setup process again. For more information, see Setting Up Physical Appliances.
5. Press **Enter.**

Creating Data Collectors

Before You Begin

Before you can create a data collector, you must have already successfully set up a physical appliance or virtual appliance.

For information, see Setting Up Appliances.

ClearPass Device Insight Requirements

This topic lists the ClearPass Device Insight requirement.

Network Requirements for CPDI Collector

The network requirements for CPDI collector include:

- Static IP address
- Outbound Internet Access on TCP port 443
- Optional: Proxy Server

Network Services (Internal or External) from the collector

The network services (internal or external) requirements from the data collector include:

- TCP/UDP 53 (DNS)
- UDP 123 (NTP)

Recommended access to network devices from the collector

The recommended access to network devices from the collector include UDP 161: SNMP (V1 through 3, but 3 is preferred).

Recommended access from the network devices to the collector

The recommended access to network devices from the collector include:

- UDP 67: DHCP for the ip-helpers / DHCP relays
- When used: Netflow or IPFix

Recommended access to endpoints from the collector

The recommended access to endpoints from the collector include:

- TCP, UDP, ICMP - For nmap profiling and WMI profiling
- TCP:22 - For SSH scans
- UDP:161 - for SNMP scans

Creating Data Collectors

To create a data collector:

1. Go to the **Account Home** page.
2. Under **Global Settings**, click **Data Collectors**.
3. If no data collectors have been created, the **Get Started** dialog is displayed. Otherwise, the **Data Collectors** page is displayed.
4. The number of appliances that are available to form new data collectors is displayed in the **Get Started** dialog and in the **Create Collector** card of the **Data Collectors** page.
5. Click **Create Collector** in the **Get Started** dialog or the **Create Collector** card in the **Data Collectors** page. The **Create Collector** dialog is displayed.

The **Create Collector** dialog can also be accessed by clicking the **Create Collector** button within the **Managed Collectors** card - **List** view.

6. In the **Give collector a name** field, enter a name for the data collector.
7. Select the application you want to install on the data collector. Applications include **ClearPass Device Insight**.
8. Click **Next.** All of the appliances that are available to become data collectors are listed in a grid. The appliance **Name,** IP **Address,** and **Model** are displayed.
9. Select the row in the grid for the appliance you want to become the data collector.
10. Click **Create.** The application you previously selected is installed on the appliance and the data collector is created. You can manage this data collector using the **Managed Collectors** card. Plus, the data collector is now available for use by the application that was installed on the data collector. For more information, see About Data Collectors Page.

Viewing Data Collectors

Using the **Data Collectors** page you can view managed data collectors in the **Managed Collectors** card and view the unmanaged data collectors that are connected or not connected in the **Other Collectors** card.

Viewing Managed Data Collectors

To view managed data collectors:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. The **Data Collectors** page opens, displaying all of the managed data collectors in the **Managed Collectors** card by status by default.
3. (Optional) Click the down arrow in the **Managed Collectors** card heading and select **By Apps,** to view the data collectors by applications.
4. (Optional) Click the down arrow in the **Managed Collectors** card heading and select **By Update,** to view the data collectors by update status.
5. Click the **View Grid** icon to view more details for the data collectors. The **Managed Collectors - List** view opens, displaying all of the data collectors in a grid format.
6. Expand a row in the grid to view additional details for a specific data collector. The row is expanded displaying an **Overview** tab and a **Performance** tab. View the data collector overview information in the **Overview** tab. View the data collector performance information in the **Performance** tab. For more information, see About Data Collectors Page.

Viewing Unmanaged Data Collectors

To view unmanaged data collectors:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. The **Data Collectors** page is displayed.
3. Click the **Connected** number in the **Others** card to view the connected unmanaged data collectors. The **Other Collectors** dialog opens, displaying the connected data collectors in a grid format. The following table describes the information that is displayed in the grid:

Table 55: *Other Collectors Dialog*

Field	Description
Name	Data collector name.
Status	Status of the data collector. **Connected** is displayed for data collectors that are connected.
Address	IP address for the data collector.

4. Click the **Not Connected** number in **Others** card to view the unmanaged data collectors that are not connected. The **Other Collectors** dialog opens, displaying the data collectors that are not connected in a grid format. The following table describes the information that is displayed in the grid:

Table 56: *Other Collectors Dialog*

Field	Description
Name	Data collector name.

Table 56: *Other Collectors Dialog*

Field	Description
Status	Status of the data collector. **Not Connected** is displayed for data collectors that are not connected.
Address	IP address for the data collector.

For more information, see About Data Collectors Page.

Updating Data Collectors

Setting the Data Collectors Global Auto-Update Preference

To set the data collectors global auto-update preference:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. The **Data Collectors** page opens, displaying all of the managed data collectors in the **Managed Collectors** card by status by default.
3. Click the down arrow in the **Managed Collectors** card heading and select **By Update.** The **Managed Collectors** card displays the data collectors by update status. In lower right hand corner of the card is displayed an **Auto-Update** field that displays the current global setting for the data collector auto-update preference. **As soon as available** is displayed by default in this field.
4. Click the **Auto-Update** field. The **Collector Update** dialog opens displaying the data collector update options.
5. Select when you want to install the updates for all data collectors. Options are:
   - **Apply Instantly:** All data collectors will be updated as soon as a new version is available.
   - **Apply on specific time:** All data collectors will be updated at the day and time that you set when a new version is available. When you select this option, a **Day** field and **Time** field are displayed. Click the down arrow next to the **Day** field and select the day. Day options are: **Monday** through **Sunday.** Click the up and down arrows in the **Time** field and select the time. You can also update one or more data collectors earlier than what you have specified with the auto-update option, by clicking the **Update All** button or **Update Now** button on the **Managed Collectors card - List** view. For more information, see Manually Updating All Data Collectors and Manually Updating a Specific Data Collector.
6. Click **Save.**

Manually Updating All Data Collectors

To manually update all data collectors:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. The **Data Collectors** page opens displaying all of the managed data collectors in the **Managed Collectors** card by status by default.
3. Click the down arrow in the **Managed Collectors** card heading and select **By Update.** The **Managed Collectors** card displays the data collectors by update status. In lower right hand corner of the card is displayed an **Auto-Update** field that displays the current setting for the data collector global auto-update preference.

4. Click the **Grid View** icon in the upper right corner of the **Managed Collectors** card. The **Managed Collectors card - List** view opens displaying all of the data collectors in a grid format. The **List** view lists the data collectors that are currently represented in the **Dashboard** view. If an update is available for one or more data collectors, the **Update All** button is available at the top of the **List** view.
5. Click **Update All.** All of the data collectors are updated.

Manually Updating a Specific Data Collector

To update a specific data collector:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. The **Data Collectors** page opens displaying all of the managed data collectors in the **Managed Collectors** card by status by default.
3. Click the down arrow in the **Managed Collectors** card heading and select **By Update.** The **Managed Collectors** card displays the data collectors by update status. In lower right hand corner of the card is displayed an **Auto-Update** field that displays the current setting for the data collector global auto-update preference.
4. Click the **Grid View** icon in the upper right corner of the **Managed Collectors** card. The **Managed Collectors card - List** view opens displaying all of the data collectors in a grid format. The **List** view lists the data collectors that are currently represented in the **Dashboard** view. If an update is available for one or more data collectors, **Update available** is displayed in the **Update Status** for those data collectors in the grid.
5. Expand the row in the grid for the individual data collector that you want to update. The row expands displaying the additional overview details for that specific data collector. In the lower portion of the expanded row, the update version is displayed in the **Version** field and the **Update Now** button is available.
6. Click **Update Now.** The data collector is updated.

Deleting Data Collectors

To delete a data collector:

1. Go to **Account Home.**
2. Under **Global Settings**, click **Data Collectors**. The **Data Collectors** page opens, displaying all of the managed data collectors in the **Managed Collectors** card by status by default.
3. Click the **Grid View** icon in the upper right corner of the **Managed Collectors** card. The **Managed Collectors card - List** view opens, displaying all of the data collectors in a grid format. The **List** view lists the data collectors that are currently represented in the **Dashboard** view.
4. Hover over a data collector row in the grid that you want to delete. The **Delete** icon is displayed to the right of **Applications.**
5. Click the **Delete** icon. The **Delete Collector** dialog opens asking if you are sure you want to delete the data collector.
6. Click **Delete.** The Aruba application running on the collector is uninstalled from the collector. The appliance is freed up and can be used for creating another data collector in the future. For more information about creating a data collector, see Creating Data Collectors.

Webhooks

Webhooks allow you to implement event reactions by providing real-time information or notifications to other applications. Aruba Central allows you to create Webhooks and select Webhooks as the notification delivery option for all alerts.

Using Aruba Central, you can integrate Webhooks with other third-party applications such as ServiceNow, Zapier, IFTTT, and so on.

You can access the Webhooks service either through the Aruba Central UI or API Gateway. Aruba Central supports creating up to 10 Webhooks. To enable redundancy, Aruba Central allows you to add up to three URLs per Webhook.

From Aruba Central, you can add, list, or delete Webhooks; get or refresh Webhooks token; get or update Webhooks settings for a specific item; and test Webhooks notification.

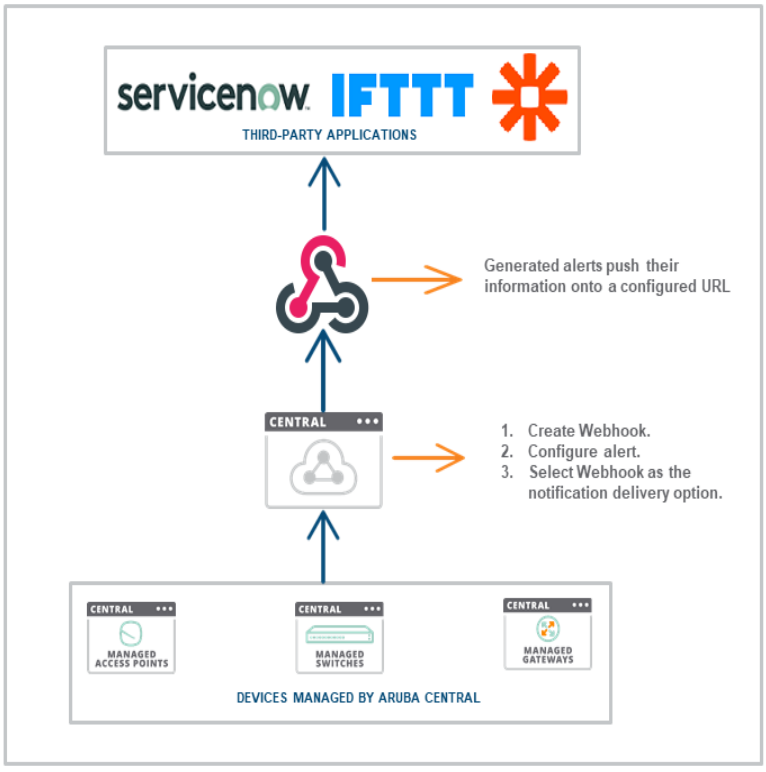
This section includes the following topics:

- Creating and Updating Webhooks Through the UI
- Refreshing Webhooks Token Through the UI
- Creating and Updating Webhooks Through the API Gateway
- List of Webhooks APIs
- Sample Webhooks Payload Format for Alerts

In the **Alerts & Events** page, click the **Configuration** icon to configure and enable an alert. In the **Notification Options**, select **Webhooks** as the notification delivery option.

The following figure illustrates how Aruba Central integrates with third-party applications using Webhooks.

Figure 93 *Webhooks Integration*



Creating and Updating Webhooks Through the UI

To access the Webhooks service from the UI:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.The **Webhooks** page is displayed.
2. In the **Webhook** tab, click **+** sign. The **Add Webhook** pop-up window is displayed.

Figure 94 *Webhooks Page*

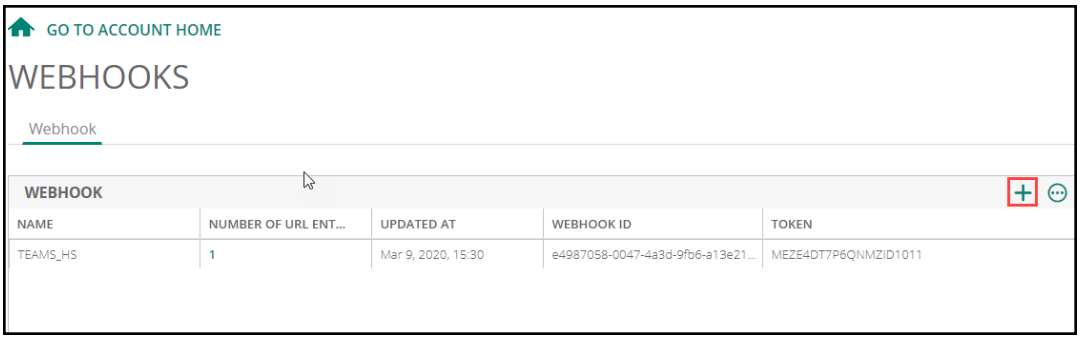
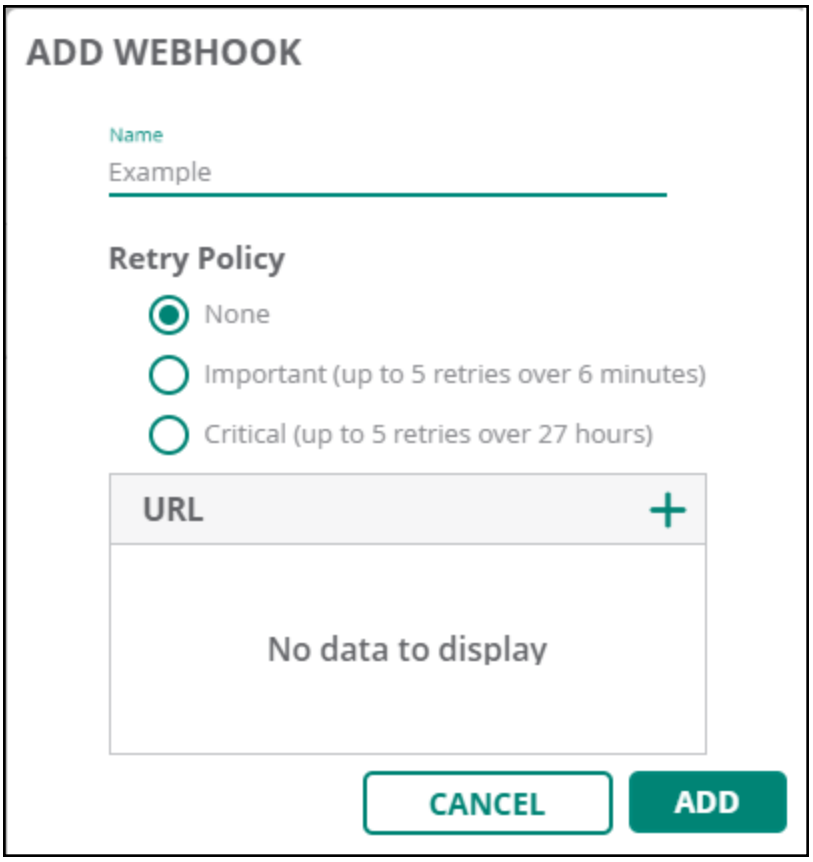


Figure 95 *Add Webhooks Page*



3. To create webhooks, enter the following details:
   a. **Name**—Enter a name for the Webhook.
   b. **Retry Policy**—Select one of the following options:

- **None**—No retries.
- **Important**—Up to 5 retries over 6 minutes.
- **Critical**—Up to 5 retries over 27 hours.

c. **URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.

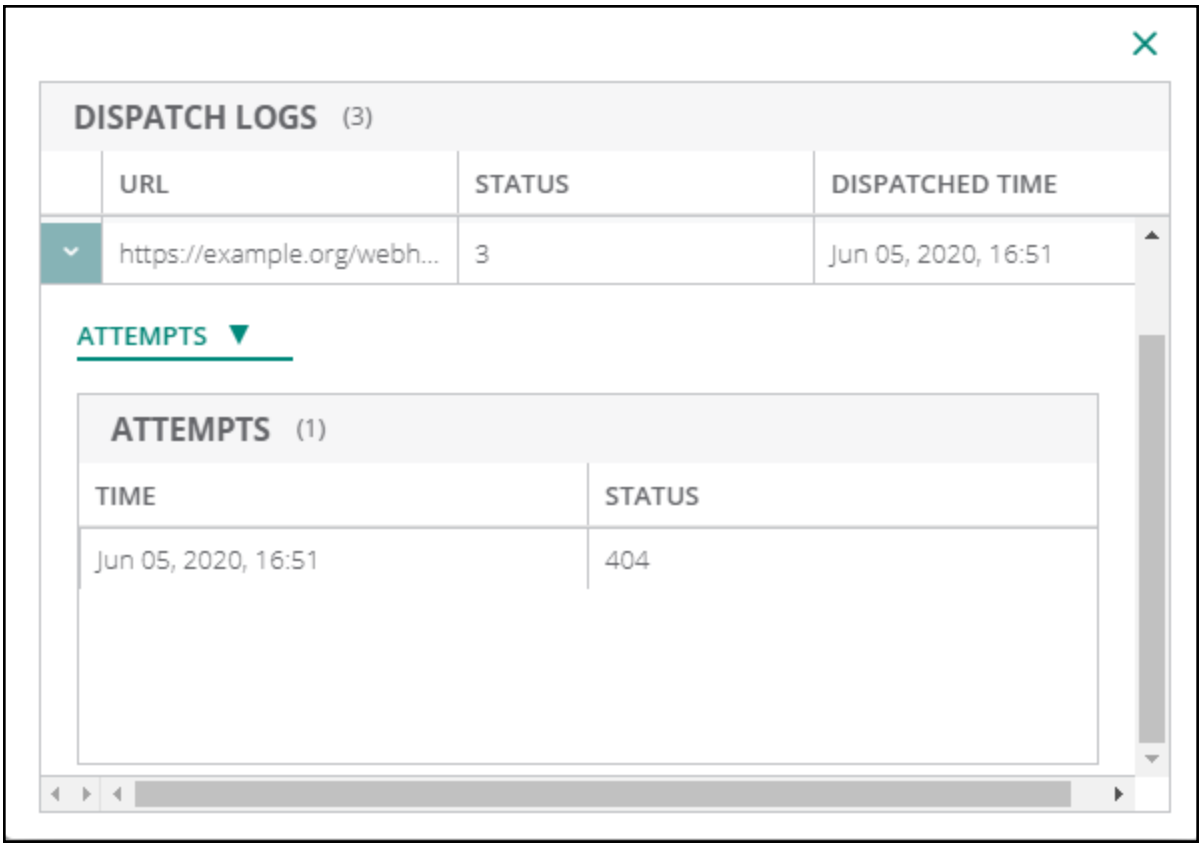
4. Click **Save**. The Webhooks is created and listed in the **Webhook** table.

Viewing Webhooks

To view the Webhooks, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.
2. The **Webhooks** page with Webhook table is displayed.
   The **Webhook** table allows you to edit or delete Webhooks and also displays the following information:
   - **Name**—Name of the Webhooks.
   - **Number of URL Entries**—Number of URLs in Webhooks. Click the number to view the list of URLs.
   - **Updated At**—Date and time at which Webhooks was updated.
   - **Webhook ID**—Webhooks ID.
   - **Token**—Webhooks token. Webhooks token enables header authentication and the third-party receiving service must validate the token to ensure authenticity.
   - **Edit**—Select the Webhook from the list and click the **Edit** icon to edit the Webhook. You can refresh the token and add URLs. Click **Save** to save the changes.
   - **Delete**—Select the Webhook from the list and click the **Delete** icon and click **Yes** to delete the Webhook.
   - **Test Webhooks**—Select the Webhook from the list and click the **Test Webhooks** icon to test the Webhook by posting sample webhook payload to the configured URL. The **Test Webhooks** table provides the **URL** and **Status** of the selected Webhook.
   - **View Dispatch Logs**—Select the Webhook from the list and click the **View Dispatch Log** icon to view the **Dispatch Logs** for the selected Webhook. The **Dispatch Logs** table provides the **URL**, **Status,** and **Dispatched Time**. Click the arrow against each row to view the **Log Details** and **Attempts** in the drop-down for the respective URL.

Figure 96 *Dispatch Logs Details Page*



Refreshing Webhooks Token Through the UI

To refresh Webhooks token through the UI:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.
   The **Webhooks** page is displayed.
2. In the **Webhook** table, select the Webhook from the list and click **Edit** icon to edit.
3. In the pop-up window, click the **Refresh** icon next to the token. The token is refreshed.

Creating and Updating Webhooks Through the API Gateway

The following HTTP methods are defined for Aruba Central API Webhooks resource:

- **GET**
- **POST**
- **PUT**
- **DELETE**

You can perform CRUD operation on the Webhooks URL configuration. The key configuration elements that are required to use API Webhooks service are Webhooks URL and a shared secret.

A shared secret token is generated for the Webhooks URL when you register for Webhooks. A hash key is generated using SHA256 algorithm by using the payload and the shared secret token. The API required to refresh the shared secret token is provided for a specific Webhooks configuration. You can choose the frequency at which you want to refresh the secret token.

To access and use the API Webhooks service:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.The **API Gateway** page is displayed.
2. In the **APIs** tab, click the **Swagger** link under the **Documentation** header. The Swagger website opens.
3. In the Swagger website, from the **URL** drop-down list, select **Webhook**. All available Webhooks APIs are listed under **API Reference**.

For more information on Webhooks APIs, see:
https://app1-apigw.central.arubanetworks.com/swagger/central.

List of Webhooks APIs

Aruba Central supports the following Webhooks APIs:

- **GET /central/v1/webhooks**—Gets a list of Webhooks.

  The following is a sample response:

```
{
  "count": 1,
  "settings": [
    {
      "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
      "name": "AAA",
      "updated_ts": 1523956927,
      "urls": [
        "https://example.org/webhook1",
        "https://example.org/webhook1"
      ],
      "secure_token": "KEu5ZPTi44UO4MnMiOqz"
    }
  ]
}
```

- **POST /central/v1/webhooks**—Creates Webhooks.

  The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **DELETE /central/v1/webhooks/{wid}**—Deletes Webhooks.

  The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8"
}
```

- **GET /central/v1/webhooks/{wid}**—Gets Webhooks settings for a specific item.

The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
  "name": "AAA",
  "updated_ts": 1523956927,
  "urls": [
    "https://example.org/webhook1",
    "https://example.org/webhook1"
  ],
  "secure_token": "KEu5ZPTi44UO4MnMiOqz"
}
```

- **PUT /central/v1/webhooks/{wid}**—Updates Webhooks settings for a specific item.

  The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **GET /central/v1/webhooks/{wid}/token**—Gets the Webhooks token for the Webhooks ID.

  The following is a sample response:

```
{
  "name": "AAA",
  "secure_token": "[{\"token\": \"zSMrzuYrblgBfByy2JrM\", \"ts\": 1523957233}]"
}
```

- **PUT /central/v1/webhooks/{wid}/token**—Refreshes the Webhooks token for the Webhooks ID.

  The following is a sample response:

```
{
  "name": "AAA",
  "secure_token": "[{\"token\": \"zSMrzuYrblgBfByy2JrM\", \"ts\": 1523957233}]"
}
```

- **GET /central/v1/webhooks/{wid}/ping**—Tests the Webhooks notification and returns whether success or failure.

  The following is a sample response:

```
"Ping Response [{'url': 'https://example.org', 'status': 404}]"
```

Sample Webhooks Payload Format for Alerts

```
URL POST <webhook-url>
```

Custom Headers

```
Content-Type: application/json
X-Central-Service: Alerts
X-Central-Event: Radio-Channel-Utilization
```

```
X-Central-Delivery-ID: 72d3162e-cc78-11e3-81ab-4c9367dc0958
X-Central-Delivery-Timestamp: 2016-07-12T13:14:19-07:00
X-Central-Customer-ID: <########>
```

Refer to the following topics to view sample JSON content:

- Access Point Alerts—Sample JSON
- Switch Alerts—Sample JSON
- Gateway Alerts—Sample JSON
- Miscellaneous Alerts—Sample JSON

Access Point Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

AP Disconnected


```
{
  "alert_type": "AP disconnected",
  "description": "AP with Name 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8c
disconnected, Group:unprovisioned",
  "timestamp": 1564326129,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-4",
  "state": "Open",
  "nid": 4,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "conn_status": "disconnected",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:09 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm2zVQO1ZtiGF20e",
  "severity": "Critical"
}
```


AP Connected Clients


```
{
  "alert_type": "AP_CONNECTED_CLIENTS",
  "description": "Number of Clients connected to AP with name 84:d4:7e:c5:c8:8c has been
above 1 for about 5 minutes
     since 2019-07-29 12:26:00 UTC.",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1255",
  "state": "Open",
  "nid": 1255,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "name": "84:d4:7e:c5:c8:8c",
    "duration": "5",
    "threshold": "1",
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
```

```
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVGH9ZtiGF20d",
  "severity": "Major"
}
```


AP CPU Over Utilization


```
{
  "alert_type": "AP_CPU_OVER_UTILIZATION",
  "description": "CPU utilization for AP 84:d4:7e:c5:c8:8c with serial CT0779239 has been
above 10% for about 5 minutes
     since 2019-07-28 14:21:00 UTC.",
  "timestamp": 1564323960,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1250",
  "state": "Open",
  "nid": 1250,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "84:d4:7e:c5:c8:8c",
    "duration": "5",
    "time": "2019-07-28 14:21:00 UTC",
    "threshold": "10",
    "ds_key": "201804170291.CT0779239.cpu_utilization.5m",
    "serial": "CT0779239",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw4-VVrVQO1ZtiGFkZ3",
  "severity": "Critical"
}
```


AP Memory Over Utilization


```
{
  "alert_type": "AP_MEMORY_OVER_UTILIZATION",
  "description": "Memory utilization for AP iap-303-iphone456-offline with serial
CNGHKGX004 has been above 40% for about 5 minutes
     since 2019-07-24 07:11:00 UTC.",
  "timestamp": 1563952560,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1251",
  "state": "Open",
  "nid": 1251,
  "details": {
    "_rule_number": "1",
    "group": "3",
    "name": "iap-303-iphone456-offline",
    "labels": "3,118",
    "duration": "5",
    "time": "2019-07-24 07:11:00 UTC",
    "threshold": "40",
    "ds_key": "201804170291.CNGHKGX004.memory_utilization.5m",
    "serial": "CNGHKGX004",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWwi1jihVQO1ZtiGThDA",
  "severity": "Major"
}
```


AP Radio Noise Floor

```
{
  "alert_type": "AP_RADIO_NOISE_FLOOR",
  "description": "Noise floor on AP iap-303-iphone456-offline operating on Channel 10 and
serving 0 clients has been above -110 dBm
     for about 10 minutes since 2019-07-24 07:06:00 UTC.",
  "timestamp": 1563952560,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1253",
  "state": "Open",
  "nid": 1253,
  "details": {
    "_rule_number": "0",
    "group": "3",
    "name": "iap-303-iphone456-offline",
    "_radio_num": "1",
    "client_count": "0",
    "labels": "3,118",
    "_band": "0",
    "duration": "10",
    "time": "2019-07-24 07:06:00 UTC",
    "threshold": "110",
    "ds_key": "201804170291.CNGHKGX004.radio.noisefloor",
    "serial": "CNGHKGX004",
    "channel": "10"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWwi1jjgVQO1ZtiGThDB",
  "severity": "Critical"
}
```


AP Radio Over Utilization


```
{
  "alert_type": "AP_RADIO_OVER_UTILIZATION",
  "description": "Radio utilization on AP 84:d4:7e:c5:c8:8c operating on Channel 36E and
serving 0 clients has been above 1%
     for about 5 minutes since 2019-07-28 14:31:00 UTC.",
  "timestamp": 1564324560,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1252",
  "state": "Open",
  "nid": 1252,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "84:d4:7e:c5:c8:8c",
    "_radio_num": "0",
    "client_count": "0",
    "_band": "1",
    "duration": "5",
    "unit": "%",
    "time": "2019-07-28 14:31:00 UTC",
    "threshold": "1",
    "ds_key": "201804170291.CT0779239.radio.busy64",
    "serial": "CT0779239",
    "channel": "36E"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5An08VQO1ZtiGFpgm",
  "severity": "Critical"
}
```


Client Attack detected

```
{
  "alert_type": "Client attack detected",
  "description": "An AP (NAME iap-303-iphone456-o and MAC 90:4c:81:cf:27:74 on RADIO 1)
detected an unencrypted frame
     between a valid client (88:63:df:bb:2a:9d) and access point (BSSID 90:4c:81:72:77:55)
with source 88:63:df:bb:2a:9d
     and receiver ff:ff:ff:ff:ff:ff SNR value is 55",
  "timestamp": 1564392710,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-13",
  "state": "Open",
  "nid": 13,
  "details": {
    "group": "3",
    "labels": "3,142,141",
    "params": "None",
    "_rule_number": "0",
    "time": "2019-07-29 09:31:50 UTC"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWw9EmBxVQO1ZtiGO1Q8",
  "severity": "Critical"
}
```


Connected Clients


```
{
  "alert_type": "CONNECTED_CLIENTS",
  "description": "Number of Clients connected to swarm with name SetMeUp-CA:35:56 has been
above 1 for about 5 minutes
     since 2019-07-29 12:26:00 UTC.",
  "timestamp": 1564403460,
  "webhook": "68612ee3-3ee9-4da4-b07b-13977a350344",
  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-1254",
  "state": "Open",
  "nid": 1254,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "SetMeUp-CA:35:56",
    "duration": "5",
    "aggr_context": "swarm",
    "time": "2019-07-29 12:26:00 UTC",
    "threshold": "1",
    "ds_key": "b8be21720dc04a8e9f0028374b6a9bbd.cluster.156.device.clients.5m",
    "serial": "156"
  },
  "operation": "create",
  "device_id": "156",
  "id": "AWw9tmhNVQO1ZtiGQR5U",
  "severity": "Critical"
}
```


Infrastructure Attack Detected


```
{
  "alert_type": "Infrastructure attack detected",
  "description": "An AP (NAME iap-303-iphone456-o and MAC 90:4c:81:cf:27:74 on RADIO 1)
detected that the Access Point with
     MAC f0:5c:19:23:56:10 and BSSID f0:5c:19:23:56:10 has sent a beacon for SSID tan This
beacon advertizes channel 149
     but was received on channel 161 with SNR 50 ",
  "timestamp": 1564400165,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-12",
```

```
  "state": "Open",
  "nid": 12,
  "details": {
    "group": "3",
    "labels": "3,142,141",
    "params": "None",
    "_rule_number": "0",
    "time": "2019-07-29 11:36:05 UTC"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWw9hCLAVQO1ZtiGP1ig",
  "severity": "Critical"
}
```


Insufficient Power Alert


```
{
  "alert_type": "INSUFFICIENT_POWER_ALERT",
  "description": "Insufficient inline power supplied to AP-205 with name
04:bd:88:c3:b6:f0",
  "timestamp": 1564403450,
  "webhook": "68612ee3-3ee9-4da4-b07b-13977a350344",
  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-21",
  "state": "Open",
  "nid": 21,
  "details": {
    "group": "0",
    "name": "04:bd:88:c3:b6:f0",
    "labels": [],
    "label_site_desc": "",
    "time": "2019-07-29 12:30:50 UTC",
    "serial": "CM0381143",
    "group_name": "default",
    "ap_model": "AP-205"
  },
  "operation": "create",
  "device_id": "CM0381143",
  "id": "AWw9tkNGVQO1ZtiGQRz-",
  "severity": "Major"
}
```


Modem Plugged


```
{
  "alert_type": "Modem Plugged",
  "description": "Modem plugged to ap with name 84:d4:7e:c5:c8:8c'and MAC address
84:d4:7e:c5:c8:8c",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-18",
  "state": "Open",
  "nid": 18,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zJKL90tiGF20d",
  "severity": "Critical"
```

```
}
```


Modem Unplugged


```
{
  "alert_type": "Modem Unplugged",
  "description": "Modem unplugged from ap with name 84:d4:7e:c5:c8:8c'and MAC address
84:d4:7e:c5:c8:8c",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-19",
  "state": "Open",
  "nid": 19,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVQO1ZtiGF20d",
  "severity": "Critical"
}
```


New AP Detected


```
{
  "alert_type": "New AP detected",
  "description": "New AP with Name 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8c
detected, Group:unprovisioned",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-3",
  "state": "Open",
  "nid": 3,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVQO1ZtiJH56e",
  "severity": "Major"
}
```


New Virtual Controller Detected


```
{
  "alert_type": "New Virtual Controller detected",
  "description": "New Virtual Controller with Name SetMeUp-CA:51:D6, Version 8.4.0.0_69847
and IP address 10.29.43.70
     detected, Group:unprovisioned",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1",
  "state": "Open",
```

```
  "nid": 1,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "SetMeUp-CA:51:D6",
      "8.4.0.0_69847",
      "10.29.43.70"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVQO1ZtiJH56j",
  "severity": "Critical"
}
```


Rogue AP Detected


```
{
  "alert_type": "Rogue AP detected",
  "description": "An AP (NAME 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8con RADIO
1) detected an access point
     (BSSID  0c:00:01:34:69:62 and SSID ssid1 on CHANNEL 52) as rogue",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-10",
  "state": "Open",
  "nid": 10,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c",
      "1",
      "0c:00:01:34:69:62",
      "ssid1",
      "52"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVQO1ZtiJK89l",
  "severity": "Critical"
}
```


Uplink Changed


```
{
  "alert_type": "Uplink Changed",
  "description": "Uplink changed from 0 to 1 for ap'with name {params[2]} and MAC address
{params[3]}",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-17",
  "state": "Open",
  "nid": 17,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
```

```
      "0",
      "1",
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVQO1ZtiGF20d",
  "severity": "Critical"
}
```


Virtual Controller Disconnected


```
{
  "alert_type": "Virtual controller disconnected",
  "description": "Virtual Controller with Name SetMeUp-CA:51:D6, Version 8.4.0.0_69847 and
IP address 10.29.43.70
     disconnected, Group:unprovisioned",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-2",
  "state": "Open",
  "nid": 2,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "conn_status": "disconnected",
    "params": [
      "SetMeUp-CA:51:D6",
      "8.4.0.0_69847",
      "10.29.43.70"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVQO1ZtiGF20d",
  "severity": "Critical"
}
```


Switch Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

Switch Disconnected


```
{
  "alert_type": "Switch Disconnected",
  "description": "Switch with serial CN8AHKW095, MAC address 54:80:28:b8:f6:20 IP address
10.22.41.3 and
     Hostname Aruba-2930F-24G-PoEP-4SFPP disconnected, Group:unprovisioned",
  "timestamp": 1569475139,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-203",
  "state": "Open",
  "nid": 203,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "conn_status": "disconnected",
    "params": [
```

```
      "CN8AHKW095",
      "54:80:28:b8:f6:20",
      "10.22.41.3",
      "Aruba-2930F-24G-PoEP-4SFPP"
    ],
    "time": "2019-09-26 05:18:59 UTC"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1sAhfAYu0OgJ2anzUD",
  "severity": "Major"
}
```

New Switch Connected

```
{
  "alert_type": "New Switch Connected",
  "description": "New Switch with serial CN8AHKW095, MAC address 54:80:28:b8:f6:20 IP
address 10.22.41.3 and
     Hostname Aruba-2930F-24G-PoEP-4SFPP connected, Group:unprovisioned",
  "timestamp": 1569476559,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-201",
  "state": "Open",
  "nid": 201,
  "details": {
    "group": "1",
    "labels": "",
    "params": [
      "CN8AHKW095",
      "54:80:28:b8:f6:20",
      "10.22.41.3",
      "Aruba-2930F-24G-PoEP-4SFPP"
    ],
    "_rule_number": "0",
    "time": "2019-09-26 05:42:39 UTC"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1sF8IGYu0OgJ2an0Aq",
  "severity": "Major"
}
```

Switch Memory Over Utilization

```
{
  "alert_type": "SWITCH_MEMORY_OVER_UTILIZATION",
  "description": "Memory utilization for Switch Aruba-2930F-24G-PoEP-4SFPP with serial
CN8AHKW095 has been above 10% for about 5 minutes
     since 2019-09-26 05:48:00 UTC",
  "timestamp": 1569477180,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1301",
  "state": "Open",
  "nid": 1301,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "duration": "5",
    "time": "2019-09-26 05:48:00 UTC",
    "threshold": "10",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.memory_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
```

```
  "device_id": "CN8AHKW095",
  "id": "AW1sITrfYu0OgJ2an0UP",
  "severity": "Critical"
}
```


Switch CPU Over Utilization


```
{
  "alert_type": "SWITCH_CPU_OVER_UTILIZATION",
  "description": "CPU utilization for Switch Aruba-2930F-48G-PoEP-4SFPP with serial
CN88HKX1CR has been above 5% for about 5 minutes
     since 2019-09-26 06:07:00 UTC.",
  "timestamp": 1569478320,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1300",
  "state": "Open",
  "nid": 1300,
  "details": {
    "_rule_number": "0",
    "group": "41",
    "name": "Aruba-2930F-48G-PoEP-4SFPP",
    "duration": "5",
    "time": "2019-09-26 06:07:00 UTC",
    "threshold": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN88HKX1CR.cpu_utilization.5m",
    "serial": "CN88HKX1CR",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN88HKX1CR",
  "id": "AW1sMqB4Yu0OgJ2an055",
  "severity": "Critical"
}
```


Switch Interface Rx Rate


```
{
  "alert_type": "SWITCH_INTERFACE_RX_RATE",
  "description": "Receive rate for Interface 15 on Switch Aruba-2930F-24G-PoEP-4SFPP has
been above 1 % for about 5 minutes
     since 2019-09-26 13:18:00 UTC.",
  "timestamp": 1569504180,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1303",
  "state": "Open",
  "nid": 1303,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "max_value_for_percentage": "1000.0",
    "threshold": "1",
    "intf_name": "15",
    "time": "2019-09-26 13:18:00 UTC",
    "duration": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.rx_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1tvTgBYu0OgJ2 aoCgl",
  "severity": "Critical"
}
```


Switch Interface Tx Rate

```
{
  "alert_type": "SWITCH_INTERFACE_TX_RATE",
  "description": "Transfer rate for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP has
been above 1 % for about 5 minutes
     since 2019-09-26 13:18:00 UTC.",
  "timestamp": 1569504180,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1302",
  "state": "Open",
  "nid": 1302,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "max_value_for_percentage": "1000.0",
    "threshold": "1",
    "intf_name": "19",
    "time": "2019-09-26 13:18:00 UTC",
    "duration": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.tx_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1tvTgBYu0OgJ2aoCgk",
  "severity": "Critical"
}
```


Switch POE Utilization


```
{
  "alert_type": "SWITCH_POE_UTILIZATION",
  "description": "PoE utilization for Switch Aruba-2930F-24G-PoEP-4SFPP with serial
CN69HKW05T MAC address e0:07:1b:c4:8d:80
     and IP address 10.22.182.78 has been above 1%",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```


Switch Interface Input Errors


```
{
  "alert_type": "SWITCH_INTERFACE_INPUT_ERRORS",
  "description": "Input errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP has
been above 90% for about
     30 minutes since 2019-09-26 06:07:00 UTC .",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
```

```
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```


Switch Interface Output Errors


```
{
  "alert_type": "SWITCH_INTERFACE_OUTPUT_ERRORS",
  "description": "Output errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP has
been above 90% for about
     30 minutes since 2019-09-26 06:07:00 UTC.",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```


Switch Mismatch Config


```
{
  "alert_type": "Switch Mismatch Config",
  "description": "Config mismatch occurred in switch with serial CN69HKW05T MAC address
e0:07:1b:c4:8d:80 and
     IP address 10.22.182.78 and Hostname Aruba-2930F-48G-PoEP-4SFPP ",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
```

```
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```


Switch Hardward Failure


```
{
  "alert_type": "SWITCH_HARDWARE_FAILURE",
  "description": "Switch with serial CN8AHKW095 : Fan 1 failed ",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```


Switch Interface Duplex Mode


```
{
  "alert_type": "SWITCH_INTERFACE_DUPLEX_MODE",
  "description": "Interface 19 on switch Aruba-2930F-24G-PoEP-4SFPP with serial CN8AHKW095
is operating at Half-Duplex mode",
  "timestamp": 1569901561,
  "webhook": "c71404f4-00c1-4241-8bf4-c8d3f981caa2",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1306",
  "state": "Open",
  "nid": 1306,
  "details": {
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "labels": "",
    "mode": "Half",
    "intf_name": "19",
    "time": "2019-10-01 03:46:01 UTC",
    "serial": "CN8AHKW095"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW2FbMiOYu0OgJ2asaWh",
  "severity": "Critical"
}
```


Gateway Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

WAN Uplink Flap

```
{
  "alert_type": "WAN_UPLINK_FLAP",
  "description": "Uplink link1_inet link status flapped 1% on device with CNHHKLB031 for
about 15 minutes
     since 2019-07-25 12:36:00 UTC.",
  "timestamp": 1564059060,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1600",
  "state": "Open",
  "nid": 1600,
  "details": {
    "status": "DOWN",
    "_rule_number": "0",
    "group": "77",
    "labels": "8,661",
    "current_status": "UP",
    "duration": "15",
    "intf_name": "link1_inet",
    "time": "2019-07-25 12:36:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.uplink.flap.5m",
    "serial": "CNHHKLB031",
    "uplink_tag": "link1_inet",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpL0fvVQO1ZtiGh-2_",
  "severity": "Critical"
}
```


WAN Tunnel Flap


```
{
  "alert_type": "WAN_TUNNEL_FLAP",
  "description": "Tunnel data-vpnc-00:1a:1e:03:83:30-link1_inet status flapped 1%
    on device CNHHKLB031 for about 15 minutes since 2019-07-25 12:26:00 UTC.",
  "timestamp": 1564058460,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1601",
  "state": "Open",
  "nid": 1601,
  "details": {
    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
    "_rule_number": "0",
    "group": "77",
    "dst_ip": "172.168.101.9",
    "labels": "8,661",
    "src_ip": "192.168.51.254",
    "duration": "15",
    "time": "2019-07-25 12:26:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.uplink.tunnel.flap.5m",
    "serial": "CNHHKLB031",
    "uplink_tag": "link1_inet",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpJiAiVQO1ZtiGh5tw",
  "severity": "Critical"
}
```


WAN Auto Negotiation Flap

```
{
  "alert_type": "WAN_AUTO_NEGOTIATION_FLAP",
  "description": "Uplink GE0/0/1 speed flapped 1% on device CNHHKLB031 for about
     15 minutes since 2019-07-25 12:32:00 UTC.",
  "timestamp": 1564058820,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1602",
  "state": "Open",
  "nid": 1602,
  "details": {
    "new_speed": "Auto",
    "group": "77",
    "labels": "8,661",
    "duration": "15",
    "_rule_number": "0",
    "intf_name": "GE0/0/1",
    "time": "2019-07-25 12:32:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.uplink.speed.flap.5m",
    "serial": "CNHHKLB031",
    "speed": "1000",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpK55sVQO1ZtiGh8zr",
  "severity": "Minor"
}
```


WAN IPsec SA Establishment Failed


```
{
  "alert_type": "WAN_IPSEC_SA_ESTABILSHMENT_FAILED",
  "description": "IPSec Tunnel Establishment from 192.168.51.254 to 172.168.101.9 failed
     on device CNHHKLB031 at 2019-07-25 12:49:56 UTC",
  "timestamp": 1564058996,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1550",
  "state": "Open",
  "nid": 1550,
  "details": {
    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "src_ip": "192.168.51.254",
    "link_tag": "link1_inet",
    "time": "2019-07-25 12:49:56 UTC",
    "dst_ip": "172.168.101.9",
    "serial": "CNHHKLB031"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpLlB0VQO1ZtiGh-WS",
  "severity": "Minor"
}
```


WAN IPsec SA Down


```
{
  "alert_type": "WAN_IPSEC_SA_DOWN",
  "description": "IPSec tunnel from 192.168.52.254 to 172.168.101.9 is DOWN on device
```

```
CNHHKLB031.
     Reason: Administrator cleared IPSEC SA at 2019-07-25 12:40:22 UTC",
  "timestamp": 1564058422,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1551",
  "state": "Open",
  "nid": 1551,
  "details": {
    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link2_mpls",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "src_ip": "192.168.52.254",
    "reason": "Administrator cleared IPSEC SA",
    "time": "2019-07-25 12:40:22 UTC",
    "dst_ip": "172.168.101.9",
    "serial": "CNHHKLB031",
    "uplink_tag": "link2_mpls"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpJY4aVQO1ZtiGh5c-",
  "severity": "Minor"
}
```


WAN IPsec SA All Down


```
{
  "alert_type": "WAN_IPSEC_SA_ALL_DOWN",
  "description": "All IPSec SAs down for device CNHHKLB031 at 2019-07-25 12:40:22 UTC",
  "timestamp": 1564058446,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1552",
  "state": "Close",
  "nid": 1552,
  "details": {
    "serial": "CNHHKLB031",
    "labels": [
      "8",
      "661"
    ],
    "group": "77",
    "name": "None",
    "time": "2019-07-25 12:40:22 UTC"
  },
  "operation": "update",
  "device_id": "CNHHKLB031",
  "id": "AWwpJY3NVQO1ZtiGh5c9",
  "severity": "Critical"
}
```


CFG Set Advertisement Failure


```
{
  "alert_type": "CFG_SET_ADVERTISEMENT_FAILURE",
  "description": "CFG-Set advertisement failure for Gateway with CNHHKLB031 on tunnel data-
vpnc-00:1a:1e:03:83:30-link1_inet
     from 192.168.51.254 to 172.168.101.9",
  "timestamp": 1564059635,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1554",
  "state": "Open",
  "nid": 1554,
```

```
  "details": {
    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "src_ip": "192.168.51.254",
    "time": "2019-07-25 13:00:35 UTC",
    "map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
    "dst_ip": "172.168.101.9",
    "serial": "CNHHKLB031"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpOBCVVQO1ZtiGiD0f",
  "severity": "Major"
}
```


Controller CPU Over Utilization


```
{
  "alert_type": "CONTROLLER_CPU_OVER_UTILIZATION",
  "description": "CPU utilization for Gateway Aruba9004_40_0C_28 with serial CNHHKLB031 has
been above 1% for about 15 minutes
     since 2019-07-25 09:30:00 UTC.",
  "timestamp": 1564047900,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1351",
  "state": "Open",
  "nid": 1351,
  "details": {
    "_rule_number": "0",
    "group": "77",
    "name": "Aruba9004_40_0C_28",
    "labels": "8,661",
    "duration": "15",
    "time": "2019-07-25 09:30:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.cpu_utilization.5m",
    "serial": "CNHHKLB031",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwohP4LVQO1ZtiGgfbQ",
  "severity": "Critical"
}
```


Controller Memory Over Utilization


```
{
  "alert_type": "CONTROLLER_MEMORY_OVER_UTILIZATION",
  "description": "Memory utilization for Gateway Aruba9004_40_0C_28 with serial CNHHKLB031
has been above 1% for about 10 minutes
     since 2019-07-25 09:30:00 UTC.",
  "timestamp": 1564047600,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1352",
  "state": "Open",
  "nid": 1352,
  "details": {
    "_rule_number": "0",
    "group": "77",
    "name": "Aruba9004_40_0C_28",
```

```
    "labels": "8,661",
    "duration": "10",
    "time": "2019-07-25 09:30:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.memory_utilization.5m",
    "serial": "CNHHKLB031",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwogGqYVQO1ZtiGgc2L",
  "severity": "Major"
}
```


Controller OSPF Session Error


```
{
  "alert_type": "CONTROLLER OSPF SESSION ERROR",
  "description": "OSPF session state change for Gateway with hostname GSK_VPNC2 and serial
CW0003307 from Init State to Down State
     for neighbor 1.0.0.2 on interface 100 with reason No hello packets received from
neighbour.Inactivity timer fired",
  "timestamp": 1564121712,
  "webhook": "60785e88-9513-4352-94d6-ec25fedbeddc",
  "setting_id": "b27f67fa44234c51a890fccea7c9b83e-1354",
  "state": "Open",
  "nid": 1354,
  "details": {
    "dst_state": "Down State",
    "neighbour_ip": "1.0.0.2",
    "group": "4",
    "uniq_identifier": "100-16777218",
    "labels": [
      "2",
      "11",
      "12",
      "15",
      "13",
      "8"
    ],
    "src_state": "Init State",
    "reason": "No hello packets received from neighbour.Inactivity timer fired",
    "time": "2019-07-26 06:15:12 UTC",
    "interface": "100",
    "serial": "CW0003307",
    "hostname": "GSK_VPNC2"
  },
  "operation": "create",
  "device_id": "CW0003307",
  "id": "AWws60Yxon2R5PyMmUU4",
  "severity": "Major"
}
```


Gateway Base License Capacity Exceeded


```
{
  "alert_type": "GATEWAY_BASE_LICENSE_CAPACITY_EXCEEDED",
  "description": "Base license capacity limit exceeded for Gateway with name: Dev-BR1-GW-
Kafka, serial: CP0015859",
  "timestamp": 1564141290,
  "webhook": "1348bcc4-ce00-4180-b314-32849c3638a1",
  "setting_id": "2fb4b8a7e77c496395950510a1d270bc-1356",
  "state": "Open",
  "nid": 1356,
  "details": {
    "serial": "CP0015859",
    "labels": [],
```

```
    "group": "1",
    "name": "Dev-BR1-GW-Kafka",
    "time": "2019-07-26 11:41:30 UTC"
  },
  "operation": "create",
  "device_id": "CP0015859",
  "id": "AWwuFgZqnGtA5yFV0hCr",
  "severity": "Critical"
}
```


DHCP Pool Consumption Alert


```
{
  "alert_type": "DHCP_POOL_CONSUMPTION_ALERT",
  "description": "DHCP Pool Consumption on Gateway CNHHKLB031 is 12% at 2019-07-25 13:02:39
UTC for 192.168.53.0/24",
  "timestamp": 1564059759,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1510",
  "state": "Open",
  "nid": 1510,
  "details": {
    "subnet": "192.168.53.0/24",
    "group": "77",
    "name": "None",
    "labels": "8,661",
    "time": "2019-07-25 13:02:39 UTC",
    "threshold": "12",
    "serial": "CNHHKLB031",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpOfQAVQO1ZtiGiE2H",
  "severity": "Critical"
}
```


WAN Auto Negotiation


```
{
  "alert_type": "WAN_UPLINK_AUTONEGOTIATION_STATE_CHANGE",
  "description": "WAN ports autonegotiaton speed changed from 1000 Mbps to Auto Mbps for
device with CNHHKLB031 for
     uplink GE0/0/1 at 2019-07-25 12:46:36 UTC",
  "timestamp": 1564058796,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1506",
  "state": "Open",
  "nid": 1506,
  "details": {
    "new_speed": "Auto",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "intf_name": "GE0/0/1",
    "time": "2019-07-25 12:46:36 UTC",
    "serial": "CNHHKLB031",
    "speed": "1000"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpK0IxVQO1ZtiGh8oh",
  "severity": "Minor"
}
```

WAN Uplink Status Change


```
{
  "alert_type": "WAN_UPLINK_STATUS_CHANGE",
  "description": "Uplink port link1_inet status change UP -&gt; DOWN for device with
CNHHKLB031 at 2019-07-25 09:22:31 UTC",
  "timestamp": 1564046551,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1505",
  "state": "Open",
  "nid": 1505,
  "details": {
    "status": "UP",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "current_status": "DOWN",
    "intf_name": "link1_inet",
    "time": "2019-07-25 09:22:31 UTC",
    "serial": "CNHHKLB031",
    "uplink_tag": "link1_inet"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwocGtYVQO1ZtiGgT03",
  "severity": "Major"
}
```


Gateway Threat Count


```
{
  "alert_type": "GW_IDS_IPS_ALERT_THREAT_OVER_A_PERIOD",
  "id": "AXX7N0IhaFBUFq6FQ2R1",
  "nid": 2305,
  "setting_id": "8fc0df01a43b42aa9f8e9fbc3d3b9d35-2305",
  "device_id": "TWJ6KSP005",
  "description": "Dear Incident Manager, Your Aruba Central Portal admin configured an
   email alert notification to be sent to this email address Why this alert? Aruba Branch
   Gateway
   https://app-yoda.arubathena.com/frontend/#/GATEWAYDETAIL/OVERVIEW/TWJ6KSP005aruba9004
   _lte with serial number TWJ6KSP005exceeded 50 threat events in last 10 minutes,
   triggering this CRITICAL Alert notification What is next? Reach out to your
   Aruba Central Portal admin to address this incident .If not addressed or
   if the situation escalates, you may continue to receive similar alert
   notifications. More Information Go to
   https://app-yoda.arubathena.com/frontend/#/IDPS_DASHBOARDSystem Generated Email
   from Aruba Central based on alert configuration; do not reply Thanks, Aruba Central",
  "state": "Close",
  "severity": "Critical",
  "operation": "update",
  "timestamp": 1606238738,
  "details__threshold": 50,
  "details__agg_field_name": "device",
  "details__duration": 10,
  "details__device": "TWJ6KSP005",
  "details__severity": "CRITICAL",
  "details__rule_id": 0,
  "details__serial": "TWJ6KSP005",
  "details__name": "aruba9004_lte",
  "details__group_id": 73,
  "details__time": "2020-11-24 16:55:04 UTC",
  "webhook": "001378a5-bfb1-465e-a955-0034ef801136",
  "text": "Dear Incident Manager, Your Aruba Central Portal admin configured an email
```

```
   alert notification to be sent to this email address Why this alert? Aruba Branch
   Gateway
   https://app-yoda.arubathena.com/frontend/#/GATEWAYDETAIL/OVERVIEW/TWJ6KSP005aruba9004
   _lte with serial number TWJ6KSP005exceeded 50 threat events in last 10 minutes,
   triggering this CRITICAL Alert notification What is next? Reach out to your Aruba
   Central Portal admin to address this incident. If not addressed or if the situation
   escalates, you may continue to receive similar alert notifications.
   More Information Go to
   https://app-yoda.arubathena.com/frontend/#/IDPS_DASHBOARDSystem Generated Email
   from Aruba Central based on alert configuration; do not reply Thanks, Aruba Central"
}
```

Gateway Threat Count per Signature

```
{
  "alert_type": "GW_IDS_IPS_ALERT_THREAT_SID_OVER_A_PERIOD",
  "id": "AXX7N0LFaFBUFq6FQ2R2",
  "nid": 2306,
  "setting_id": "8fc0df01a43b42aa9f8e9fbc3d3b9d35-2306",
  "device_id": 2003068,
  "description": "Dear Incident Manager, Your Aruba Central Portal admin configured
   an email alert notification to be sent to this
   email address Why this alert? Threat events of signature id 2003068 exceeded the
   threshold 30 in last 30minutes, triggering this CRITICAL Alert notification. What
   is next? Reach out to your Aruba Central Portal admin to address this incident.
   If not addressed or if the situation escalates, you may continue to receive
   similar alert notifications. More Information
   Go to https://app-yoda.arubathena.com/frontend/#/IDPS_DASHBOARDSystem Generated
   Email from Aruba Central based on alert
   configuration; do not reply Thanks, Aruba Central",
  "state": "Close",
  "severity": "Critical",
  "operation": "update",
  "timestamp": 1606239938,
  "details__threshold": 30,
  "details__duration": 30,
  "details__agg_field_name": "signature",
  "details__signature": 2003068,
  "details__severity": "CRITICAL",
  "details__rule_id": 0,
  "details__serial": 2003068,
  "details__time": "2020-11-24 16:35:04 UTC",
  "webhook": "001378a5-bfb1-465e-a955-0034ef801136",
  "text": "Dear Incident Manager, Your Aruba Central Portal admin configured an email
   alert notification to be sent to this email address .Why this alert? Threat events
   of signature id 2003068 exceeded the threshold30 in last 30minutes, triggering this
   CRITICAL Alert notification. What is next? Reach out to your Aruba Central Portal
   admin to address this incident. If not addressed or if the situation escalates,
   you may continue to receive similar alert notifications. More Information Go
   to https://app-yoda.arubathena.com/frontend/#/IDPS_DASHBOARD System Generated
   Email from Aruba Central based on alert configuration; do not reply Thanks,
   Aruba Central"
}
```

Miscellaneous Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

Device Config Change Detected

```
{
  "alert_type": "DEVICE_CONFIG_CHANGE_DETECTED",
  "description": "Config change detected on group nbapi_test for device type Switch by user
     example@hpe.com.\n\nSerial: None, \nMacAddress: None,
```

```
     \nConfig Content: Template Updated
     \nmodel: ALL\nversion: ALL\ndevice_type: HPPC\ntemplate changes: \n @@ -18,6 +18,6
@@\n\n\n
     ip address dhcp-bootp\n\n exit\n\n vlan 13\n\n- name \"vlan_8888\"\n\n+ name \"vlan_
44\"\n\n no ip address\n\n exit ",
  "timestamp": 1564383294,
  "webhook": "272eda1a-f79b-4192-ad6f-b35da11515bc",
  "setting_id": "715e45fe3ff8453da355cd34aff2afa5-2000",
  "state": "Open",
  "nid": 2000,
  "details": {
    "config_change": "Template Updated\nmodel: ALL\nversion: ALL\ndevice_type:
HPPC\ntemplate changes: \n @@ -18,6 +18,
     6 @@\n\n\n ip address dhcp-bootp\n\n exit\n\n vlan 13\n\n- name \"vlan_8888\"\n\n+
name \"vlan_44\"\n\n no ip address\n\n exit ",
    "macaddr": "None",
    "group": "8",
    "dev_type": "Switch",
    "labels": "None",
    "group_name": "nbapi_test",
    "_rule_number": "0",
    "params": "None",
    "user": "example@hpe.com",
    "time": "2019-07-29 06:54:54 UTC",
    "serial": "None"
  },
  "operation": "create",
  "device_id": "",
  "id": "AWw8grSBeZ6A6PlBvMk4",
  "severity": "Warning"
}
```


User Account Deleted


```
{
  "alert_type": "User account deleted",
  "description": "User with name v@gmail.com deleted.",
  "timestamp": 1569234480,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-15",
  "state": "Open",
  "nid": 15,
  "details": {
    "group": "-1",
    "labels": "None",
    "params": [
      "v@gmail.com"
    ],
    "_rule_number": "0",
    "time": "2019-09-23 10:28:00 UTC"
  },
  "operation": "create",
  "device_id": "",
  "id": "AW1dqe6rYu0OgJ2alXzT",
  "severity": "Major"
}
```


New User Account Added


```
{
  "alert_type": "New User account added",
  "description": "User account setting updated for user: newuser@gmail.com with
language:en_US and idle timeout: 1800",
  "timestamp": 1569234534,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-14",
```

```
  "state": "Open",
  "nid": 14,
  "details": {
    "group": "-1",
    "labels": "None",
    "params": [],
    "_rule_number": "0",
    "time": "2019-09-23 10:28:54 UTC"
  },
  "operation": "create",
  "device_id": "",
  "id": "AW1dqr6nYu0OgJ2alX1l",
  "severity": "Major"
}
```


User Account Edited


```
{
  "alert_type": "User account edited",
  "description": "User with Name newuser@gmail.com, role readwrite and access [] updated.",
  "timestamp": 1569235100,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-16",
  "state": "Open",
  "nid": 16,
  "details": {
    "group": "-1",
    "labels": "None",
    "params": [
      "newuser@gmail.com",
      "readwrite",
      "[]"
    ],
    "_rule_number": "0",
    "time": "2019-09-23 10:38:20 UTC"
  },
  "operation": "create",
  "device_id": "",
  "id": "AW1ds2LcYu0OgJ2alYM2",
  "severity": "Major"
}
```


Integrating Aruba Central with ServiceNow

ServiceNow is an IT service management platform that allows you to automatically create incidents or IT tickets based on a live data feed from a Webhook service. If you have a ServiceNow instance, you can configure a Webhook service in Aruba Central to send a notification feed. The ServiceNow integration enables your current IT Infrastructure management systems to automatically generate an IT incident or a ticket whenever an alert is triggered due to a user-generated event in Aruba Central.

Before You Begin

Before you begin, ensure that you have a valid ServiceNow account. If you do not have a ServiceNow instance, create an instance before you proceed with the steps described in following sections.

For more information on creating a ServiceNow instance, see the ServiceNow user documentation.

Integration Workflow

Complete the following steps to enable ServiceNow integration with Aruba Central:

- Step 1: Add the Hash Library to Your ServiceNow Instance
- Step 2: Create a Scripted REST API to Obtain a Webhook URL
- Step 3: Configure a Webhook in Aruba Central
- Step 4: Configure an Alert in Aruba Central
- Step 5: Verify the Integration Status

Step 1: Add the Hash Library to Your ServiceNow Instance

To get started with the ServiceNow integration, create a new script with the hash library in your ServiceNow instance. The hash library is required for header authentication.

1. Log in to ServiceNow with your user credentials.
2. Click **Manage** > **Instance** and log in to your instance.
3. Go to **System Definition** > **Script Includes**.
4. Click **New**.
5. Name the script as **Hashes**.
6. Select **All application scopes** from the **Accessible from** drop-down list.
7. Select the **Client callable** check box.
8. Go to the GitHub Gist website that hosts the hash library.
9. Copy the **snow_hashes.js** file content and paste it in the **Script** text box.
10. Click **Submit**.

Step 2: Create a Scripted REST API to Obtain a Webhook URL

To create a Scripted REST API:

1. In your ServiceNow instance, go to **System Web Services** > **Scripted REST APIs**.
2. Click **New**. The REST API creation page is displayed.
3. Enter a name and the API ID.
4. Click **Submit**. The API is added to the list of REST APIs.
5. Open the REST API that you created.
6. To add a REST resource with the header and query parameters, click **New** in the **Resources** tab. The **Scripted REST Resource New record** page is displayed.
7. Provide a name for the resource.
8. Select **POST** for the HTTP method.
9. Clear the **Requires authentication** check box.
10. In the **Script** section, add the following text:

```
(function process( /*RESTAPIRequest*/ request, /*RESTAPIResponse*/ response) {
    // Calcuate signature for verification using request headers, data and token
    var centralService = request.getHeader('X-Central-Service');
    var centralDeliveryId = request.getHeader('X-Central-Delivery-ID');
```

```
    var centralDeliveryTimestamp = request.getHeader('X-Central-Delivery-
Timestamp');
    var token = "<webhook_token>";
    var body = request.body.dataString;
    var message = body + centralService + centralDeliveryId +
centralDeliveryTimestamp;
    var calculatedSign = new Hashes.SHA256().b64_hmac(token, message);
    var signFromServer = request.getHeader('X-Central-Signature'); // Signature
sent by Aruba Central
    var low_severities = ["Minor", "Warning"];
    if (calculatedSign == signFromServer) {
        event = JSON.parse(body);
        // Only process events from Central which has status Open
        if (event.state == "Open") {
            var inc = new GlideRecord('incident');
            inc.initialize();
            inc.short_description = event.alert_type;
            inc.state = 1;
            if (low_severities.includes(event.severity)) {
                inc.impact = 3;
                inc.urgency = 3;
            } else if (event.severity == "Major") {
                inc.impact = 2;
                inc.urgency = 2;
            } else if (event.severity == "Critical") {
                inc.impact = 1;
                inc.urgency = 1;
            }
            inc.description = event.description;
            inc.insert();
        }
        response.setStatus(200);
        response.setBody({
            status: "success"
        });
    } else {
        response.setStatus(200);
        response.setBody({
            status: "failure"
        });
     }
})(request, response);
```

After you create a Webhook in Aruba Central replace the Webhook token (see highlighted text in the above code sample) in your Scripted REST API.

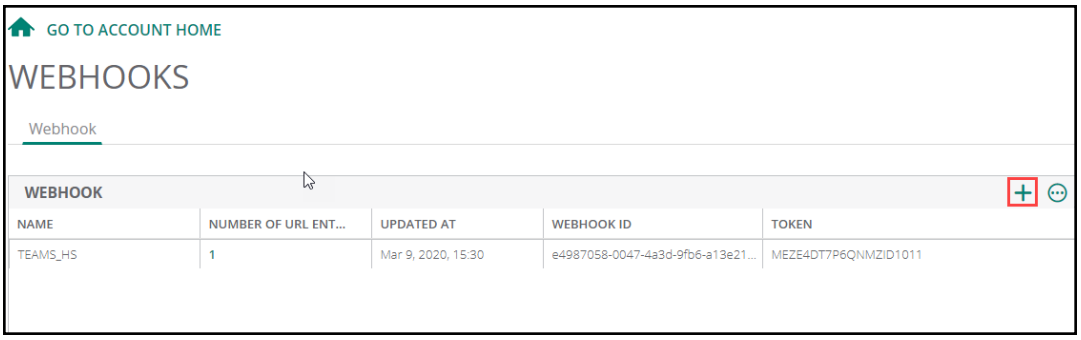
11. Click **Submit**. The Scripted REST API that you created is added to the list of APIs.

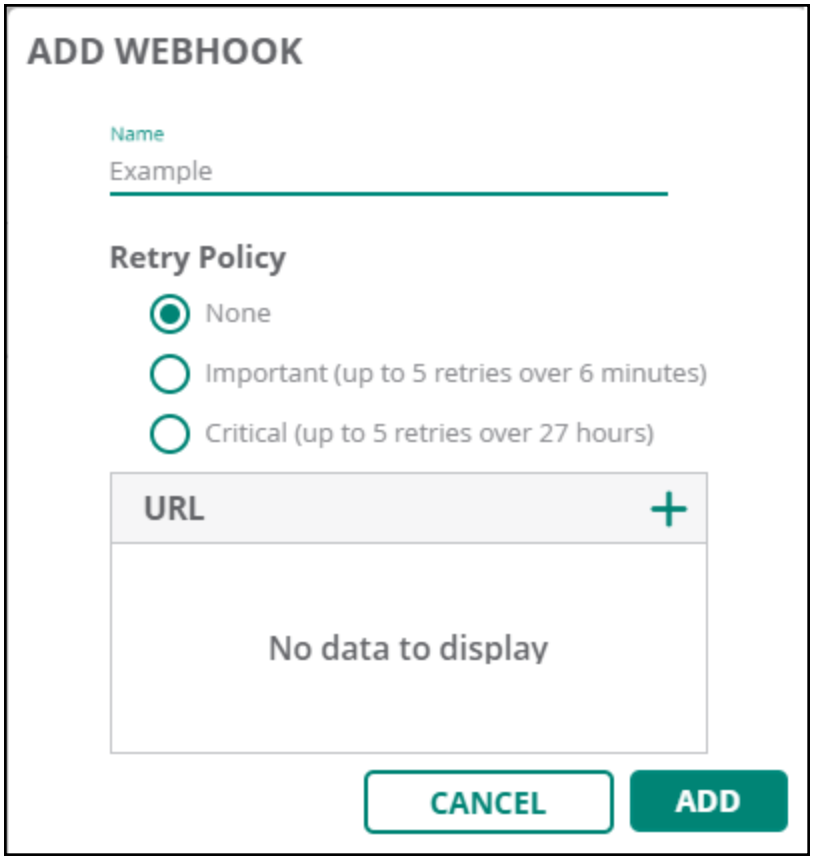
12. Note the base API path. The base API path must be appended to your Webhook URL.
13. Ensure that your Webhook URL is in the following format: **https://<yourInstanceName>.service-now.com/<baseApiPath>**.

Step 3: Configure a Webhook in Aruba Central

To create a Webhook in Aruba Central:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**. The **Webhooks** page is displayed.
2. In the **Webhook** tab, click the **+** sign. The **Add Webhook** window is displayed.





a. **Name**—Enter a name for the Webhook
b. **Retry Policy**— Select any one of the following options:
   - **None**—Select this to have no retry.
   - **Important**—Select this to have up to 5 retries over 6 minutes.
   - **Critical**—Select this to have up to 5 retries over 27 hours.
c. **URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.

   https://<yourInstanceName>.service-now.com/<baseApiPath>

   The URL must include your ServiceNow instance and the base API path generated for your Scripted REST API.

3. Click **Save**. The Webhooks is created and listed in the **Webhook** table.
4. Note the token ID.
5. Go back to your ServiceNow instance and update the Webhook token in the script text of the Scripted REST API you created in step 2.

NOTE

You can also create a Webhook using the API interface. For more information, see Webhook documentation in Aruba Central documentation portal.

Step 4: Configure an Alert in Aruba Central

To configure an alert in Aruba Central:

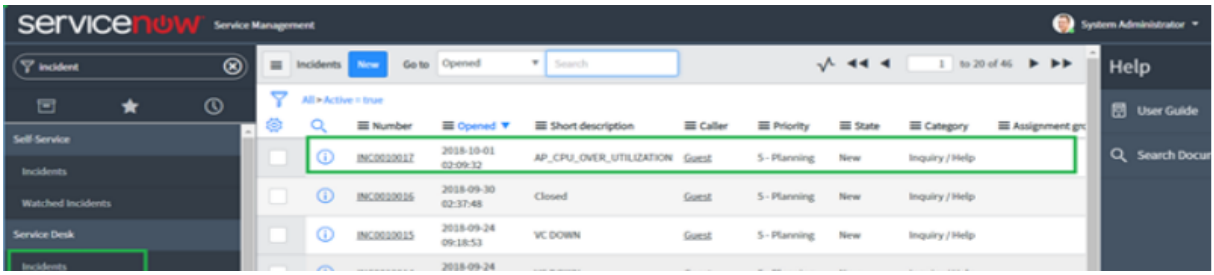
1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Alerts & Events** to view the alert and events dashboard.

3. To configure alerts, click the **Config** icon.
4. In the **Alert Severities & Notifications** page, click **All**.
5. Select an alert and click **+** to enable the alert with default settings.
6. Configure the following alert parameters.
   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning.
   b. **Duration**—Enter the duration in minutes.
   c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting any of the following parameters:
      - **Group**—Select a group to limit the alert to a specific group.
      - **Label**—Select a label to limit the alert to a specific label.
      - **Device**—Select a device to limit the alert to a specific device.
   d. Select **Webhook** check box under **Notification Options** and select a webhook from the drop-down list.
   e. Click **Save**.

Step 5: Verify the Integration Status

To verify if the integration is successful:

1. Trigger an alert from Aruba Central.
2. Verify if an incident is created in your ServiceNow instance.



Streaming API

Streaming API allows customers to subscribe to select set of services instead of polling the NB API to get an aggregated state or statistics of the events. For example, with Streaming API, the customers can get notifications about the following types of events:

- The UP and DOWN status of the devices
- Change in location of stations

For a complete list of supported services, with Streaming API, users can write value-added applications based on the aggregated context.

- Streaming API service in Aruba Central is enabled if one of the devices in the account has an Advanced License. If the account has only Foundation License, Steaming API tab is not displayed in Aruba Central. For more information about streaming API feature in the Aruba Central licensing model, see *Aruba Central Licensing Guide*.
- Streaming API service is not supported at MSP level.

Supported Services

Streaming API supports the following services:

- Audit—The Audit messages are sent to notify events like device connectivity, configuration status, and firmware status.
- AppRF—AppRF stream is the flow of all the client sessions. For each connected devices (IAP/BGW), It lists the client's web session information of the past 14/15 minutes (Ip, Rx/Tx, Timestamp, etc).
- Monitoring—The monitoring streaming event is generated for state message (on state change) and stats message (received for every 5 minutes).
- Presence —The Presence events are sent to provide details of all associated and unassociated clients detected by Instant AP devices.
- Location—A location event is generated when the location of a client is computed using RSSI values reported by IAPs. The event message includes co-ordinates of the client on the VisualRF floorplan.
- Security—The Security streaming event is generated when the IAPs have enabled Intrusion Detection. This feed contains all the IDS detections reported by the IAPs in the network.

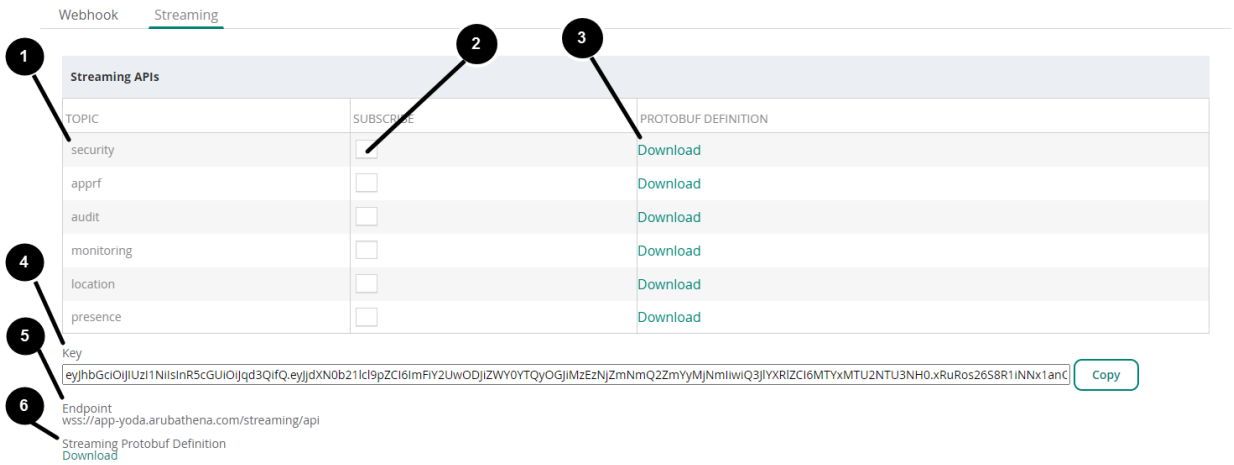
Viewing the Streaming API Page

Perform the following steps to view the **Streaming API** page:

1. Log in to **Account Home**.
2. Under **Global Settings**, click the **Webhooks** menu option.
3. Click the **Streaming** tab.

   The following is an illustration of the **Streaming API** page:

Figure 97 *View of the Streaming API Page*



The parameters in the page are described in the following table. Refer to the callout numbers.

Table 57: *Parameters of the Streaming API Page*

Callout	API	Description
1	**Topic**	A list of available topics for streaming APIs. To receive streaming events from a topic, subscribe to the specific topic.
2	**Subscribe**	Enables Aruba Central to stream events for a specific topic when this box is enabled.
3	**Protobuf Definition**	Definition of the specific topic. All WebSocket response messages are encapsulated in a protocol buffer, the format of which you can download.
4	**Key**	Access token for establishing a WebSocket connection.
5	**Endpoint**	WebSocket endpoint address for the Aruba Central instance.
6	**Streaming Protobuf Definition**	The protocol buffer in which all the incoming streaming messages are encapsulated. This protobuf is further used to identify the topic of the message received and decode the topic-specific protobuf message.

Subscribing to a Streaming API Topic

- Only Aruba Central admin users can subscribe to, or unsubscribe from, a topic.
- In case a live WebSocket connection breaks, reconnect the connection.

To subscribe to a streaming API topic:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**. The **Webhooks** page is displayed.
2. In the **Webhooks** page, click **Streaming** tab. The Streaming page is displayed.

3. In the **Streaming APIs** table, select the check box corresponding to the topic that you want to subscribe. To unsubscribe a topic, clear the corresponding check box.
4. In the **Webhooks > Streaming** page, the following details are displayed:
   - **Key**—Access token. The token comes with a validity of seven days after which a new token needs to be generated.
   - **Endpoint**—WebSocket endpoint.
   - **Streaming Protobuf Definition**—Allows you to download the Streaming protocol buffer definition.

Use the WebSocket endpoint and access token to establish a WebSocket connection and start streaming data for the topics you have subscribed to.

Downloading Protobuf Definition for a Streaming API topic

To download the protobuf definition, complete the following steps:

1. In the **Streaming APIs** table, click the **Download** button corresponding to the protobuf definition for the topic to which you have subscribed. The following topics are available for download:
   - **Apprf**—Protocol buffer specification of the AppRF topic.
   - **Audit**—Protocol buffer specification of the Audit topic.
   - **Monitoring**—Protocol buffer specification of the Monitoring topic.
   - **Presence**—Protocol buffer specification of the Presence topic.
   - **Location**—Protocol buffer specification of the Location topic.
   - **Security**—Protocol buffer specification of the Security topic.

Retrieving a New Token

The access token comes with a validity of seven days after which a new token needs to be generated.

You can retrieve the token either directly from the UI or by using the API.

1. To retrieve the new access token from the Aruba Central UI, complete the following steps:
   a. In the **Account Home** page, under **Global Settings**, click **Webhooks > Streaming** tab. The **Streaming** page is displayed.
   b. You can retrieve the valid token from the **Key** field. The token gets refreshed automatically after seven days of its generation.
2. To retrieve the new access token from the API, here are the details required:
   - **API**— `https://<central-host>/streaming/token/validate`
   - **Method**—GET
   - **Authorization**—Enter the current token

     The API will return the same token if the old token is not expired or will return a new token in case the old token is expired.

Enabling Data Streaming From a Topic

Complete the following steps to receive streaming events from Aruba Central:

1. Create a WebSocket connection: `wss://<central-host>/streaming/api`
2. Set the following additional headers:
   - **UserName**—Username of the admin. This is an optional header.
   - **Authorization**—Access token. For more information about how to generate the key, see Subscribing to a Streaming API Topic.
   - **Topic**—Value of the topic to which you have subscribed. The value should be one of the following:
     - apprf
     - monitoring
     - audit
     - presence
     - location
     - security
3. Start the read loop to read the events. The payload is a protocol buffer message.

Decoding WebSocket Response Messages

All WebSocket response messages are encapsulated in a protocol buffer. When a message is received, use the subject (topic) to identify the message and invoke an appropriate message processor. To decode the message, refer to the protocol buffer specification of the respective topic.

The format is as follows:

```
message MsgProto {
string subject = 2; // subject
bytes data = 3; // payload
int64 timestamp = 4; // received timestamp
string customer_id = 5; // customer id to which this data belongs
string msp_id = 6; // optional field indicating the msp_id
}
```

Viewing Audit Trails in the Account Home Page

The **Audit Trail** page shows the logs for all the device management, configuration, and user management events triggered in Aruba Central.

To view audit trail logs:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**. The **Audit Trail** page opens.
2. From the **Select App** drop-down list, select one of the following:
   - **All Apps**—Displays audit trail logs for all apps.
   - **Network Operations**—Displays audit trail logs for the **Network Operations** app.
   - **ClearPass Device Insight**—Displays audit trail logs for the **ClearPass Device Insight** app.

The following table describes the fields displayed in the **Audit Trail** table:

Table 58: *Audit Trail Details*

Parameter	Description
Occurred On	Time stamp of the events for which the audit trails are shown.
IP Address	IP address of the client device.
Username	Username of the admin user who applied the changes.
Target	Group or device to which the changes were applied.
Source	Tenant account in which the changes occurred. **NOTE:** This column is applicable only in the MSP mode.
Category	Type of modification and the affected device management category.
Description	A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click  to view the complete details of the event. For example, if an event was not successful, click the ellipsis to view the reason for the failure.

The **Maintain** menu includes the following options:

- **Firmware**—Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. For more information see, Managing Software Upgrades.
- **Organization**—Allows you to create groups, sites or labels, upload certificates, and manage site installations. See the following topics:
  - Groups for Device Configuration and Management
  - Sites and Labels
  - Certificates
  - Installation Management

Groups for Device Configuration and Management

Aruba Central simplifies the configuration workflow for managed devices by allowing administrators to combine a set of devices into groups. A group in Aruba Central is the primary configuration element that functions as a container for device management, monitoring, and maintenance. Groups enable administrators to manage devices efficiently by using either a UI-based configuration workflow or CLI-based configuration template.

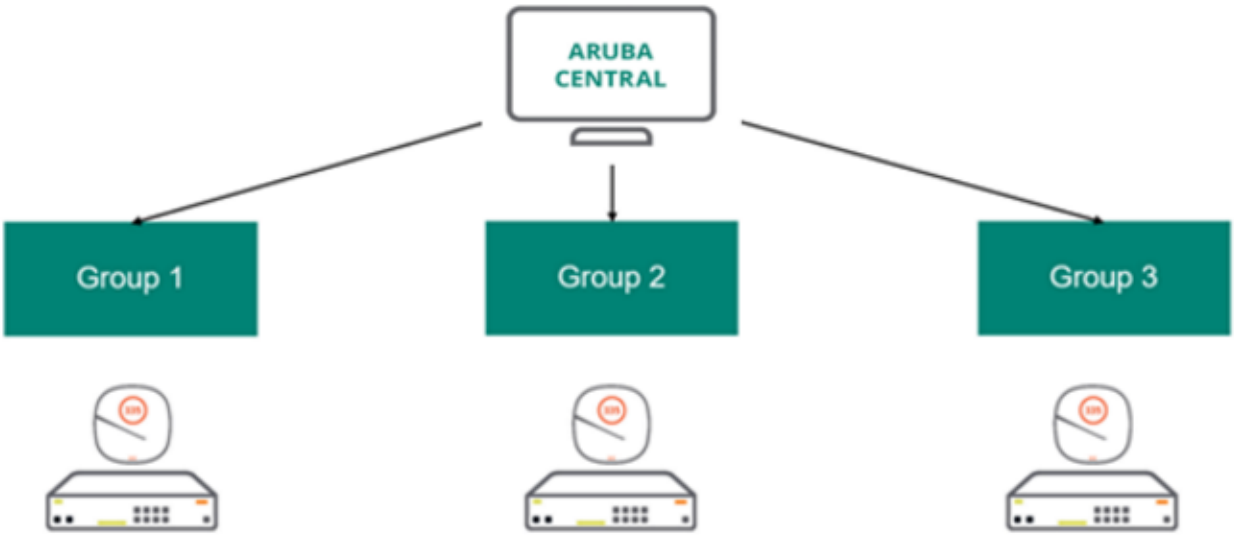
Groups provide the following functions and benefits:

- Ability to provision multiple devices in a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to member Instant APs in their respective Instant AP clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.
- Ability to provision different types of devices in a group. For example, a group can consist of Instant APs, Gateways, and Switches.
- Ability to create a configuration base and add devices as necessary. When you assign a new device to a group, it inherits the configuration that is currently applied to the group.
- Ability to create a clone of an existing group. If you want to build a new group based on an existing group, you can create a clone of the group and customize it as per your network requirements.

- A device can be part of only one group at any given time.
- Groups in Aruba Central are mutually exclusive (independent) and do not follow a hierarchical model.

The following figure illustrates a generic group deployment scenario in Aruba Central:

Figure 98 *Group Deployment*



Group Operations

The following list shows the most common tasks performed at a group level:

- Configuration— Add, modify, or delete configuration parameters for devices in a group
- User Management—Control user access to device groups and group operations based the type of user role
- Device Status and Health Monitoring—View device health and performance for devices in a specific group.
- Report Generation—Run reports per group.
- Alerts and Notifications—View and configure notification settings per group.
- Firmware Upgrades—Enforce firmware compliance across all devices in a group.

Group Configuration Modes

Aruba Central allows network administrators to manage device configuration using either UI workflows or configuration templates:

- UI-based configuration method—For device groups that use UI-based workflows, Aruba Central provides a set of UI menu options. You can use these UI menu options to configure devices in a group. You can also secure the UI-based device groups with a password and thus restrict user access.
- Template-based configuration method—For device groups that use a template-based workflow, Aruba Central allows you to manage devices using configuration templates. A device configuration template includes a set of CLI commands and variable definitions that can be applied to all other devices deployed in a group.

If your site or store has different types of devices, such as the Instant APs, Switches, and Gateways, and you want to manage these devices using different configuration methods, that is, either using the UI or template-based workflows, you can create a single group and define a configuration method to use for each type of device. This allows you to use a single group for both UI and template based configuration and eliminates the need for creating separate groups for each configuration method.

For example, you can create a group with the name **Group1** and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and

Gateways. Aruba Central identifies both these groups under a single name (**Group1**). If a device type in the group is marked for template-based configuration method, the group name is prefixed with **TG** prefix is added (**TG Group1**. You can use **Group1** as the group ID for workflows such as user management, monitoring, reports, and audit trail.

When you add Instant APs, Gateways, and switches to a group, Aruba Central groups these devices based on the configuration method you chose for the device type, and displays relevant workflows when you try to access the respective configuration menu.

For information on how to create a group, see Creating a Group.

Default Groups and Unprovisioned Devices

The **default** group is a system-defined group to which Aruba Central assigns all new devices with factory default configuration. When a new device with factory default configuration connects to Aruba Central, it is automatically added to the **default** group.

If a device has customized configuration and connects to Aruba Central, Aruba Central marks the device as **Unprovisioned**. If you want to preserve the device configuration, you can create a new group and assign this device to the newly created group. If you want to overwrite the configuration, you can move the unprovisioned device to an existing group.

The unprovisioned state does not apply to Aruba Switches as only the factory-default switches can join Aruba Central.

Best Practices and Recommendations

Use the following best practices and recommendations for deploying devices in groups:

- Determine the configuration method (UI or template-based) to use based on your deployment, configuration, and device management requirements.
- If there are multiple sites with similar characteristics—for example, with the same device management and configuration requirements—assign the devices deployed in these sites to a single group.
- Apply device-level or cluster-level configuration changes if necessary.
- Use groups cloning feature if you need to create a group with an existing group configuration settings.
- If the user access to a particular site must be restricted, create separate groups for each site.

Working with Groups

See the following topics for detailed information and step-by-step instructions on how to manage groups and provision devices assigned to a group:

- Managing Groups
- Provisioning Devices Using UI-based Workflows
- Provisioning Devices Using Configuration Templates

Managing Groups

The **Groups** page allows you to create, edit, or delete a group, view the list of groups provisioned in Aruba Central, and assign devices to groups.

This section describes the following topics:

Creating a Group

Aruba Central allows you to manage configuration for different types of devices, such as Aruba Instant APs, Gateways, and switches in your inventory. These devices can be configured using either UI workflows or configuration templates. You can define your preferred configuration method when creating a group.

Aruba Central allows you to create a single group with different configuration methods defined for each device type. For example, you can create a group with the name **Group1** and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (**Group1**). If a device type in the group is marked for template-based configuration method, the group name is prefixed with **TG**, (**TG Group1**. You can use **Group1** as the group ID for workflows such as user management, monitoring, reports, and audit trail.

After you assign devices to group and when you access configuration containers, Aruba Central automatically displays relevant configuration options based on the configuration method you defined for the device group.

To create a group:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.

   By default, the **Groups** page is displayed.
3. Click (+) **New Group**. The **Create New Group** pop-up window opens.
4. Enter a name for the group. The group name can be a maximum of 32 single byte ASCII characters if you use the UI to create the names. However, if you are using an NB API, the character limit increases to 128. A group name supports all special characters excluding the ">" character. System-defined group names such as "default", "unprovisioned", and "global" are not allowed in group names.

By default, Aruba Central enables template-based configuration method for switches and UI-workflow-based configuration method for Instant AP and Gateway.

5. To enable template-based configuration method for all device categories:
   - For Instant APs or Gateways, select the **IAP and Gateway** check box.
   - For Switches, ensure that **Switch** check box is selected. The **Switch** check box is enabled by default.
6. To enable UI-based configuration method on all device categories:
   a. For Instant APs and Gateways, ensure that the **IAP and Gateway** check box is cleared.
   b. For switches, clear the **Switch** check box.
7. Assign a password. This password enables administrative access to the device interface.
8. Click **Add Group**.

NOTE

You can also create a group that uses different provisioning methods for switch, and IAP and Gateway device categories. For example, you can create a group with template-based provisioning method for switches and UI-based provisioning method for Instant APs and Gateways.

Assigning Devices to Groups

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory.**

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Viewing Groups and Associated Devices

To view the groups dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed. The groups table on the left side of the page displays the following information:
   - **Group Name**—Name of the group.
   - **Devices**—Number of devices assigned to a group.
   - **All Connected Devices**—Total number of devices provisioned in Aruba Central. The devices table on right side of the page shows all the devices provisioned in Aruba Central.
   - **Unassigned Devices**—Total number of devices that are yet to be assigned. The devices table on the right shows the devices are not assigned any group.

NOTE

The devices table is not available for MSP users as the devices are primarily assigned to tenant accounts. However, MSP administrators can drill down to a tenant account and view devices mapped to a group.

3. To view the devices assigned to a group, select the group from the table on the left. The devices table displays the following information:
   - **Name**—Name of the device.
   - **Location**—Physical location of the device.
   - **Type**—Type of the device such as Instant AP or Switch.
   - **Serial**—Serial number of the device.
   - **MAC Address**—MAC address of the device.

Creating a New Group by Importing Configuration from a Device

To import configuration from an existing device to a new group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. Select the device from which you want to import the configuration.
4. Click **Import Configuration to New Group**. The **Import Configuration** pop-up window opens.
5. Enter a name for the group.
6. Configure a password for the group.
7. Click **Import Configuration**.

Cloning a Group

To clone a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. To create a clone of an existing group, select the group from the groups table and click **Clone Selected Group**.
4. Enter a name for the cloned group.
5. Click **Add Group**.

When you clone a group, Aruba Central also copies the configuration templates applied to the devices in the group.

Moving Devices between Groups

To move a device from one group to another group:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. From the devices table on the right, select from the following device options that you want to move:
   - Virtual Controller—Moving a Commander VC also moves the member IAP(s) to the new group.
   - Switch stack—Moving a commander stack also moves the member switches to the new group.
   - Standalone IAP—Moving a standalone IAP moves only that particular IAP to the new group.
   - Standalone switch—Moving a standalone switch moves only that particular switch to the new group.
   - Gateways (MC)—Moving a standalone MC moves only that particular MC to the new group.
4. Drag and drop the device to group to which you want to assign the device.
5. Click **Yes** when the system prompts you to confirm device movement.

MSP mode does not support moving devices across different groups.

Configuring Device Groups

For information on provisioning devices in groups, see the following topics:

- Provisioning Devices Using UI-based Workflows
- Provisioning Devices Using Configuration Templates

Configuring Groups in MSP Mode

For information on using groups in the MSP mode and instructions on how to assign devices to MSP tenants, see the *Aruba Central Managed Service Provider User Guide*.

Deleting a Group

When you delete a group, Aruba Central removes all configuration, templates, and variable definitions associated with the group. Before deleting a group, ensure that there are no devices attached to the group.

To delete a group:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. From the list of groups, select the group that you want to delete.
4. Click the delete icon.
5. Confirm deletion.

Assigning Devices to Groups

In Aruba Central, devices are assigned to groups for configuration, monitoring, and management purposes. A group in Aruba Central is a primary configuration element that acts like a container. In other words, groups are a subset of one or several devices that share common configuration settings. Aruba Central supports assigning devices to groups for the ease of configuration and maintenance. For example, you can create a common group for Branch Gateways or Instant APs that have similar configuration requirements.

Assigning Instant APs to Groups

The Instant AP groups may consist of the configuration elements:

- Instant AP Cluster—Consists of a conductor Instant AP and a set of member Instant APs in the same VLAN.
- Virtual Controller—A virtual controller provides an interface for entire cluster. The member Instant APs and conductor Instant APs function together to provide a virtual interface.
- Conductor Instant AP and Member Instant AP—In a typical Instant AP deployment scenario, the first Instant AP that comes up is elected as the conductor Instant AP. All other Instant APs joining the cluster function as the member Instant APs. When a conductor Instant AP is elected, the member Instant APs download the configuration changes.

The following table describes the group assignment criteria for Instant APs:

Table 59: *Instant AP Group Assignment*

APs with Default Configuration	APs with Non-Default Configuration
If an Instant AP with factory default configuration joins Aruba Central, it is automatically assigned to the **default** group or to an existing group with similar configuration settings. The administrators can perform any of the following actions: ■ Manually assign them to a pre-provisioned group. ■ Create a new group.	If an Instant AP with non-default or custom configuration joins Aruba Central, it is automatically assigned to an **unprovisioned** group. The administrators can perform any of the following actions: ■ Create a new group for the device and preserve device configuration. ■ Move the device to an existing group and override the device configuration.

To manually assign Instant AP(s) to a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. To view a list of unassigned devices, click **Unassigned Devices**.
   A list of unassigned devices is displayed in the devices table.
4. Select the group to which you want to assign the devices.
5. From the devices table on the right, select Instant AP(s) to assign.
6. Drag and drop the Instant APs to the group that you selected.

Assigning Switches to Groups

Aruba Central allows switches to join groups only if the switches are running factory default configuration. Switches with factory default configuration are automatically assigned to the **default** group. Administrators can either move the switch to an existing group or create a new group.

Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central.

To manually assign switch(s) to a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. To view a list of unassigned devices, click **Unassigned Devices**. A list of unassigned devices is displayed in the devices table.
4. Select the group to which you want to assign the devices.
5. From the devices table on the right, select the switch(s) to assign.
6. Drag and drop the switches to the group that you selected.

Moving Instant Access Point(s) Between Groups

In Aruba Central, an Instant AP device group may consist of any of the following:

- Instant AP—Consist a commander Instant AP.
- Virtual Controller (VC)—VC provides an interface for entire cluster. The member Instant APs and commander Instant APs function together to provide a virtual interface.

In typical Instant AP deployment scenario, the first Instant AP that comes up is elected as the commander Instant AP. All other Instant AP(s) joining the cluster function as the member Instant AP(s). When a commander Instant AP is configured, the member Instant AP(s) download the configuration changes. The commander Instant AP may change as necessary from one device to another without impacting network performance.

To move an Instant AP or VC from one group to another group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.

   By default, the **Groups** page is displayed.
3. From the groups table on the left, select the group from which you want to move the Instant APs.
4. From the devices table on the right, select the standalone IAP or VC that you want to move.

Moving a VC also moves the member IAP(s) to the new group.

5. Drag and drop the IAP to the group that you want to assign the IAP to.
6. Click **Yes** when the system prompts you to confirm device movement.

MSP mode does not support moving devices across different groups.

Important Points to Note

- The instant AP(s) inherits the configuration of the group to which it is moved. However, only the system configuration is inherited and the **Per AP Settings** on the IAP(s) are retained.
- If the instant AP(s) did not inherit the configuration of the new group, go to the **Configuration Audit** page of the IAP(s) to check the configuration difference. For more information, see Viewing Configuration Status.
- If firmware compliance is enabled on the new group and if the firmware version enforced by the group is different from the IAP(s) firmware version, the firmware is upgraded and the IAP(s) reboots.

Provisioning Devices Using UI-based Workflows

This section describes the important points to consider when assigning devices to UI groups:

- Provisioning Instant APs using UI-based Configuration Method
- Provisioning Switches Using UI-based Configuration Method
- Provisioning Aruba Gateways Using UI-based Configuration Method

Provisioning Instant APs using UI-based Configuration Method

An Instant AP device group may consist of any of the following:

- Instant AP Cluster—Consists of a conductor Instant AP and member Instant APs in the same VLAN.
- VC—A virtual controller. VC provides an interface for entire cluster. The member Instant APs and conductor Instant APs function together to provide a virtual interface.
- Conductor Instant AP and Member Instant AP—In typical Instant AP deployment scenario, the first Instant AP that comes up is elected as the conductor Instant AP. All other Instant APs joining the cluster function as the member Instant APs. When a conductor Instant AP is configured, the member Instant APs download the configuration changes. The conductor Instant AP may change as necessary from one device to another without impacting network performance.

Aruba Central allows configuration operations at the following levels for a device group with Instant APs.

- **Per group configuration**—Aruba Central allows you to maintain unique configuration settings for each group. However, these settings are applied to all devices within that group. For example, all VCs within a group can have common SSID settings.
- **Per VC Configuration**—Any changes that need to applied at the Instant AP cluster level can be configured on a VC within a group. For example, VCs within a group can have different VLAN configuration for the SSIDs.
- **Per Device Configuration**—Although devices are assigned to a group, the users can maintain device - specific configuration such as radio, power, or uplink settings for an individual AP within a group.

When the APs that are not pre-provisioned to any group join Aruba Central, they are assigned to groups based on their current configuration.

Table 60: *Instant AP Provisioning*

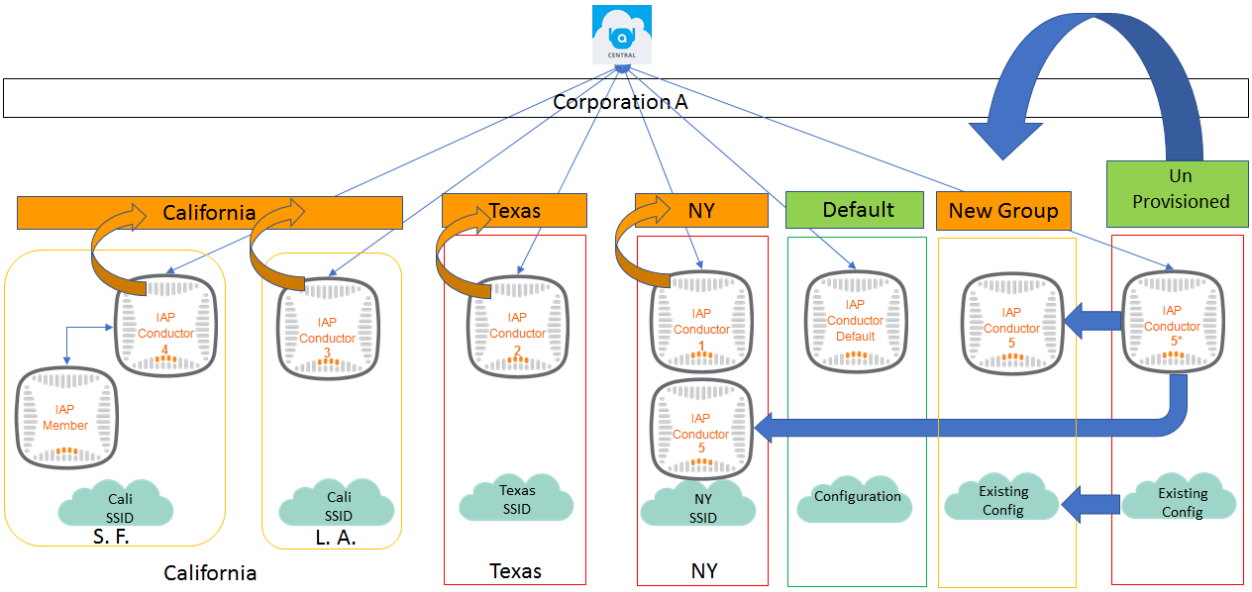
APs with Default Configuration	APs with Non-Default Configuration
If an Instant AP with factory default configuration joins Aruba Central, it is automatically assigned to the **default** group or an existing group with similar configuration settings. The administrators can perform any of the following actions: ■ Manually assign them to an existing group. ■ Create a new group.	If an Instant AP with non-default or custom configuration joins Aruba Central, it is automatically assigned to an **unprovisioned** group. The administrators can perform any of the following actions: ■ Create a new group for the device and preserve device configuration. ■ Move the device to an existing group and override the device configuration.

Ensure that the conductor Instant AP and member Instant APs are assigned to the same group. You must convert the member Instant AP to a standalone AP in order to move the member Instant AP to another group independently.

In the following illustration, Instant APs from three different geographical locations are grouped under California, Texas, and New York states. Each state has unique SSIDs and can support devices from multiple locations in a state. As shown in Figure 99, the California group has devices from different locations and has the same SSID, while devices in the other states/groups have different SSIDs.

When a device with the factory default configuration connects to Aruba Central, it is automatically assigned to the default group. If the device has custom configuration, it is marked as unprovisioned. If you want to preserve the custom configuration, create a new group for the device. If you want to overwrite the custom configuration, you can assign the device to an existing group.

Figure 99 *Instant AP Provisioning*



For more information on how to configure Instant APs using UI-based configuration workflows, see Deploying a Wireless Network Using Instant APs.

To view local overrides and configuration errors, select a template group and navigate to **Devices** > **Access Points** > **Settings** > **Configuration Audit** page.

Provisioning Switches Using UI-based Configuration Method

Aruba Central allows switches to join UI groups only if the switches are running factory default configuration. Aruba Central assigns switches with factory default configuration to the **default** group.

The administrators can either move the switch to an existing group or create a new group.

NOTE

Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central

Aruba Central allows the following configuration operations at the following levels for switches in a UI group:

- **Per group configuration**— Aruba Central allows you to maintain unique configuration settings for each group. However, these settings are applied to all devices within that group. For example, all switches within a group can have common VLAN settings.
- **Per Device Configuration**—Although the Switches inherit group configuration, the users can maintain device-specific configuration, for example, ports or DHCP pools.

For more information on how to configure switches using UI-based configuration workflows, see Configuring or Viewing AOS-Switch Properties in UI Groups.

To view local overrides and configuration errors, select a template group and navigate to **Devices** > **Switches** > **Settings** > **Configuration Audit** page.

Provisioning Aruba Gateways Using UI-based Configuration Method

For SD-Branch deployments with Aruba Gateways, the following recommendations apply:

- Combine Branch Gateways of identical characteristics and configuration requirements under a single group.
- Create groups according to your branch requirements.
  - You can create separate groups for the small, medium, and large sized branches.
  - You can also create separate groups for the branch sites in different geographical locations; for example, East Coast and West Coast branch sites. If these groups have similar characteristics with minor differences, you can create the first group and then clone it.
  - You can use either a single group for all their devices or deploy devices in multiple groups. For example, you can deploy 7008 controllers and Aruba 2930F Switch Series with 24 ports in a single group for every branch.
  - You can also deploy 7005 controller and Aruba 2930F Switch Series with 24 ports in one group and provision 7008 controller with Aruba 2930F Switch Series with 48 ports in another group.

Important Points to Note

- The groups in Aruba Central are not device-specific, however, Aruba recommends that you use the following guidelines for provisioning SD-WAN Gateways.
  - Assign Branch Gateways and VPN Concentrators to separate groups. Because the configuration requirements for Branch Gateways and VPN Concentrators are different, the Branch Gateways and VPN Concentrators must be assigned to different groups.
  - Ensure that the configuration group for SD-WAN Gateways consists of the same type of devices. For example, Branch Gateways assigned to a group must have the same number of ports.
- Before assigning SD-WAN Gateways to groups, you must set the device persona or role as Branch Gateway or VPN Concentrator.

Example

The following figures shows a few sample group deployment scenarios for Aruba Branch Gateways and VPN Concentrators:

Figure 100 *Branch Gateway Groups*

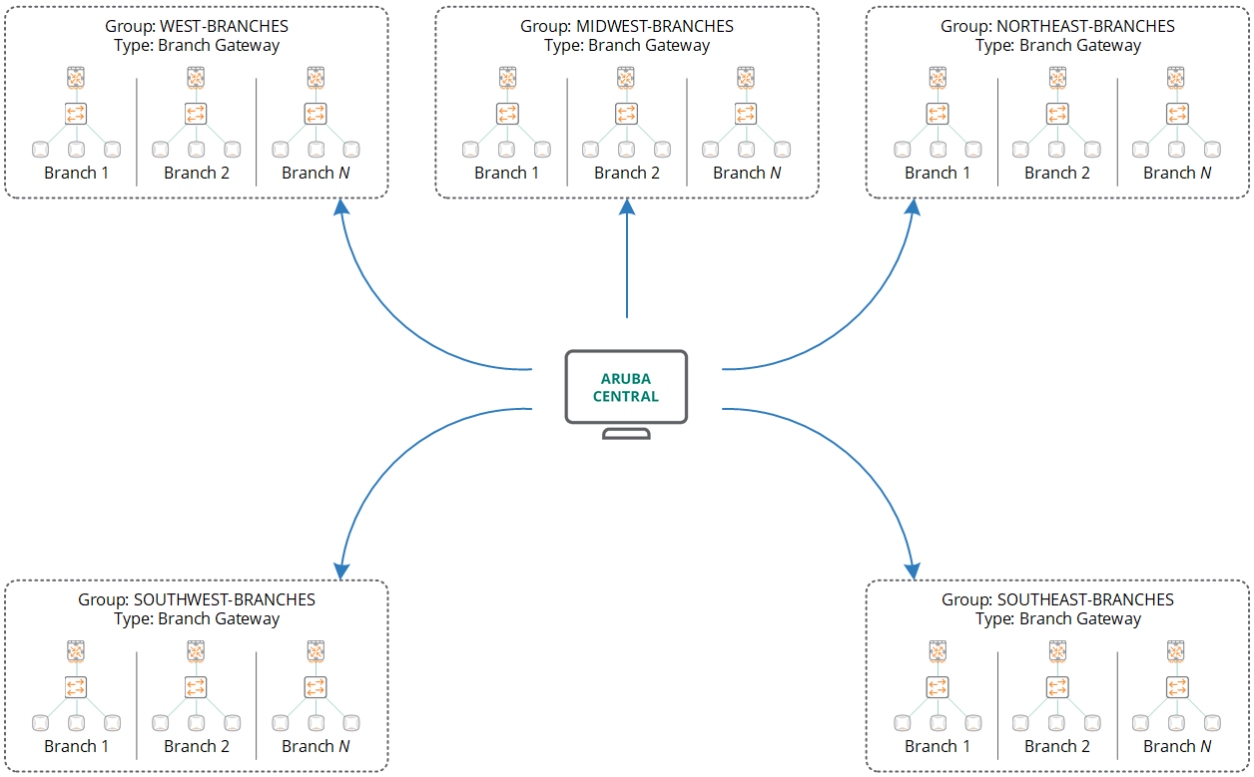
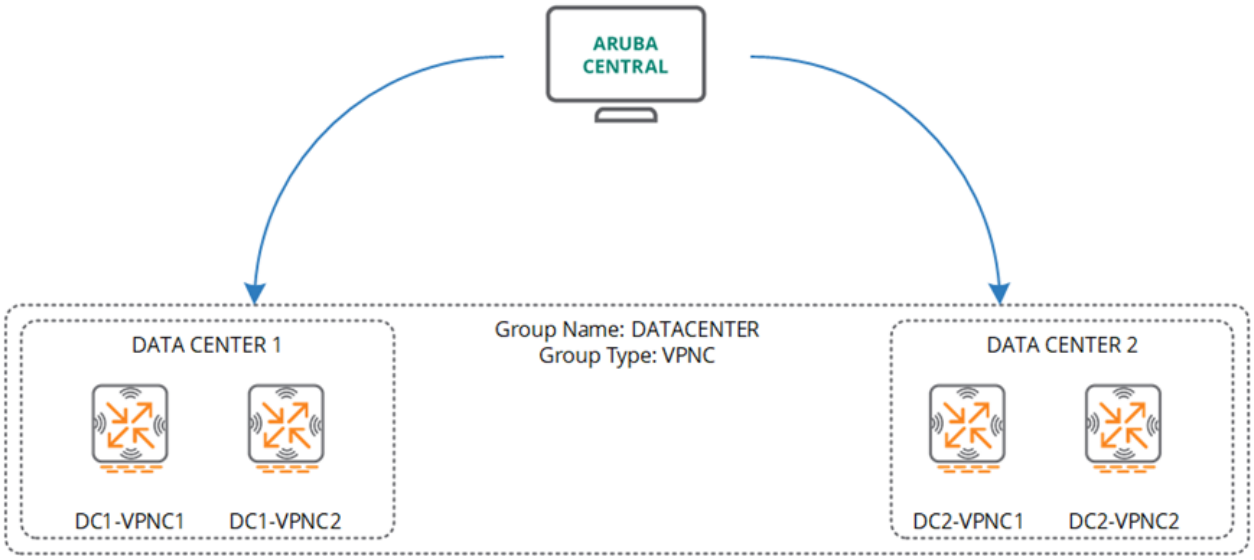


Figure 101 *VPN Concentrator Groups*



For more information on how to configure Aruba using UI-based configuration workflows, see the *SD-Branch Configuration* section in *Aruba Central Help Center*.

To view local overrides and configuration errors, select a template group and navigate to **Devices** > **Gateways** > **Settings** > **Configuration Audit** page.

Provisioning Devices Using Configuration Templates

Aruba Central allows you to provision devices using UI-based or template-based configuration method. If you have groups with template-based configuration enabled, you can create a template with a common set

of CLI scripts, configuration commands, and variables. Using templates, you can apply CLI-based configuration parameters to multiple devices in a group.

If the template-based configuration method is enabled for a group, the UI configuration wizards for the devices in that group are disabled.

Creating a Group with Template-Based Configuration Method

To create a template group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for selected filter is displayed.
2. Under **Maintain**, click **Organization**.
   By default, the **Groups** page is displayed.
3. Click **(+) New Group**.
   The **Create New Group** window is displayed.
4. Enter the name of the group.
5. Select one of the following device types for which you want to create a template group:
   - IAP and Gateway
   - Switch
6. Enter the password and confirm the password.
7. Click **Save**.

If the group is set as a template group, a configuration template is required for managing device configuration.

Provisioning Devices Using Configuration Templates and Variable Definitions

For information on configuration template, see the following topics:

- Configuring APs Using Templates
- Using Configuration Templates for AOS-Switch Management
- Managing Variable Files

Managing Variable Files

Aruba Central allows you to configure multiple devices in bulk using templates. However, in some cases, the configuration parameters may vary per device. To address this, Aruba Central identifies some customizable CLI parameters as variables and allows you to modify the definitions for these variables as per your requirements.

You can download a sample file with variables for a template group or for the devices deployed in a template group, update the variable definitions, upload the file with the customized definitions, and apply these configuration changes in bulk.

Important Points to Note

- Variables are associated to a device and not to a group. If you move a device between groups, variables remain with the device.
- Variables are displayed as part of the group to which the device belongs. After you upload the variables for a device, the association would stay in the system even if the device is moved to a UI group or template group.

- If the device is part of a UI group, variables are unused and not displayed in the UI. Aruba Central ignores the variables.
- If the device is moved to a template group, variables are displayed in the UI and used for configuration purposes.

Downloading a Sample Variables File

The sample variables file includes a set of sample variables that the users can customize. You can download the sample variables file in the JSON or CSV format.

To download a sample variables file:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
4. Click **Variables**.
5. Select one of the following formats to download the sample variables file:
   - JSON—shows the file in JSON format.
   - CSV—Shows the variables in different columns.
6. Click **Download Sample Variables File**. The sample variables file is saved to your local directory.

Modifying a Variable File

The CSV file includes the following columns for which the variable definitions are mandatory:

- **_sys_serial**—Serial number of the device.
- **_sys_lan_mac**—MAC address of the device.
- **modified**—Indicates the modification status of the device. The value for this column is set to **N** in the sample variables file. When you edit a variable definition, set the **modified** column to **Y** to allow Aruba Central to parse the modified definition.

Predefined Variables for Aruba Switches

The system defined variables in the sample variables files are indicated with **sys** prefix.

Table 61 lists the predefined variables for switches.

Table 61: *Predefined Variables Example*

Variable Name	Description	Variable Value
_sys_gateway	Populates gateway IP address.	10.22.159.1
_sys_hostname	Maintains unique host name.	HP-2920-48G-POEP
_sys_ip_address	Indicates the IP address of the device.	10.22.159.201
_sys_module_command	Populates module lines.	module 1 type j9729a
_sys_netmask	Netmask of the device.	255.255.255.0

Variable Name	Description	Variable Value
_sys_oobm_command	Represents Out of Band Management (OOBM) block.	oobm ip address dhcp-bootp exit
_sys_snmpv3_engineid	Populates engine ID.	00:00:00:0b:00:00:5c:b9:01:22:4c:00
_sys_stack_command	Represents stack block.	stacking member 1 type "J9729A" mac-address 5cb901-224c00 exit
_sys_template_header	Represents the first two lines of the configuration file. Ensure that this variable is the first line in the template.	; J9729A Configuration Editor; Created on release #WB.16.03.0003+ ; Ver #0f:3f.f3.b8.ee.34.79.3c.29.eb.9f.fc.f3.ff.37.ef:91
_sys_use_dhcp	Indicates DHCP status (true or false) of VLAN 1	0
_sys_vlan_1_untag_command	Indicates untagged ports of VLAN 1	1-28,A1-A2
_sys_vlan_1_tag_command	Indicates tagged ports of VLAN 1	28-48

The **_sys_template_header_** and **_sys_snmpv3 engineid** are mandatory variables that must have the values populated, irrespective of their use in the template. If there is no value set for these variables, Aruba Central re-imports the values for these mandatory variables when it processes the running configuration of the device.

Predefined Variables for APs

For APs, the sample variables file includes the **_sys_allowed_ap** variable for which you can specify a value to allow new APs to join the Instant AP cluster.

Conditions

The following conditions apply to the variable files:

- The variable names must be on the left side of condition and its value must be defined on the right side. For example, %if var=100% is supported and %if 100=var% is not supported.
- The < or <= or > or >= operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as %if dpi_value > 2.8%, it is converted as %if dpi_value > 2 for comparison.
- The variable names should not include white space, and the **&** and **%** special characters. The variable names must match regular expression [a-zA-Z0-9_]. If the variables values with **%** are defined, ensure that the variable is surrounded by space. For example, *wlan ssid-profile %ssid_name%*.
- The first character of the variable name must be an alphabet. Numeric values are not accepted.
- The values defined for the variable must not include spaces. If quotes are required, they must be included as part of the variable value. For example, if the intended variable name is *wlan ssid-profile*

"emp ssid", then the recommended format for the syntax is "*wlan ssid-profile %ssid_name%*" and variable as *"ssid_name": "\"emp ssid\""*.

- If the configuration text has the percentage sign **%** in it—for example, **"url "/portal/scope.cust-5001098/Splash%20Profile%201/capture"**—Aruba Central treats it as a variable when you save the template. To allow the use of percentage **%** as an escape character, use **\"** in the variable definition as shown in the following example:

  Template text

  ```
  wlan external-captive-portal
  "Splash Profile 1_#guest#_"server naw1.cloudguest.central.arubanetworks.comport
  url %url%
  ```

  Variable

  ```
  "url": "\"/portal/scope.cust-5001098/Splash%20Profile%201/capture\""
  ```

- Aruba Central supports adding multiple lines of variables in Instant AP configuration templates. If you want to add multiple lines of variables, you must add the `HAS_MULTILINE_VARIABLE` directive at the beginning of the template.

  Example

  ```
  #define HAS_MULTILINE_VARIABLE 1
  %if allowed_aps%
  %allowed_aps%
  %endif%
  ```

  Variable

  ```
  "allowed_aps": "allowed-ap 24:de:c6:cb:76:4e\n allowed-ap ac:a3:1e:c5:db:d8\n
  allowed-ap 84:d4:7e:c4:8f:2c"
  ```

For Instant APs, you can configure a variable file with a set of values defined for a master AP in the network. When the variable file is uploaded, the configuration changes are applied to all Instant AP devices in the cluster.

Examples

The following example shows the contents of a variable file in the JSON format for Instant APs:

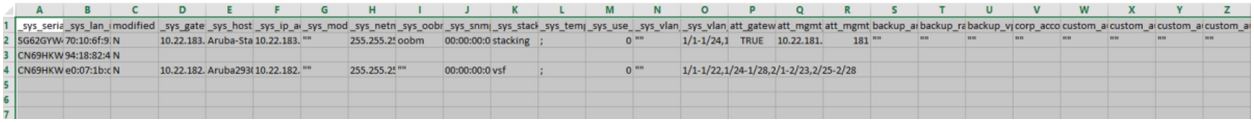
```
{
"CK0036968": {
"_sys_serial": "CK0036968",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:7a",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
```

```
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_1"
},
"CJ0219729": {
"_sys_serial": "CJ0219729",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:cb:04:92",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_2"
},
"CK0112486": {
"_sys_serial": "CK0112486",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c8:29:76",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_3"
},
"CT0779001": {
"_sys_serial": "CT0779001",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c5:c6:b0",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_4"
},
"CM0640401": {
"_sys_serial": "CM0640401",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c4:8f:2c",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_6"
},
"CK0037015": {
"_sys_serial": "CK0037015",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:d8",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
```

```
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_7"
},
"CK0324517": {
"_sys_serial": "CK0324517",
"ssid": "s1",
"_sys_lan_mac": "f0:5c:19:c0:71:24",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_8"
}
}
```


Figure 102 shows a sample variables file in the CSV format:

Figure 102 *Variables File in the CSV Format*



Uploading a Variable File

To upload a variable file, complete the following steps:

NOTE

While uploading the variables file to Aruba Central in the CSV format, make sure to choose the default language in Microsoft Excel as **English (United States)**.

1. Ensure that the **_sys_serial** and **_sys_lan_mac** variables are defined with the serial number and MAC address of the devices, respectively.
2. In the **Network Operations** app, set the filter to one of the template groups under **Groups**.
3. Under **Manage**, click **Devices** > **Switches**.
4. Click the **Config** icon.
5. Click **Variables**.
6. Click **Upload Variables File** and select the variable file to upload.
7. Click **Open**. The contents of the variable file is displayed in the **Variables** table.
8. To search for a variable, specify a search term and click **Search** icon.
9. To download variable file with device-specific definitions, click the download icon in the **Variables** table.

Modifying Variables

To modify variables without downloading a variable file, modifying the variable file, and uploading the customized variable file:

1. In the **Network Operations** app, set the filter to one of the template groups under **Groups**.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
4. Click **Variables**.
5. Select a device and variable.
6. Modify the value and click **Add to Modifications**.
7. Click **Save**.

Alternatively, to modify a single variable without downloading a variable file, modifying the variable file, and uploading the customized variable file:

1. In the **Network Operations** app, set the filter to one of the template groups under **Groups**.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
4. Hover over a desired variable and click **Edit**.
5. Modify the value and click **Save**.
6. Click **Save**.

Backing Up and Restoring Configuration Templates

Aruba Central allows you to create a backup of configuration templates and variables that you can restore in the event of a failure or loss of data. The **Configuration Backup and Restore** feature is available in the **Configuration Audit** page for devices deployed using the template-based configuration method.

The **Configuration Backup and Restore** feature enables administrators to perform the following functions:

- Back up templates and variable files applied to the devices, managed using the template-based configuration method.
- Restore an earlier known working combination of the configuration template and device variables in the event of a failure.

Important Points to Note

- The backup and restoration options are available for devices deployed using the template-based configuration method.
- When the backup or restore for a group is in progress, you cannot make configuration changes to that group.
- The restore operation restores the variables only for the devices that are currently provisioned or pre-provisioned to the group.
- The restore operation is terminated if the firmware version running on any one device in the group does not match the firmware version in the backed up file that is being restored. For example, if the configuration file was backed up when a switch was running 16.03.0003 and was later upgraded to 16.04.0003, the restore operation fails for the group.
- The restore operation deletes any templates applied to the group before the restore. It also deletes and replaces device variables with the backed up version that is being restored.
- The details pertaining to the actions carried out during the backup and restore operations are logged in the **Audit Trail** page.

Creating a Configuration Backup

To back up configuration templates and variables applied to devices:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**.
2. Navigate to the **Configuration Audit** page. See Viewing Configuration Status.
3. Under **Configuration Backup and Restore**, click **New Configuration Backup**.

   The **Create New Backup** window is displayed.
4. Enter a **Backup Name**.
5. Select **Do Not Delete** if you do not want the backed up file to be deleted by a new backup after the threshold of 20 backups is exceeded.

NOTE

You can create and maintain up to 20 backed up configuration files. If the number of backup files exceed 20, the old backed up configuration files are overwritten. However, if the backed up files are marked as **Do not Delete**, Aruba Central does not overwrite the backed up configuration files.

6. Click **OK**. The **Confirm Backup** window is displayed.
7. Read through the information. Select the check box to confirm that configuration changes to the group cannot be done when the backup is in progress.
8. Click **Proceed**.

   The backup for the group configuration is created.

Viewing Contents of a Backed Up Configuration

To view the contents of a backed up configuration:

1. Click the **Manage Backup** option.
2. Download the backup and `untar` the downloaded file. The following example shows the tree structure of a typical backup download.

```
<backup-name_timestamp>
├── templates
│   ├──<hppctemplate1.tmpl>
│   ├──<iaptemplate1.tmpl>
│   ├──template_meta.json
└── variables
    ├──HPPC_variables_1.json
    ├──IAP_variables_1.json
    └──devices_meta.json
```

NOTE

The variables are stored according the device type, such as, Instant APs and Aruba Switches. For example, for all Instant APs, the variables are aggregated and stored together.
The aggregated file can include variables for up to 80 devices or up to 5 MB of variables data, based on whichever condition is met first. When the number of variables or the data size exceeds this limit, new aggregate files are created and added to the backup until all the variables in the selected group are backed up. The variable data limit applies only to the aggregated files. Aruba Central does not impose any limit on the number of devices or the device variables that can be backed up.

The following details are available for a backed up configuration snapshot:

- **Backups**—Provides details of the number of available and allowed backup and allows you to perform the following actions:
  - Manage group configuration backups
  - Create new configuration backups
  - Modify backup delete protection
- **Last Backup**—Provides details of the status and the timestamp of the last backup.
- **Last Restore**—Provides details of the status and the timestamp of the last restore.

Restoring a Backed Up Configuration

To restore a backed up configuration snapshot:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See Viewing Configuration Status.
3. Under **Configuration Backup and Restore**, click **Restore Configuration Backup**.

   The **Restore from Backup** window is displayed.
4. Select the backup name that you want to restore, from the **Backup Name** drop-down list.
5. Select the required device type from the **Device Type** drop-down list.

Selecting a device type allows you to restore the backed up configuration by the specific device type, for example, Instant APs, Aruba Switch. By default, **All** is selected. When the device type is set to **All**, configuration restore does not follow any specific order.

6. Click **OK**. The **Confirm Configuration Restore** window is displayed.
7. Read the instructions and select the check boxes to confirm your action for configuration restore.
8. Click **Proceed.**

   The selected backup configuration is restored.

Aruba recommends that the administrators take a backup of the current configuration of the group before the restore operation.

Managing Backups

To manage the backed up configuration files:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See Viewing Configuration Status.
3. Under **Configuration Backup and Restore**, click **Manage Backup**.

   The **Last <#> Backups** window is displayed.
4. View the backup details such as date and time of backup, backup name, username, and the delete protection status for each configuration backup.
5. Click **Close**.
6. Click **Last Backup Log** to view the details of the latest backup. The **Last Backup Log** window displays the following details:

- Group name
- Backup name
- Username that initiated the configuration backup
- Details on whether templates and device variables are being saved, and completion of the configuration backup process.

7. To get the status of the last restore, click **Last Restore Log**. To get the error log for a restore error event, click **Last Restore Error Log**.

Backing Up and Restoring Templates and Variables Using APIs

Aruba Central supports the following NB APIs for the backup and restore feature:

- Create new configuration backup for group
  [POST] /configuration/v1/groups/snapshot/{group}
- Create backups for multiple groups associated with a customer account
  [POST]/configuration/v1/groups/snapshot/create_backups

Aruba Central creates a backup of configuration template and variables only for the groups included in the API request payload. You can use the include or exclude parameters to create backups for specific list of groups.

The following table describes the API response based on the inputs provided in the parameters:

Table 62: *API Functionality for Backup Creation*

include_groups	exclude_groups	API Functionality
No groups specified	No groups specified	Raises an exception to either include or exclude groups.
group names	group names	Raises an exception to include or exclude groups.
[]	No groups specified	Raises an exception to provide valid values for the include groups parameter.
group names	No groups specified	Includes selected groups for the backup operation.
No groups specified	ALL_GROUPS	Creates a backup for all groups.
No groups specified	group names	Does not create backup for the excluded groups.

- Restore a backed up version of the configuration template for all devices in a group:
  [POST] /configuration/v1/groups/<group_name>/snapshots/<snapshot_name>/restore
  The API restores a specific version of the backup snapshot for the group specified in the API request.
- Restore a backed up version of the configuration template by device type:
  The **[POST]/configuration/v1/groups/{group}/snapshots/{snapshot}/restore** API provides you an option to restore the configuration by device type. By selecting a specific device type, you can control the order in which the configuration is restored by device type. This minimizes the impact of the configuration restore activity on the network.

If monitor mode is enabled at the device level, the selected device functions in the monitor mode. If the monitor mode is enabled at the group level, all devices in the group inherit this setting.
If a device managed by Aruba Central displays a **configuration sync issue** and persistently fails to receive configuration updates from Aruba Central, contact Aruba Central Technical Support.

Sites and Labels

Sites

A site in refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you could create a site called CampusA. You can also tag the devices within CampusA using labels. For example, if the campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**. If the devices in a specific location or an area within a specific location must have similar configuration, the devices can be grouped together.

For more information, see Managing Sites.

Labels

Labels are tags attached to a device provisioned in the network. Labels determine the ownership, departments, and functions of the devices. You can use labels for creating a logical set of devices and use these labels as filters when monitoring devices and generating reports.

For example, consider an Instant AP labeled as **Building 25** and **Lobby**. These tags identify the location of the Instant AP within the enterprise campus or a building. The Instant APs in other buildings within the same campus can also be tagged as **Lobby**. To filter and monitor Instant APs in the lobbies of all the campus buildings, you can tag all the Instant APs in a lobby with the label **Lobby**.

For more information, see Managing Labels.

Device Classification

Devices can also be classified using **Groups** and **Sites**.

- The group classification can be used for role-based access to a device, while labels can be used for tagging a device to a location or a specific area at a physical site. However, if a device is already assigned to a group and has a label associated with it, it is classified based on both groups and labels.
- The site classification is used for logically grouping devices deployed at a given physical location. You can also convert labels to sites.

Managing Sites

The **Sites** page allows you to create sites, view the list of sites configured in your setup, and assign devices to sites. The **Sites** page includes the following functions:

Table 63: *Sites Page*

Name	Contents of the Table
Convert Labels to Sites	Allows you to convert existing labels to sites. To convert labels, download the CSV file with the list of labels configured in your setup, add the site information, and upload the CSV file. For more information, see Creating a Site.

Name	Contents of the Table
Sites table	Displays a list of sites configured. It provides the following information: ▪ **Site Name**—Name of the site. ▪ **Address**—Physical address of the site. ▪ **Device Count**—Number of devices assigned to a site. The table also includes the following sorting options to reset the table view on the right: ▪ **All Devices**—Displays all the devices provisioned in Aruba Central. ▪ **Unassigned**—Displays the list of devices that are not assigned to any site. You can also use the filter and sort icons on the **Sites** and **Address** columns to filter and sort sites respectively.
New Site	Allows you to create a new site.
Bulk upload	Allows you to add sites in bulk from a CSV file.
Devices table	Displays a list of devices provisioned. It provides the following information: ▪ **Name**—Name of the device ▪ **Group**—Group to which the device is assigned. ▪ **Type**—Type of the device.

Creating a Site

To create a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. To add a new site, click **(+) New Site**. The **Create New Site** pop-up window opens.
6. In the **Create New Site** pop-up window, enter the following details:
   a. **Site Name**—Name of the site. The site name can be a maximum of 255 single byte characters. Special characters are allowed.
   b. **Street Address**—Address of the site.
   c. **City**—City in which the site is located.
   d. **Country**—Country in which the site is located.
   e. **State/Province**—State or province in which the site is located.
   f. **ZIP/Postal Code**—(Optional) ZIP or postal code of the site.
7. Click **Add**. The new site is added to the **Sites** table.

Adding Multiple Sites in Bulk

To import site information from a CSV file in bulk, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Click **(+) Bulk upload**. The **Bulk Upload** pop-up opens.
6. Download a sample file.

7. Fill the site information and save the CSV file in your local directory.

The CSV file for bulk upload of sites must include the mandatory information such as the name, address, city, state, and country details.

8. In the Aruba Central UI, click **Browse** and add the file from your local directory.
9. Click **Upload**. The sites from the CSV file are added to the site table.

Assigning a Device to a Site

To assign devices to a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Select **Unassigned**. The list of devices that are not assigned to any site is displayed.
6. Select device(s) from the list of devices.

It is recommended not to add more than 20 devices at a time for seamless operation.

7. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
8. Click **Yes**.

Converting Existing Labels to Sites

To convert existing labels to sites, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Click **Convert Labels to Sites**. The **Confirm Conversion** pop-up window opens.
6. To download a CSV file with the list of labels configured in your setup, click **Download a File**. A CSV file with a list of all the labels in your setup is downloaded to your local directory.
7. Enter address, city, state, country, and ZIP code details for the labels that you want to convert to sites.

In the CSV file, you must enter the following details: address, city, state, and country.

8. Save the CSV file.
9. On the **Confirm Conversion** pop-up window, click **Browse** and select the CSV file with the list of labels to convert.
10. Click **Upload**.
11. Click **Convert**. The labels are converted to sites.

Points to Note

- If the conversion process fails for some labels, Aruba Central generates and opens an Excel file showing a list of labels that could not be converted to sites. Verify the reason for the errors, update the CSV file, and re-upload the file.
- Aruba Central does not allow conversion of sites to labels. If the existing labels are converted to sites, you cannot revert these sites to labels.
- When the existing labels are converted to sites, Aruba Central retains only the historical data for these labels. Aruba Central displays the historical data for these labels only in reports and on the monitoring dashboard.

Editing a Site

To modify site details, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Select the site to edit and click the edit icon.
6. Modify the site information and click **Update**.

Deleting a Site

To delete a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Select the site to delete and click the delete icon.
6. Confirm deletion.

Managing Labels

The **Labels** page allows you to create labels, view a list of labels, and assign devices to labels. The page includes two tables. The table on the left lists the labels, whereas the table on the right lists the devices. These tables provide the following information:

Table 64: *Labels*

Name	Contents of the Table
Labels	Displays a list of labels configured. The table provides the following information: ■ Name of the label ■ Number of devices assigned to a label The table also includes the following sorting options to reset the table view on the right: ■ **All Devices**—Displays all the devices provisioned in Aruba Central. ■ **Unassigned**—Displays the list of devices that are not assigned to any label.
Devices	Displays a list of devices provisioned. The table provides the following information about the devices:

Name	Contents of the Table
	▪ **Name**—Name of the device ▪ **Group**—Group to which the device is assigned ▪ **Type**—Type of the device ▪ **Labels**—Number of labels assigned to a device

Creating a Label

To create a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. To add a new label, click **(+) Add Label**. The **Create New Label** pop-up window opens.
6. Enter a name for the label. The label name can be a maximum of 255 single byte characters. Special characters are allowed.
7. Click **Add**. The new label is added to the **All Labels** table.

Assigning a Label to a Device

To assign a label to a device, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Locate the label to which you want to assign a device.
6. In the table that lists the labels, you can perform one of the following actions:
   - Click **All Devices** to view all devices.
   - Click **Unassigned** to view all the devices that are not assigned to any labels.
7. Select **Unassigned**. The list of devices that are not assigned to any label is displayed.
8. Select device(s) from the list of devices.

It is recommended not to add more than 20 devices at a time for seamless operation.

9. Drag and drop the selected device(s) to a specific label. A pop-up window asking you to confirm the label assignment opens.
10. Click **Yes**.

Aruba Central allows you to assign up to five label tags per device.

Detaching a Device from a Label

To remove a label assigned to a device, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Select the device from the table on the right.
6. Click the delete icon.
7. To detach labels from the multiple devices at once, select the devices, and click **Batch Remove Labels**.
8. Confirm deletion.

Editing a Label

To edit a label, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Select the label to edit.
6. Click the edit icon.
7. Edit the label and click **Update**.

Deleting a Label

To delete one or several labels, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Select the label to delete.
6. Click the delete icon.
7. Confirm deletion.

Certificates

By default, Aruba Central includes a self-signed certificate that is available on the **Certificates** page. The default certificate is not signed by a root certificate authority (CA). For devices to validate and authorize Aruba Central, administrators must upload a valid certificate signed by a root CA.

Aruba devices use digital certificates for authenticating a client's access to user-centric network services. Most devices such as controllers and Instant APs include a server certificate by default for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Aruba Central-managed devices such as Instant AP and switches support the following root CA certificates:

Instant APs	Switches
▪ AddTrust ▪ GeoTrust ▪ VeriSign ▪ Go Daddy	▪ Comodo ▪ GeoTrust

Uploading Certificates

To upload certificates, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Select the **Certificates** tab.

   The **Certificates** page opens.
4. Click the plus icon to add the certificate to the certificate store.
5. In the **Add Certificate** dialog box, do the following:
   a. In the **Name** text box, specify the certificate name.
   b. Select the type of certificate. You can select any one of the following certificates:
      - **CA** —Digital certificates issued by the CA.
      - **Server**—Server certificates required for communication between devices and authentication servers.
      - **CRL**—Certificate Revocation List that contains the serial numbers of certificates that have been revoked. This certificate is required for performing a certificate revocation check.
      - **OCSP Responder Cert**—OCSP responder certificates.
      - **OCSP Signer Cert**—OCSP Response Signing Certificate.

        OCSP certificates are required for OCSP server authentication.
   c. From the **Format** drop-down list, select a certificate format; for example, PEM, DER, and PKCS12.
   d. In the **Passphrase** text box, enter a passphrase.
   e. In the **Retype Passphrase** text box, retype the passphrase for confirmation.

The **Passphrase** and **Retype Passphrase** text boxes are displayed only when you select **Server Certificate** from the **Type** drop-down list.

   f. In the **Certificate File** field, click **Browse** and select the certificate files.
   g. Click **Add**. The certificate is added to the Certificate Store.

Managing Certificates on Instant APs Configured Using Templates

Aruba Central supports uploading multiple certificates to Instant APs configured using templates. You can manage certificates either from the Aruba Central UI or through the API Gateway. For more information about APIs, see *API Documentation*.

To push certificates to Instant APs configured using templates:

1. Upload certificate(s) through one of the following methods:
   - **UI**—See Uploading Certificates.
   - **API**—Use the **[POST] /configuration/v1/certificates** API.

2. Get the certificate name and MD5 checksum through one of the following methods:
   - **UI**—In the **Network Operations** app, filter **All Devices**. Under **Maintain**, click **Organization** and select the **Certificates** tab. The **Certificate Store** table displays these details.
   - **API**—Use the **[GET] /configuration/v1/certificates** API.
3. In the template, anywhere before the **per-ap settings** block, depending on your requirement, add one or more of the following commands:

```
ca-cert-checksum <ca_cert_checksum/ca_cert_name>
cp-cert-checksum <captive_portal_cert_checksum/captive_portal_cert_name>
radsec-ca-checksum <radsed_ca_checksum/radsed_ca_name>
radsec-cert-checksum <radsed_cert_checksum/radsed_cert_name>
server-cert-checksum <server_cert_checksum/server_cert_name>
```

You can either use the certificate name or the checksum value in the command. Or, you can set it as a variable and enter the variable value for the Instant AP. Aruba recommends using the certificate name.

Example 1

```
ca-cert-checksum my_default_cert
```

Example 2

```
ca-cert-checksum %ca_cert_name%
variable:
{
 "ca_cert_name": "my_default_cert"
}
```

Installation Management

Site installations and device deployments at customer premises require extensive coordination between the IT administrators and installation personnel. If there are multiple sites to deploy, businesses may require more time and manual effort to coordinate and manage site installations. The Aruba Installation Management service simplifies and automates site deployments, and helps IT administrators manage site installations with ease.

The Installation Management service includes the following components:

- Install Manager on Aruba Central portal—Intended for IT administrators who oversee the installation management activities in an organization. Using Install Manager, network administrators can create installer profiles, assign site deployments to installers, and monitor deployment status for each site from a remote location. Aruba Central users can access the Install Manager application from the app selection pane in the UI.
- Aruba Installer mobile app—Intended for the installation personnel who deploy devices on a site. The Aruba Installer mobile app allows the installers to scan devices and add them to the provisioning network. The Aruba Installer mobile app is available for downloads on Apple® App Store and Google Play Store.

Installation Management and Monitoring

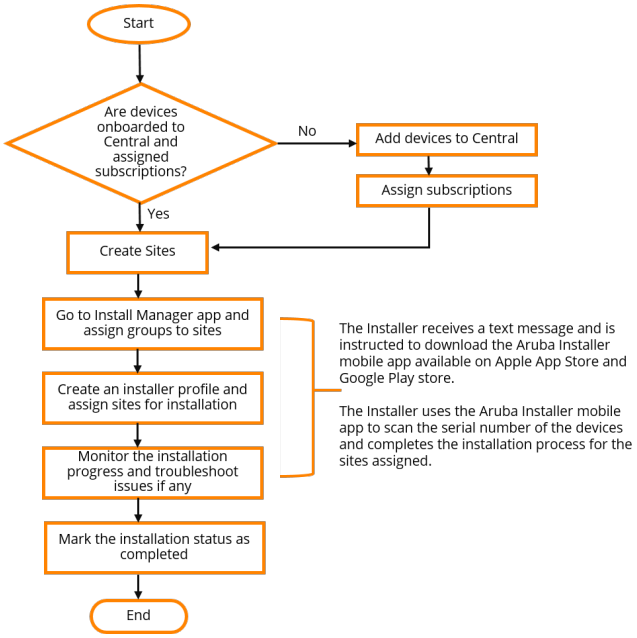
The Install Manager feature in Aruba Central includes the following menu options:

- **Site Installations** —Displays a list of sites associated with an Aruba Central account.
- **Installers**—Displays a list of installers added using the Install Manager application.

Installation Management Workflow

The following figure illustrates the installation management workflow for the Install Manager users:

Figure 103 *Installation Management Workflow*

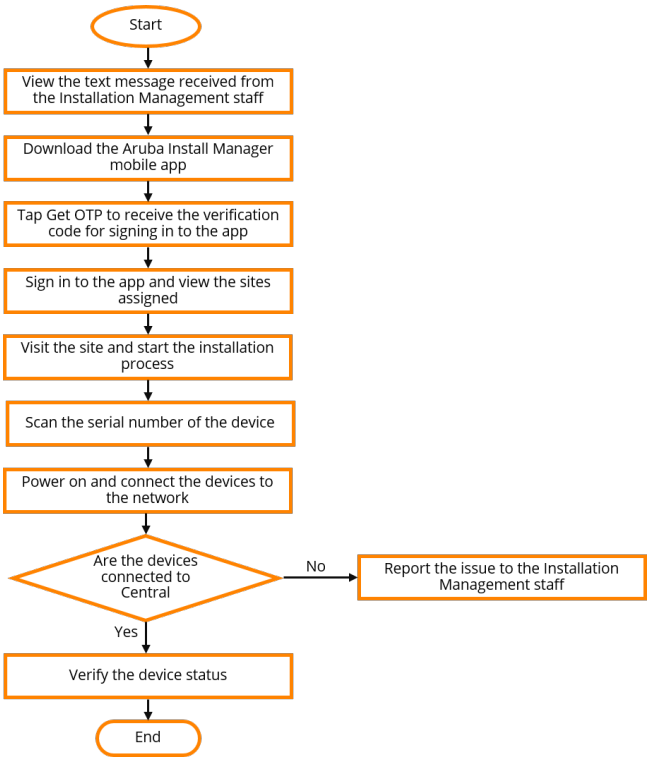


Installer Workflow

Installers are technicians who are assigned the task of visiting a physical site or location, and install devices. The Aruba Installer mobile app enables installers to scan devices and report the task status to IT administrators.

The following figure illustrates the installation workflow for the Aruba Installer mobile app users:

Figure 104 *Installer Workflow*



Managing Site Deployments

Before you begin, ensure that the following tasks are completed:

- Onboarding Devices
- Managing License Assignments

The steps required for completing a site installation procedure are listed in the following table:

Table 65: *Installation Management*

Administrator Workflow	Installer Workflow
■ Creating a Site ■ Assigning Groups to a Site ■ Adding an Installer and Assigning Sites for Installation ■ Monitoring and Troubleshooting Installation Issues	■ Downloading the Installer Mobile App ■ Registering as an Aruba Installer ■ Installing Devices on a Site

Creating a Site

To create a site in Aruba Central, complete the steps described in Creating a Site.

Assigning Groups to a Site

To assign groups to a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Install Manager** tab.
4. On the **Site Installations** page, click on the site you want to edit.
5. Select the group for each device category.
6. Click **Save**.

To assign groups to multiple sites, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Install Manager** tab.
4. On the **Site Installations** page, select the sites. The **Assign Groups** button is displayed.
5. Click **Assign Groups**.
6. In the **Assign Groups to Sites** pop-up window, select a group for each device category.
7. Click **Save**.

You can also add installation notes for sites. The installers can view the notes by clicking the info icon in the Installer mobile app.

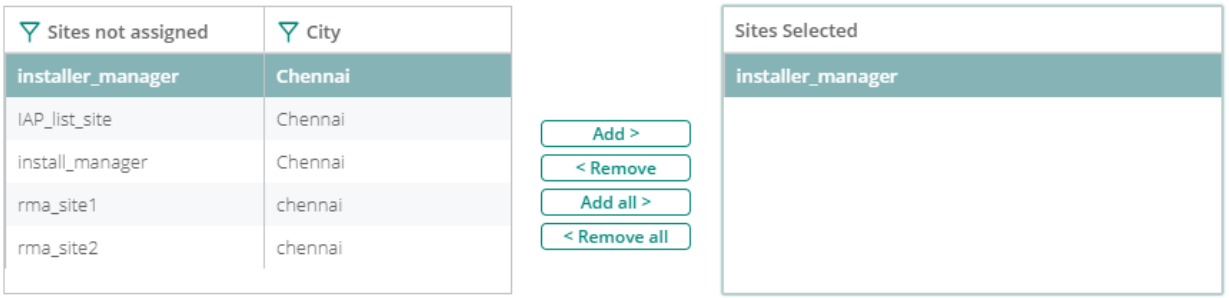
Adding an Installer and Assigning Sites for Installation

Administrators can add installers and assign installation tasks to these installers through the Aruba Installer mobile app.

To add an installer profile in Aruba Central, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Click the **Install Manager** tab.
4. In the **Install Manager** tab, click **Installers**. The **Installers** page is displayed.
5. Click **+ Add Installer**. The **Add Installer** page is displayed.
6. Enter the name and phone number of the technician to whom you want to assign a site for installing the devices.
7. Specify the time until which the installer's profile is valid. The technicians will be automatically logged out of the Aruba Installer app on the specified date.
8. On the **Add Installer** page, you can do the following:
   - Select a site in the **Sites not assigned** table and click **Add >** to add the site.
   - Select a site in the **Sites Selected** table and click **< Remove** to remove the site.
   - Click **Add all >** to add all the sites.
   - Click **< Remove all** to remove all sites.

Figure 105 *Assigning Sites*



9. Click **Save**. An SMS notification is sent to the installer's mobile device.
   The site(s) assigned are displayed in the **Sites Assigned** table.

To start the installation, the installer must download the Aruba Installer mobile app and sign up as an installer. The administrators can verify the installer registration status on the **Installers** dashboard in the Install Manager application in Aruba Central. The **Installers** dashboard displays the following status indicators for installers.

- **Invited**—The installer is added and an SMS notification is sent to the installer.
- **Registered**—The installer has registered using the Aruba Installer mobile app.
- **Verified**—The installer has accepted the installation invite and successfully completed the registration with the Aruba Installer app.

Downloading the Installer Mobile App

When an installer is added in the Install Manager application in Aruba Central, an SMS notification is sent to the installer's mobile device. The SMS notification includes the links for downloading the Aruba Installer mobile app.

If you are an installer and have received the SMS notification with the Aruba Installer mobile app details, download the Aruba Installer mobile app. The Aruba Installer mobile app is available in App Store for iOS devices and Google Play Store for Android devices.

Registering as an Aruba Installer

To register as an installer, complete the following steps:

1. Open the Aruba Installer app.
2. In the **Sign Up** tab, enter your first name, last name, country code and mobile number.
3. Click **Register**. A verification code is sent to your mobile device.
4. Enter the verification code received through the text message in the **Code** field.
5. Click **Validate Code**. If the code is valid, the installer is registered.

Installing Devices on a Site

To install a device on a site, complete the following steps:

1. Sign in to Aruba Installer mobile app.
2. View the sites assigned for deployment.
3. Select the site that you want to deploy.

4. Note the devices assigned for the site and installation notes if any.
5. Click **Scan Device**. Scan the serial number of the device. The Aruba Installer app verifies if the device is onboarded to Aruba Central device inventory and is assigned a valid subscription.
6. Power on the device and connect it to the Internet. The device automatically connects to Aruba Central and is provisioned in the group to which it is already assigned.
7. Verify the installation status and report errors if any.

Before scanning a device, ensure that the device is not connected to Aruba Central. If the device is already connected to Aruba Central, Install Manager will not assign it to a group.

Monitoring and Troubleshooting Installation Issues

To monitor the installation progress, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Select the **Install Manager** tab. The **Site Installations** table is displayed.
4. To view the status of a site installation, check the **Status** column:
   - **In Progress**—Indicates that the device installation is in progress.
   - **Completed**—Indicates that the device installation is completed.

   If the installation status displays an error:
   - Check if the devices are onboarded to Aruba Central.
   - Verify if the devices are assigned a valid subscription.
   - Check if the sites are assigned to a group.
   - View the audit trails.
5. If the installation is completed, click the site name to navigate to the site details page and click **Mark Completed**.

You can mark a site as completed even if **Install Manager** was not used to install or onboard the device.

6. Click **Save**.

Viewing Configuration Status

Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The **Configuration Audit** page is available for Instant APs, switches, and gateways.

The Configuration Audit page and the Auto Commit feature is available for Foundation and Advanced licenses for APs, switches, and gateways.

Viewing the Configuration Audit Page

To view the **Configuration Audit** page, complete the following steps:

- For Instant APs:
  a. In the **Network Operations** app, set the filter to a group that contains at least one AP.
     The dashboard context for the selected group is displayed.
  b. Under **Manage**, click **Devices** > **Access Points**.
  c. Click the **Config** icon.
     The tabs to configure access points are displayed.
  d. Click **Show Advanced**, and click the **Configuration Audit** tab.
     The **Configuration Audit** details page is displayed.
- For Aruba switches:
  a. In the **Network Operations** app, set the filter to a group that contains at least one switch.
     The dashboard context for the selected group is displayed.
  b. Under **Manage**, click **Devices** > **Switches**.
  c. Click the **Config** icon.
     The tabs to configure switches are displayed.
  d. Click **Configuration Audit**.
     The **Configuration Audit** details page is displayed.
- For Aruba gateways:
  a. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
     The dashboard context for the selected group is displayed.
  b. Under **Manage**, click **Devices** > **Gateways**.
  c. Click the **Config** icon.
     The tabs to configure gateways are displayed.
  d. Click **Show Advanced**, and click the **Configuration Audit** tab.
     The Configuration Audit details page is displayed.

Applying Configuration Changes

Aruba Central supports a two-staged configuration commit workflow for Instant APs and switches. Aruba Central now supports the auto commit feature at a group level. When auto commit state is enabled for a group, the configuration changes are instantly applied to all devices where auto commit state is enabled.

In the **Configuration Audit** page of the group, the **Auto Commit State** section allows administrators to switch their preference for committing configuration changes to the devices within the group.

- To enable auto commit, click **Change to Auto commit state ON**. When auto commit state is enabled for a group, the configuration changes are instantly applied to all devices where auto commit state is enabled.
- To disable auto commit, click **Change to Auto commit state OFF**. When auto commit state is disabled for a group, an administrator can build a candidate configuration, save it on cloud, review it, and then commit the configuration changes to all devices within the group.

Aruba Central resets the auto commit state, when a device moves to another group. The device inherits the auto commit state of the group to which the device is moved.

When auto commit state is disabled for a group, Aruba Central restricts modification to the auto commit state at a device level. When auto commit state is enabled for a group, Aruba Central allows modification to the auto commit state at a device level.

The auto commit at a group level is not applicable for Aruba MAS switches and Aruba gateways in the **Configuration Audit** page. Auto commit state is always enabled for Aruba MAS switches and Aruba gateways.

Viewing and Editing

To modify the auto commit state of devices within the group, when **Auto Commit State** for a group is enabled, complete the following steps:

1. Click **View & Edit** under **Auto Commit State: ON** tile.
2. Select a device name, click **Disable Auto Commit**, and then click **OK**.
3. Click **Yes** in the **Confirm Action** dialog box.

To modify the auto commit state of devices within the group, when **Auto Commit State** for a group is disabled, complete the following steps:

1. Click **View & Edit** under **Auto Commit State: OFF** tile.
2. Select a device name, click **Enable Auto Commit**, and then click **OK**.
3. Click **Yes** in the **Confirm Action** dialog box.

When auto commit state for a group is disabled, the **View & Edit** link is disabled to restrict modifications to the auto commit state of the devices within the group. When auto commit state for a group is enabled, the **View & Edit** link allows you to modify the auto commit state of the devices within the group.

Auto Commit Workflow

To enable Aruba Central to commit configuration changes instantly, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP and a switch.
   The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

In Aruba Central, the auto commit workflow for a group can be implemented either from the switch configuration audit page or Instant AP configuration audit page. Alternatively, you can navigate to **Devices** > **Switches**.

3. Click the **Config** icon.
   The tabs to configure access points are displayed.
4. Click **Show Advanced**, and click the **Configuration Audit** tab.
   The **Configuration Audit** details page is displayed.
5. Ensure that the **Auto Commit State** for the group is set to **ON**.

6. Based on configuration mode set for the devices in the group, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. Aruba Central automatically commits the configuration changes to all devices where auto commit state is enabled.
7. View the **Local Overrides and Configuration Sync Issues**, if any.

NOTE

Aruba Central does not support the two-staged configuration commit workflow for Aruba MAS switches and Aruba gateways.
The tenant accounts in the MSP deployments do not inherit the **Auto Commit State** configured at the MSP level. The tenant account users can enable or disable **Auto Commit** state for the devices in their respective accounts.

Manual Commit Workflow

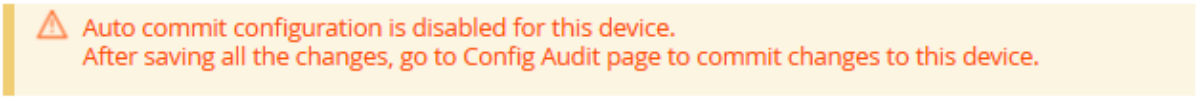
To build configuration and review it before committing the configuration changes, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP and a switch.
   The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

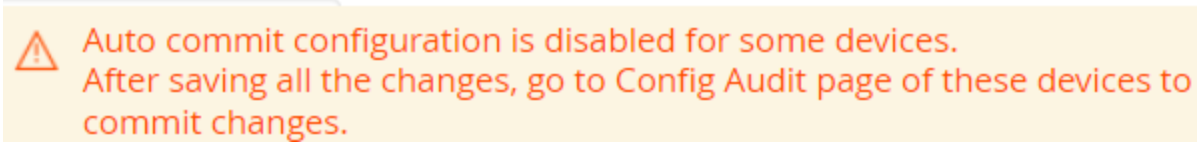
NOTE

In Aruba Central, the manual commit workflow for a group can be implemented either from the switch configuration audit page or Instant AP configuration audit page. Alternatively, you can navigate to **Devices** > **Switches**.

3. Click the **Config** icon.
   The tabs to configure access points are displayed.
4. Click **Show Advanced**, and click the **Configuration Audit** tab.
   The **Configuration Audit** details page is displayed.
5. Ensure that the **Auto Commit State** for the group is set to **OFF**.
6. Based on configuration mode set for the device, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. When you try to save the save changes, Aruba Central displays the following warning message:



7. When the auto commit state for a group is set to **OFF**, and changes are configured to the devices at a group level, Aruba Central displays the following warning message when you try to save the changes:



8. View the **Local Overrides and Configuration Sync Issues**, if any.
9. Click **Commit Now** to commits the configuration changes to all devices within the group.

Viewing Configuration Overrides and Errors

The **Configuration Audit** page allows you to view the configuration push errors, template synchronization errors, configuration sync, and device level configuration overrides. Some of notable status indicators available on the page includes:

- **Configuration Status**—Provides details of the number of devices with configuration sync errors. To view the devices with configuration sync errors, click **View Details**. The **Config Difference** window is displayed. You can view configuration differences for each device within the group.
- **Local Overrides**—Provides details of the number of devices with local overrides. To view a complete list of overrides, click **Manage Local Overrides**. The **Local Overrides** window is displayed. You can view configuration differences for each device within the group. The overrides are grouped based on the features that are configured in the UI and are displayed as drop-down sections. For example, all overrides for IGMP are listed under a separate drop-down with the heading IGMP.

  To preserve the overrides, click **Close**. To remove the overrides, select the group name with local override, type **REMOVE** in the text box and click **OK**.
- **Configuration Conflicts**—Provides details of the number of devices with configuration conflict errors. To view a complete list of configuration conflicts, click **Manage Configuration Conflicts**. The **Configuration Conflict** window is displayed. To resolve the configuration conflicts, enable the check box against each conflict, and then click **Remove** to remove the conflict.
- **Template Errors**—Provides the details of the number of devices with template errors. To view a complete list of configuration template errors, click **View Template Errors**. The **Template Errors** window is displayed. You can view a list of templates with errors.
- **Move Failures**—Aruba Central supports moving a device from one group to another. If the move operation fails, Aruba Central logs such instances as **Move Failures**.

Viewing Configuration Status for Devices at the Group Level (Template Configuration Mode)

When you select a template group from the filter, the **Configuration Audit** page displays the following information:

Table 66: *Configuration Audit Status for a Template Group*

Data Pane Content	Description
Template Errors	Provides details of the number of devices with template errors for the selected template group. Devices deployed in the template group are provisioned using configuration templates. If there are errors in the templates or variable definitions, the configuration push to the devices fails. Aruba Central records such failed instances as template errors and displays these errors on the **Configuration Audit** page. To view a complete list of errors, click **View Template Errors**. The **Template Errors** window allows you to view and resolve the template errors issues if any.
Configuration Status	Provides details of the number of devices with configuration sync errors for the selected template group. To view the configuration sync errors, click **View Details**. The Configuration Sync Issues window is displayed with the following tabs: ▪ **Not In Sync Configuration**—Displays the configuration changes that are

Table 66: *Configuration Audit Status for a Template Group*

Data Pane Content	Description
	not synched with the switch. ▪ **Device Running Configuration**—Displays the running configuration on the switch. To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.
Configuration Backup & Restore	Allows you to create a backup of templates and variables applied to the devices in the template group. For more information, see Backing Up and Restoring Configuration Templates. ▪ **New Configuration Backup**—Allows you to create a new backup of templates and variables applied to the devices in the template group.
All Devices	The **All Devices** table provides the following device information for the selected group: ▪ **Name**—The name of the device. ▪ **Type**—The type of the device. ▪ **Auto Commit**—The status of the auto commit state for all the devices within the group. ▪ **Config Sync**—Indicator showing configuration sync errors. ▪ **Template Errors**—Indicator showing configuration template errors for the devices deployed in template groups.

Viewing Configuration Status for a Device (Template Configuration Mode)

When you select a device that is provisioned in a template group, the **Configuration Audit** page displays the following information:

Table 67: *Configuration Audit Status for Devices in Template Groups*

Data Pane Content	Description
Template Applied	Displays the template that is currently applied on the selected device.
Template Errors	Displays the number of template errors for the selected device. To view a complete list of errors, click **View Template Errors**.
Configuration Status	Displays the configuration sync errors for the selected device. To view the configuration sync errors, click **View Details**. The Configuration Sync Issues window is displayed with the following tabs: ▪ **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. ▪ **Device Running Configuration**—Displays the running configuration on the switch.

Table 67: *Configuration Audit Status for Devices in Template Groups*

Data Pane Content	Description
	To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.
Config Comparison Tool	Allows you to view the difference between the current configuration (**Device Running Configuration**) and the configuration that is yet to be pushed to the device (**Attempted Configuration**). To view the running and attempted configuration changes side by side, click **View**.

Viewing Configuration Status for Devices at the Group Level (UI-based Configuration Mode)

When you select an UI group, the **Configuration Audit** page displays the following information:

Table 68: *Configuration Audit Status for a UI Group*

Data Pane Content	Description
Configuration Status	Displays the number of devices with configuration sync errors for the selected UI group. To view the configuration sync errors, click **View Details**. The Configuration Sync Issues window is displayed with the following tabs: ▪ **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. ▪ **Device Running Configuration**—Displays the running configuration on the switch. To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.
Local Overrides	Displays the number of devices with local overrides. To view a complete list of overrides, click **Manage Local Overrides**. The **Local Overrides** window is displayed. The overrides are grouped based on the features that are configured in the UI and are displayed as drop-down sections. For example, all overrides for IGMP are listed under a separate drop-down with the heading IGMP. ▪ To preserve the overrides, click **Close**. ▪ To remove the overrides, select the group name with local override, type **REMOVE** in the text box and then click **OK**.
All Devices	The **All Devices** table provides the following device information for the selected group: ▪ **MAC Address**—MAC address of the device. ▪ **Name**—The name of the device. ▪ **IP Address**—IP address of the device. ▪ **Site**—Name of the site to which the device is assigned. ▪ **Type**—The type of the device.

Table 68: *Configuration Audit Status for a UI Group*

Data Pane Content	Description
	▪ **Auto Commit**—The status of the auto commit state for all the devices within the group. ▪ **Config Sync/Config Status**—Indicator showing configuration sync errors. ▪ **Local Overrides**—Indicator showing configuration overrides for the devices deployed in the UI groups. **NOTE:** The **MAC Address**, **IP Address**, **Site**, and **Config Status** columns are available only for groups in which Aruba gateways are provisioned (**Manage** > **Device** > **Gateways**, click the **Config** icon. The gateway configuration page is displayed. Navigate to **Configuration Audit**).

Viewing Configuration Status for a Device (UI-based Configuration Mode)

When you select a device assigned to a UI group, the **Configuration Audit** page displays the following information:

Table 69: *Configuration Audit Status for a Device Assigned to a UI Group*

Data Pane Content	Description
Configuration Status	Displays the number of devices with configuration sync errors for the selected device. To view the configuration sync errors, click **View Details**. The Configuration Sync Issues window is displayed with the following tabs: ▪ **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. ▪ **Device Running Configuration**—Displays the running configuration on the switch. To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch, see the Audit Trail page.
Local Overrides	Displays the number of local overrides. To view a complete list of overrides, click **Manage Local Overrides**. The **Local Overrides** window is displayed. The overrides are grouped based on the features that are configured in the UI and are displayed as drop-down sections. For example, all overrides for IGMP are listed under a separate drop-down with the heading IGMP. ▪ To preserve the overrides, click **Close**. ▪ To remove the overrides, click **Remove Local Overrides**, type **REMOVE** in the text box and then click **OK**.

Backing up and Restoring Configuration Templates

Aruba Central allows you to back up configuration templates assigned to the devices deployed in a template group. The **Configuration Audit** pages for Instant AP, switch, and gateway configuration containers allow

you to create and manage backed up files and restore these files when required. For more information, see Backing Up and Restoring Configuration Templates.

NOTE

If monitor mode is enabled at the device level, the selected device functions in the monitor mode. If the monitor mode is enabled at the group level, all devices in the group inherit this setting.
If a device managed by Aruba Central displays a **configuration sync issue** and persistently fails to receive configuration updates from Aruba Central, contact Aruba Central Technical Support.

Managing Software Upgrades

The **Firmware** page provides an overview of the latest firmware version supported on the device, details of the device, and the option to upgrade the device.

NOTE

Changing AOS-Switches firmware from latest version to earlier major versions is not recommended if the switches are managed in UI groups. For features that are not supported or not managed in Aruba Central on earlier AOS-Switch versions, changing firmware to earlier major versions might result in loss of configuration.

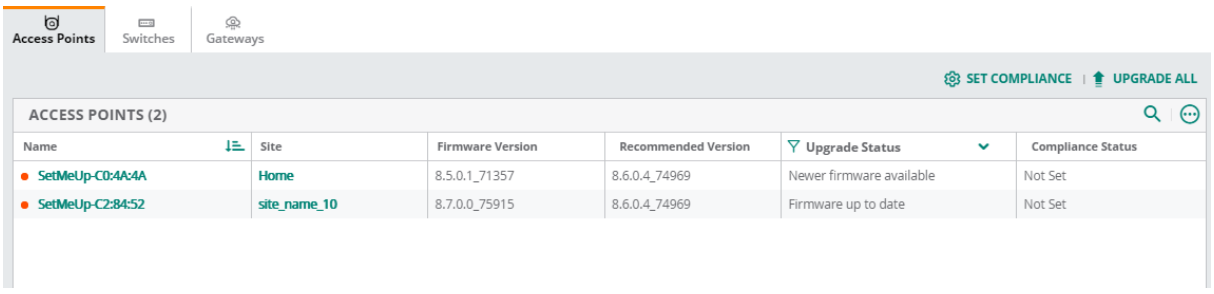
Viewing Firmware Details

To view the firmware details for devices provisioned in Aruba Central, perform the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter, set the filter to one of the options under **Group**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**. A list of devices is displayed.
     c. Click a device listed under **Device Name**. The dashboard context for the device is displayed.
2. Under **Maintain**, click **Firmware**. The **Firmware** dashboard displays the following information:

   The following image displays the **Firmware** dashboard at the global level:

   Figure 106 *Firmware Dashboard at Global Level*



Firmware Maintenance Window

The following are the data pane items and description:

1. **Access Points**—Displays the following information:
   - **Name**—Name of the AP. Clicking on the device name opens a window with connected APs and allows you to select and view the device Summary page. For more information, see Clients > Wireless Client > Overview.
   - **Site**—Displays the site information only on global context.
   - **Firmware Version**—The current firmware version running on the device.
   - **Latest Firmware Version**—The latest firmware version available on the public firmware server.
   - **Recommended Version**—The version to which the device is recommended for the upgrade.
   - **Upgrade Status**—Filters the device list based on any of the following firmware upgrade status:
     - **New firmware available**
     - **Scheduled**
     - **In progress**
     - **Failed**
     - **Firmware up to date**
   - **Compliance Status**—Status of the firmware compliance setting. The value displayed in this column is either **Set**, **Not Set**, and **Compliance scheduled on**. The **Compliance scheduled on** displays the date and time that is set in the Firmware Compliance Setting page.

Clicking on the device name from the **Name** columns, opens a window with connected APs and allows you to select and view the device **Summary** page. For more information, see Clients > Wireless Client > Overview. Click any site name from the **Site** column to view the site associated APs with their firmware details page.

2. **Switches**—Displays the following details about Aruba switches managed through Aruba Central:
   - **Name**—Host name of the switch.
   - **Family**—Displays the following types of switches:
     - AOS-S
     - CX

     This information is only available for Aruba switch and Aruba CX switches.
   - **Site**—Displays the site information only on global context.
   - **MAC Address**—MAC address of the switch.
   - **Model**—Hardware model of the switch.
   - **Firmware Version**—The current firmware version running on the switch.
   - **Recommended Version**—The version to which the device is recommended for the upgrade.
   - **Upgrade Status**—Filters the device list based on any of the following firmware upgrade status:
     - **New firmware available**
     - **Scheduled**
     - **In progress**
     - **Failed**
     - **Firmware up to date**
   - **Compliance Status**—Status of the firmware compliance setting. The value displayed in this column is either **Set**, **Not Set**, and **Compliance scheduled on**. The **Compliance scheduled on** displays the date and time that is set in the Firmware Compliance Setting page.

- The **Switch-MAS** tab is only available for accounts with MAS-switches.
- The **Switches** tab displays details of both Aruba Switch and Aruba CX switches.

3. **Gateways**—Displays the following details about the SD-WAN Gateways managed through Aruba Central in **Standalone** mode:
   - **Name**—Host name of the SD-WAN Gateway.
   - **Site**—Displays the site information only on global context.
   - **MAC Address**—MAC address of the SD-WAN Gateway.
   - **Model**—Hardware model of the SD-WAN Gateway.
   - **Firmware Version**—The current firmware version running on the SD-WAN Gateway.
   - **Recommended Version**—The version to which the device is recommended for the upgrade.
   - **Upgrade Status**—Filters the device list based on any of the following firmware upgrade status:
     - **New firmware available**
     - **Scheduled**
     - **In progress**
     - **Failed**
     - **Firmware up to date**
   - **Compliance Status**—Status of the firmware compliance setting. The value displayed in this column is either **Set**, **Not Set**, and **Compliance scheduled on**. The **Compliance scheduled on** displays the date and time that is set in the Firmware Compliance Setting page.
4. **Set Compliance**—Allows you to set firmware compliance for devices within a group. Click **Set Compliance** and turn on the toggle switch to enable and view the list of supported firmware versions for each device in a group in the **Manage Firmware Compliance** page.
   a. **Set Compliance for Access Points**—To ensure firmware version compliance, complete the following parameters in the **Manage Firmware Compliance** page:
      - **Groups**—Select a specific group or multiple groups for which the compliance must be set. Select **All Groups** if you want to set compliance for all the groups.
      - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
      - **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time.
        - **Now**—To set the compliance to be carried out immediately.
        - **Later Date**—To set at the later date and time.
      - Click **Save and Upgrade** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.

   b. **Set Compliance for Switches**—To ensure firmware version compliance, complete the following parameters in the **Manage Firmware Compliance** page:
      - **Groups**—Select the group for which the compliance must be set. Select the specific group to set compliance at group level.
      - **AOS-S Firmware Version**—Select the AOS-S firmware version number from the drop-down list to which the compliance is required to be set.
      - **CX Firmware Version**—Select the Aruba CX switch version number from the drop-down list to which the compliance is required to be set.

- **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
- **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
  - **Now**—To set the compliance to be carried out immediately.
  - **Later Date**—To set at the later date and time.
- Click **Save and Upgrade** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.

Aruba Central lists all available Aruba CX switches software versions. Select the software version that is applicable to the Aruba CX switch to which compliance is required to be set. For example, version `10.04.0020` is not applicable to Aruba CX 6200 and 6400 switch series.

c. **Set Compliance for Gateways in Standalone Mode**—To ensure firmware version compliance, complete the following parameters in the **Manage Firmware Compliance** page:
   - **Groups**—Select a specific group or multiple groups for which the compliance must be set. Select **All Groups** if you want to set compliance for all the groups.
   - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
   - **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
   - **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
     - **Now**—To set the compliance to be carried out immediately.
     - **Later Date**—To set at the later date and time.
   - Click **Save and Upgrade** button to save the firmware compliance with the above settings. To clear the compliance, turn off the toggle switch.

5. **Upgrade All**—Allows you to simultaneously upgrade firmware for all devices. Click **Upgrade All** to view a list of supported firmware versions for each device.
   a. **To Upgrade all Access Points**—Click **Upgrade All** and complete the following parameters in the **Upgrade Access Points Firmware** page:
      - **Sites**—Select a specific site or multiple sites for which the upgrade must be set. You can also search for the site in the search filter.
      - **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set. Select **None** for none of the firmware versions.
      - **When** —Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
        - **Now**—To set the compliance to be carried out immediately.
        - **Later Date**—To set at the later date and time.
      - **Upgrade**—Click this button to start the upgrade with the above settings.
      - **Cancel**—Click this button to cancel the upgrade.

While upgrading a large number of APs, cancel operation may not work as intended, and continues to upgrade.

   b. **To Upgrade all Switches**—Click **Upgrade All** and complete the following parameters in the **Upgrade Switch Firmware** page:

- **Sites**—Select a specific site or multiple sites for which the upgrade must be set. You can also search for the site in the search filter.
- **AOS-S Firmware Version**—Select the AOS-S firmware version number from the drop-down list to which the compliance is required to be set.
- **CX Firmware Version**—Select the CX switch firmware version number from the drop-down list to which the compliance is required to be set.
- **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
- **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time:
  - **Now**—To set the compliance to be carried out immediately.
  - **Later Date**—To set at the later date and time.
- **Upgrade**—Click this button to start the upgrade with the above settings.
- **Cancel**—Click this button to cancel the upgrade.

c. **To Upgrade all Gateways in Standalone Mode**—click **Upgrade All** and complete the following parameters in the **Upgrade Gateway Firmware** page:
- **Sites**—Select a specific site or multiple sites for which the upgrade must be set. You can also search for the site in the search filter.
- **Firmware Version**—Select the firmware version number from the drop-down list to which the compliance is required to be set.
- **Auto Reboot**—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device.
- **When**—Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time.
  - **Now**—To set the compliance to be carried out immediately.
  - **Later Date**—To set at the later date and time.
- **Upgrade**—Click this button to start the upgrade with the above settings.
- **Cancel**—Click this button to cancel the upgrade.

6. **Search Filter**—Allows you to define a filter criterion for searching devices based on the following properties:
   - Common to all devices—Name, Firmware Version, Recommended Version and Upgrade Status of the device.
   - Specific to switches and gateways—MAC address and Model.
7. **Column Filter**—Clicking icon enables you to customize the table columns or set it to the default view.
8. **Continue**—Allows you to continue with firmware upgrade.
9. **Cancel Upgrade**—Cancels a scheduled upgrade.
10. **Cancel All**—Cancels a scheduled upgrade for all devices.

This section also includes the following topics:

- Upgrading a Single Device or Multiple Devices
- Upgrading Devices using Upgrade All Option
- Setting Firmware Compliance For Access Points
- Setting Firmware Compliance For Switches
- Setting Firmware Compliance For Gateways in Standalone Mode

Upgrading a Single Device or Multiple Devices

To check a new version for a single device or multiple devices, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   a. To select a group, site or global in the filter:
      - Set the filter to one of the options under **Group** or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
      - Under **Maintain**, click **Firmware**.
      - Select one or more devices from the device list and click the **Upgrade** icon at the bottom of the page or hover over one of the selected device and click the **Upgrade** icon. The **Upgrade <Device> Firmware** pop-up window opens.

   b. To select a device in the filter:
      - Set the filter to **Global**.
      - Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**. A list of devices is displayed.
      - Click a device listed under **Device Name**. The dashboard context for the device is displayed.
      - Under **Maintain**, click **Firmware** and click **Upgrade** in the **Firmware Details** window. The **Upgrade <Device> Firmware** pop-up window opens.
2. In the **Upgrade <Device> Firmware** pop-up window, select the appropriate firmware version. You can either select a recommended version or manually choose a specific firmware version.

To obtain custom build details, contact Aruba Central Technical Support.

3. Select **Auto Reboot** if you want Aruba Central to automatically reboot after device upgrade.

The **Auto Reboot** option is available for Mobility Access Switches, Aruba Switch, Aruba CX switches, and Branch Gateways.

4. Specify if the upgrade must be carried out immediately or at a later date and time.
5. Click **Upgrade**. The device downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:
   - **Upgrading**—While image upgrade is in progress.
   - **Upgrade failed**—When the upgrade fails.
6. If the upgrade fails, retry upgrading your device.

After upgrading a switch, click **Reboot**.

Upgrading Devices using Upgrade All Option

To upgrade multiple devices using the **Upgrade All** option, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group** or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Firmware**.
   The firmware dashboard for Access Points is displayed by default.
3. Click **Upgrade All**. The **Upgrade <Device> Firmware** pop-up window opens.

4. In the **Upgrade <Device> Firmware** pop-up window, select the specific site or multiple sites from the **Sites** drop-down list. This option is available only at the global context.
5. Select the appropriate firmware version (for Access points and Gateways) and AOS-S firmware version and CX firmware version (for Mobility Access Switches, Aruba Switch and Aruba CX switches) from their respective drop-down list. You can either select a recommended version or manually choose a specific firmware version.

NOTE

To obtain custom build details, contact Aruba Central Technical Support.

6. Select **Auto Reboot** if you want Aruba Central to automatically reboot after device upgrade.

NOTE

The **Auto Reboot** option is available for Mobility Access Switches, Aruba Switch, Aruba CX switches, and Branch Gateways.

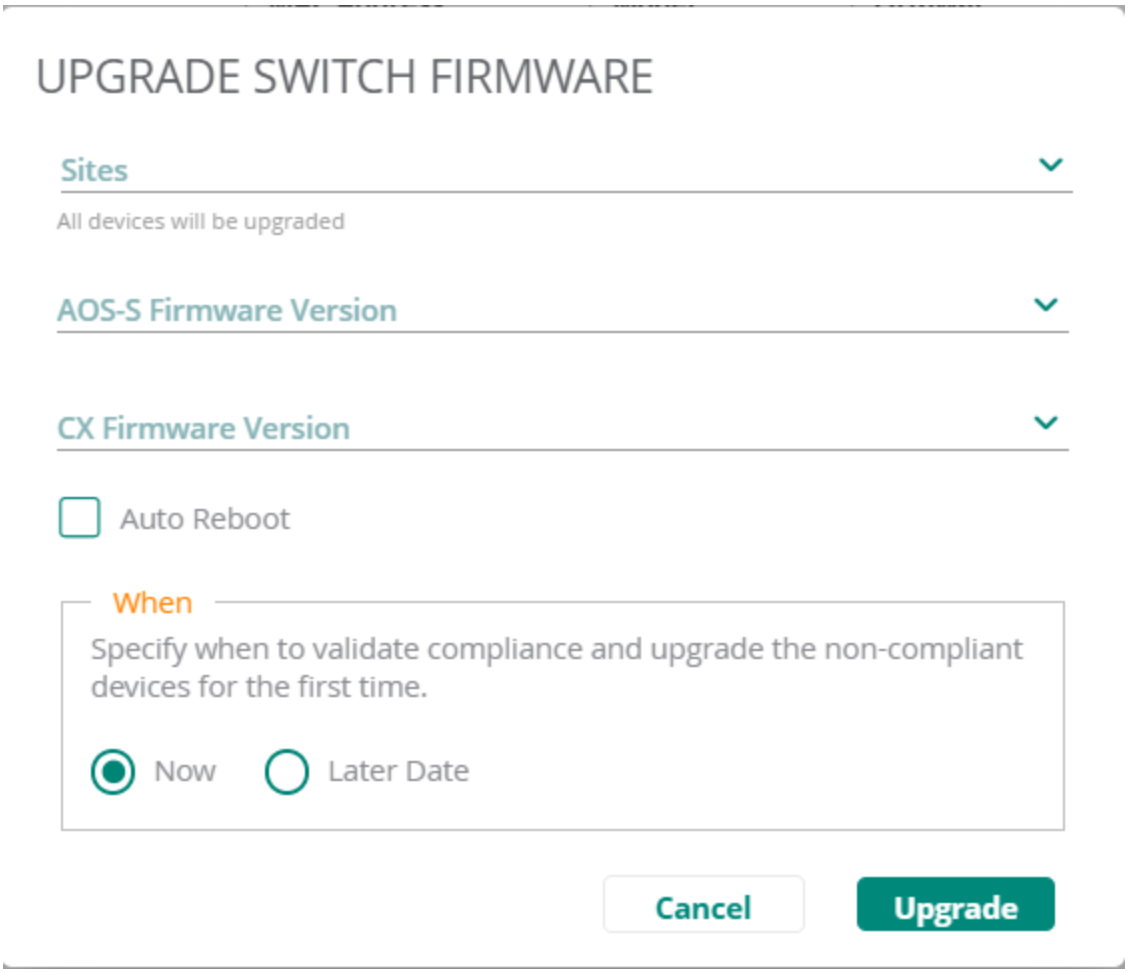
7. Specify if the upgrade must be carried out immediately or at a later date and time.
8. Click **Upgrade**. The device downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:
   - **Upgrading**—While image upgrade is in progress.
   - **Upgrade failed**—When the upgrade fails.
9. If the upgrade fails, retry upgrading your device.

NOTE

After upgrading a switch, click **Reboot**.

The following image displays the **Upgrade <Device> Firmware** window for the switches:

Figure 107 *Upgrade Switch Firmware*



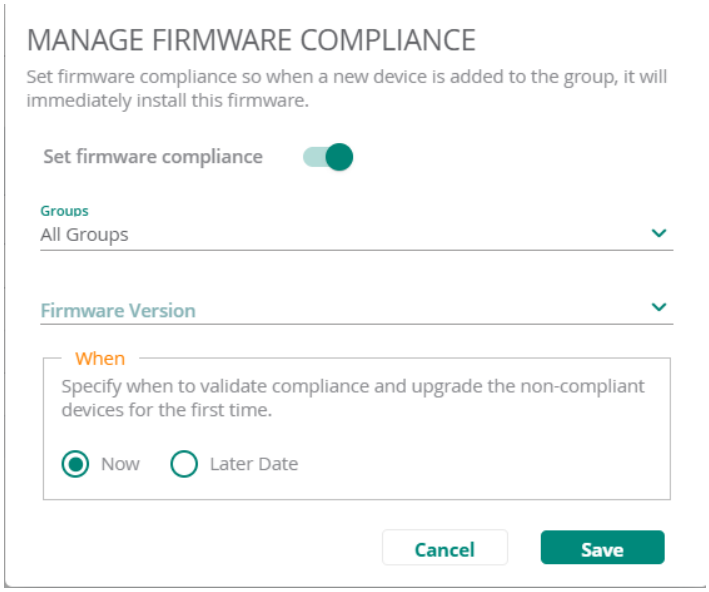
Setting Firmware Compliance For Access Points

Aruba Central allows you to run a firmware compliance check and force firmware upgrade for all APs in a group. To force a specific firmware version for all APs in a group, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware**.
   The **Access Points** tab is selected by default.
2. Verify the firmware upgrade status for all APs.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a firmware version from the **Firmware Version** drop-down list.
6. Select one of the following as required:
   - Select **Now** to set the compliance to be carried out immediately.
   - Select **Later Date** to set the compliance at the later date and time.
7. Click **Save and Upgrade**.
   Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

The following image displays the **Manage Firmware Compliance** window for Access Points:

Figure 108 *Manage Firmware Compliance*



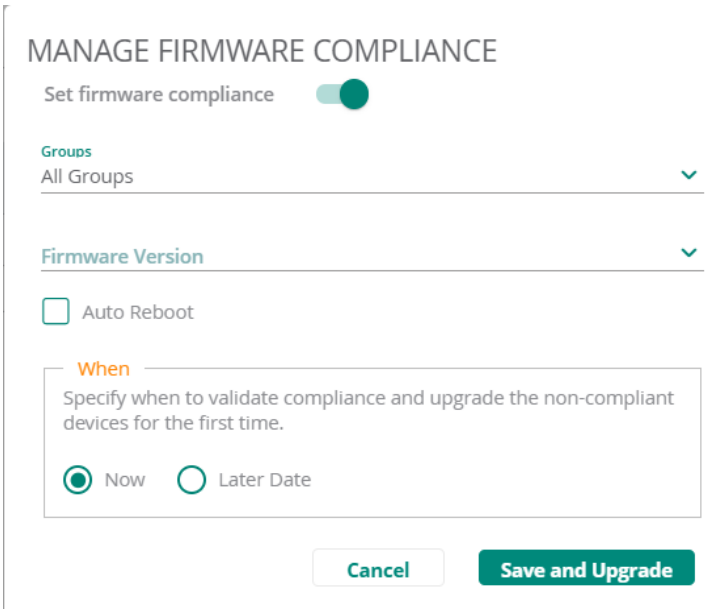
Setting Firmware Compliance For Switches

To force a specific firmware version for all MAS switches in a group, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware** > **Switch-MAS** tab.
2. Verify the firmware upgrade status for all MAS switches.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a firmware version from the **Firmware Version** drop-down list.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.
7. Select one of the following as required:
   - Select **Now** to set the compliance to be carried out immediately.
   - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**. Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

   The following image displays the **Manage Firmware Compliance** window for MAS switches:

Figure 109 *Manage Firmware Compliance Window for MAS Switches*

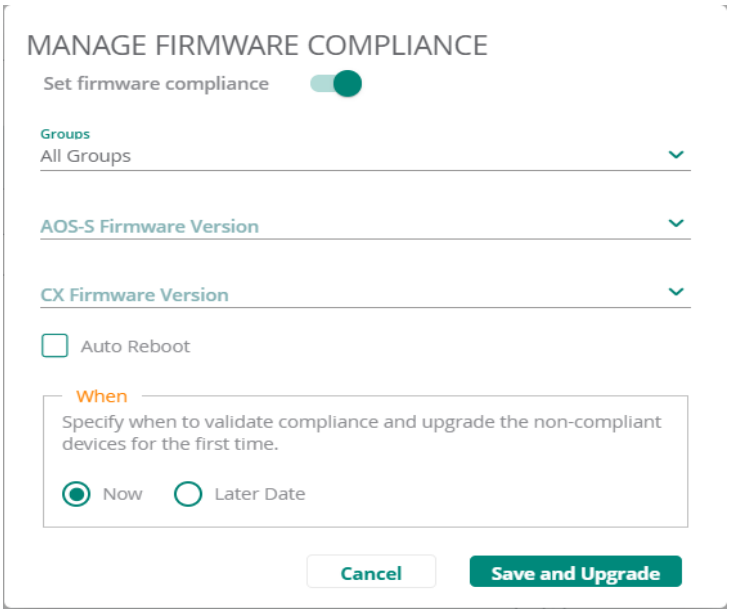


To force a specific firmware version for all Aruba switches in a group, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware** > **Switches** tab.
2. Verify the firmware upgrade status for all switches.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a AOS-S firmware version from the **AOS-S Firmware Version** drop-down list.
6. Select a CX firmware version from the **CX Firmware Version** drop-down list.
7. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.
8. Select one of the following as required:
   - Select **Now** to set the compliance to be carried out immediately.
   - Select **Later Date** to set the compliance at the later date and time.
9. Click **Save and Upgrade**. Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

   The following image displays the **Manage Firmware Compliance** window for Aruba switches:

Figure 110 *Manage Firmware Compliance Window for Aruba Switches*



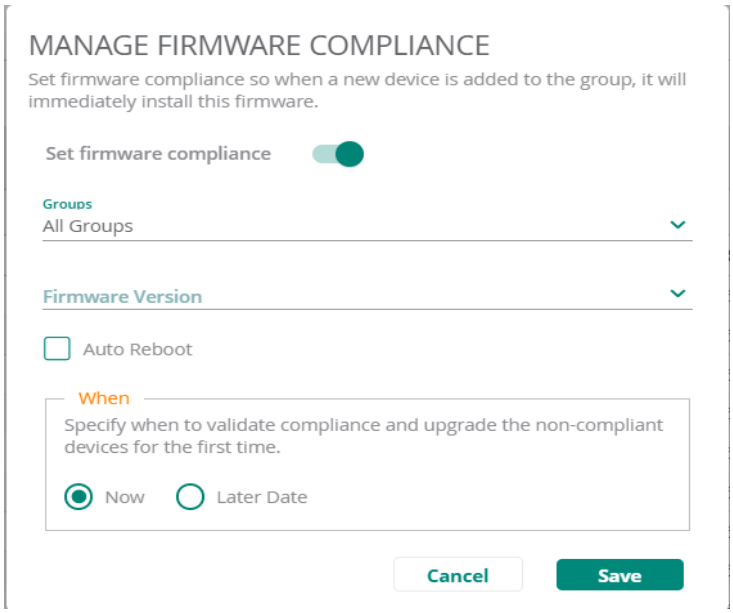
Setting Firmware Compliance For Gateways in Standalone Mode

To force a specific firmware version for all gateways in standalone mode, complete the following steps:

1. In the **Global** dashboard, under **Maintain**, click **Firmware** > **Gateways** tab. All the gateways with standalone mode is displayed.
2. Verify the firmware upgrade status for all gateways.
3. Click **Set Compliance** at the top right and turn on the toggle switch to enable the **Manage Firmware Compliance** window.
4. In the **Groups** drop-down list, select a single group, multiple, or All Groups.
5. Select a firmware version from the **Firmware Version** drop-down list.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.
7. Select one of the following as required:
   - Select **Now** to set the compliance to be carried out immediately.
   - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**. Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

   The following image displays the **Manage Firmware Compliance** window for gateways:

Figure 111 *Manage Firmware Compliance*



Viewing Audit Trail in the Standard Enterprise Mode and MSP Mode

The **Audit Trail** page in the Standard Enterprise Portal shows the total logs generated for all the device management, configuration, and user management events triggered in Aruba Central. You can search or filter the audit trail records based on any of the following columns:

- Occurred on (Custom Range)
- Username
- IP Address
- Category
- Description
- Target

To view the audit trail log details in Aruba Central, perform the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group or all devices in the filter, set the filter to **Group**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.

2. Under **Analyze**, click **Audit Trail**.

   The Audit Trail table is displayed with the following details:

   - **Occurred On**— Timestamp of the audit log. Use the sort option to sort the audit logs by date and time. Use the filter option to select a specific time range to display the audit logs.
   - **IP Address**—IP address of the client device.
   - **Username**—Username of the admin user who applied the changes.
   - **Target**—The group or device to which the changes were applied.
   - **Category**—Type of modification and the affected device management category.
   - **Description**—A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click ⋮ to view the complete details of the event. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.

To customize the **Audit Trail** table, click the eclipses icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Classification of Audit Trails

The audit trail is classified according to the type of modification and the affected device management category. The category can be one of the following:

- Configuration
- Firmware Management
- Reboot
- Device Management
- Templates
- User Management
- Variables
- Label Management
- MSP
- Guest
- Groups
- Subscription Management
- API Gateway
- RBAC
- Sites Management
- SAML Profile
- User Activity
- Federated User Activity
- Alert Configuration
- Install Manager
- Tools

Removing Devices

The device monitoring dashboards allow you to remove an offline device. However, you will not be able to remove a device completely from Aruba Central database, because the device entry remains in the **Device Inventory** page. The devices appearing in the **Device Inventory** page shows the hardware devices that belong to your account or purchase order.

For information on removing an offline device, see the following topics:

- Deleting an Offline AP
- Deleting an Offline Switch
- Deleting a Gateway

Removing a Device from the Device Inventory Page

You cannot remove a device completely from Aruba Central, but you can unsubscribe the device. After you unsubscribe, the device status changes to **Unsubscribed** in the **Device Inventory** page. If you have more than one Aruba Central account and if another Aruba Central user adds this unsubscribed device to another Aruba Central account, the device entry is removed from the **Device Inventory** page in your Aruba Central account.

Chapter 6
The AI Insights Dashboard

In an environment of rapidly changing business and user expectations driven by an explosion of connectivity requirements from the edge to the cloud, a new approach to network management is required. Aruba AIOps (Artificial Intelligence for IT operations) is the next generation of AI-powered solutions that integrates proven Artificial Intelligence solutions with recommended and automated action to provide both fast response to identified problems, along with proactive prediction and prevention.

With data collected from over 750,000 access points, switches, and gateways, Aruba Central and built-in AI Insights proactively identifies and solves issues, and provides pinpoint configuration recommendations. As the data is stored in the cloud, it is easy to view the network performance across all locations from a single pane of glass. Utilizing the cloud also provides the ability to anonymously compare a network with a peer network or the baselines for a broader perspective and optimization. All of this comes from Aruba's advantage in accessing an enormous volume and variety of data that is factored into insights. Aruba does not collect or process personal data.

In this release the insights are classified under three categories:

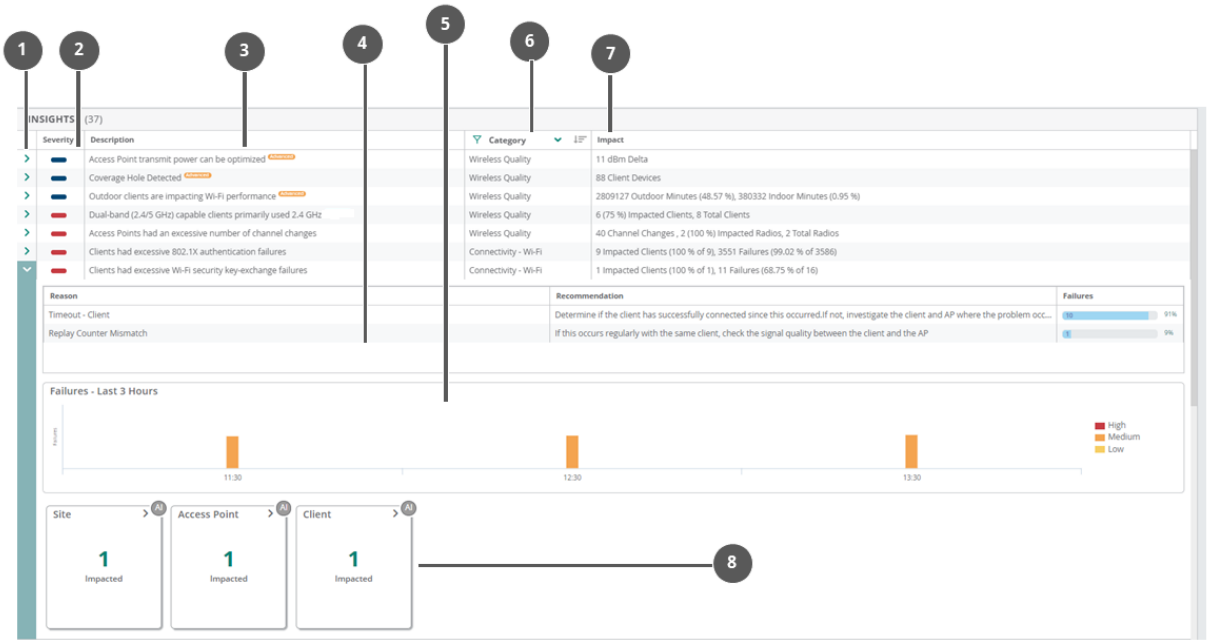
- Connectivity—Issues related to the wireless connectivity in the network.
- Wireless Quality—Issues related to the RF Info or RF Health in the network.
- Availability—Issues related to the health of your network infrastructure and the devices in the network such as, APs, switches, and gateways.

The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level for the selected time range. Each insight provides specific details on the occurrences of these events for easy debugging.

To launch the **AI Insights** dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Overview > AI Insights**. The **Insights** table is displayed. AI Insights listed in the dashboard are sorted from high priority to low priority.
3. Click the arrow › against each insight to view the further details.

Figure 112 *Insight Details*



Callout Number	Description
1	Click this arrow to expand any specific insight to view further details.
2	Displays the insight severity, using the following colors: Red—High priority Orange—Medium priority Yellow—Low priority **NOTE:** The following three configuration recommendation insights are marked in blue color ( ) in the severity column: ●Access Point Transmit Power can be Optimized ●Coverage Holes Identified ●Outdoor Clients Impacting Wi-Fi Performance
3	Short description of the insight.
4	Insight Summary displays the reason why the insight was generated along with recommendation. It also shows the number and percentage of failures that occurred against each failure reason. The reasons are classified into: ▪ Static—These reasons rely on Aruba's domain expertise. ▪ Dynamic—These reasons are generated based on error codes that is received from infrastructure devices.
5	Time Series graph is a graphical representation of the failure percentage or failure events that occurred for the selected time range. The entries in each time series bar can be customized to highlight a specific entry by clicking on it. Only one specific entry can be highlighted at a time.
6	Category of the insight. Insight category can be filtered by clicking the filter icon.

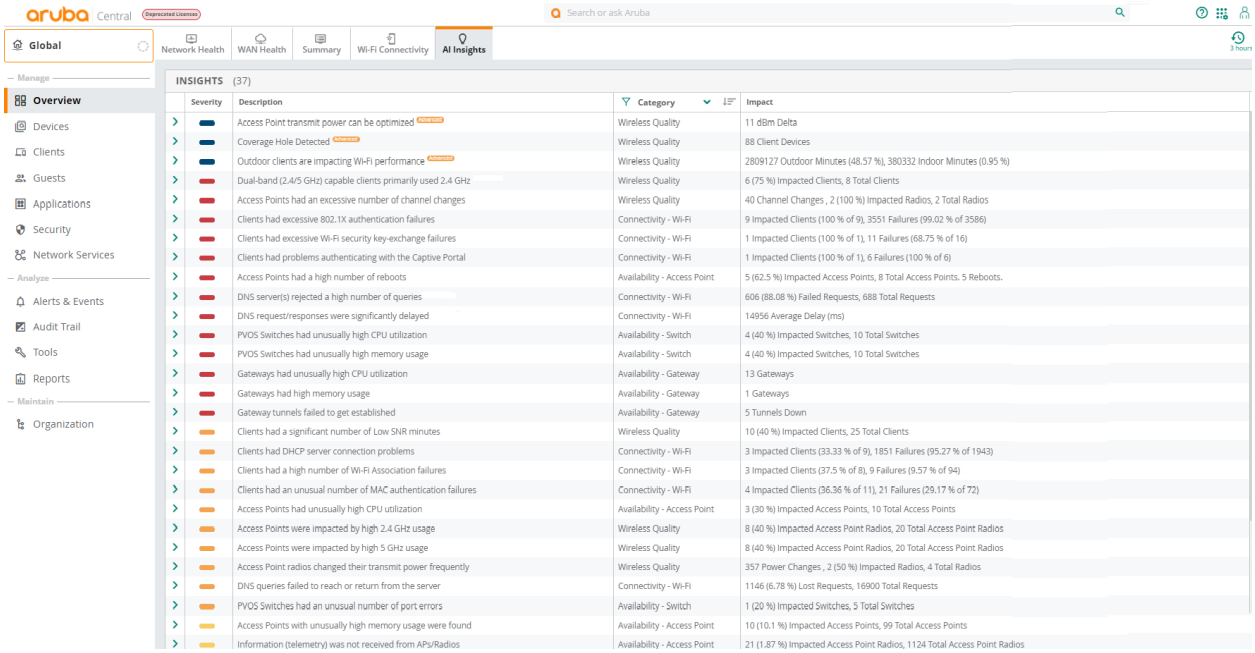
Callout Number	Description
7	Short description of the impact.
8	Cards display additional information specific to each insight. Cards might vary for each insight based on the context the insight is accessed from. For more information, see Cards.

All AI Insights generated are listed in the **Global > AI Insights** dashboard. Alternatively, AI Insights for a specific site, device, or client can be viewed by selecting the respective context. For more information on available insights and the context, see Insights Context.

NOTE

AI Insights are displayed for a selected time period based on the time selected in the **Time Range Filter** ( ). You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**.

Figure 113 *AI Insights Dashboard*



Insights Context

Insights can be accessed from different contexts such as **Global**, **Site**, **Clients**, and **Device**. The following table lists the different types of insights generated by Aruba Central and the path from where it can be accessed.

NOTE

In this release, all AI Insights are available irrespective of the user role or Aruba Central subscription. In the upcoming Aruba Central release, AI Insights marked as **Advanced** in the user interface would require an advanced subscription.

Table 70: *Navigating Insights*

Insights	Category	Context	Navigation
Access Points with High CPU Utilization	**Availability - Access Point**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
Access Points with High Memory Usage	**Availability - Access Point**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
Telemetry Information not Received from APs or Radios	**Availability - Access Point**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
Access Points with High Number of Reboots	**Availability - Access Point**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**

Insights	Category	Context	Navigation
AOS-CX Switches with High Port Flaps	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
AOS-CX Switches with High Port Errors	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
AOS-CX Switch Ports with High Power-over-Ethernet Problems	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
AOS-CX Switches with High CPU Utilization	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**

Insights	Category	Context	Navigation
AOS-CX Switches with High Memory Usage	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
AOS-Switches with High Port Flaps	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
AOS-Switches with High Port Errors	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
AOS-Switch Ports with High Power-over-Ethernet Problems	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**

Insights	Category	Context	Navigation
AOS-Switches with High CPU Utilization	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
AOS-Switches with High Memory Usage	**Availability - Switch**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Switches	**Network Operations > Global > Devices > Switches > Device Name > AI Insights**
Failure to Establish Gateway Tunnels	**Availability - Gateway**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Gateways	**Network Operations > Global > Devices > Gateways > Device Name > AI Insights**
Gateways with High CPU Utilization	**Availability - Gateway**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Gateways	**Network Operations > Global > Devices > Gateways > Device Name > AI Insights**

Insights	Category	Context	Navigation
Gateways with High Memory Usage	**Availability - Gateway**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Gateways	**Network Operations > Global > Devices > Gateways > Device Name > AI Insights**
Clients who Roamed Excessively	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
Clients with High Roaming Latency	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**

Insights	Category	Context	Navigation
Clients with Captive Portal Authentication Problems	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
Clients with High Number of Wi-Fi Association Failures	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**

Insights	Category	Context	Navigation
Delayed DNS Request or Response	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
DNS Servers Rejected High Number of Queries	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**

Insights	Category	Context	Navigation
Clients with DHCP Server Connection Problems	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
DNS Queries Failed to Reach or Return from the Server	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**

Insights	Category	Context	Navigation
Clients with High MAC Authentication Failures	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
Clients with High Wi-Fi Security Key-Exchange Failures	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**

Insights	Category	Context	Navigation
Clients with High 802.1X Authentication Failures	**Connectivity - Wi-Fi**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
Access Point Transmit Power can be Optimized	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**
Access Points Impacted by High 2.4 GHz Usage	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
Access Points Impacted by High 5 GHz Usage	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**

Insights	Category	Context	Navigation
Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
Clients with Low SNR Minutes	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
		Clients	**Network Operations > Global > Clients > Client Name > AI Insights** **Network Operations > Site > Clients > Client Name > AI Insights**
Coverage Holes Identified	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**

Insights	Category	Context	Navigation
Access Points with Excessive Number of Channel Changes	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
Access Points Radios with Frequent Transmit Power Changes	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**
		Site	**Network Operations > Sites > Overview > AI Insights**
		Access Points	**Network Operations > Global > Devices > Access Points > Device Name > AI Insights**
Outdoor Clients Impacting Wi-Fi Performance	**Wireless Quality**	Global	**Network Operations > Global > Overview > AI Insights**

Cards

All the insights in Aruba Central display certain cards with additional information specific to that insight. The top view of each card usually shows the most impacted data in a pie chart or a bar graph view. The data in a pie chart can be modified based on your requirement. To highlight specific entries in a card, click the check box next to each label. Few cards have further drill down option available, in the form of a drop-down. Additionally, a few cards have an expandable view option to view the graph.

The cards might vary for each insight based on the context the insight is accessed from. The following table displays the cards available in different insights:

Table 71: *Cards*

Card	Description
Site	The **Site** card displays the number of sites impacted by an insight. Click the arrow › to expand the card and view the most impacted sites where the issue occurred.

Card	Description
Access Points	The **Access Point** card displays the number of APs impacted by an insight. Click the arrow › to expand the card and view the most impacted APs where the issue occurred. You can also click the drop-down list to view further details about the impacted access points.
Clients	The **Client** card displays the number of clients impacted by an insight. Click the arrow › to expand the card and view the most impacted clients where the issue occurred.
Server	The **Server** card displays the number of servers impacted by an insight. Click the arrow › to expand the card and view the most impacted servers where the issue occurred.
RF Info	The **RF Info** card displays the number of channels, band, and SSID information based on the insight it is accessed from. Click the arrow › to expand the card and view the relevant information. You can also click the drop-down list to view further details about the impacted RF bands.
Switch	The **Switch** card displays the number of switches impacted by an insight. Click the arrow › to expand the card and view the most impacted switches where the issue occurred. You can also click the drop-down list to view further details about the impacted switches.
Wired Clients	The **Wired Client** card displays the number of wired clients impacted by an insight. Click the arrow › to expand the card and click the drop-down list to view further details about the impacted wired clients.
Roam	The **Roam** card displays the percentage of client latency roams. Click the arrow › to expand the card and click the drop-down list to view further details about the roaming latency and band.
Tunnel	The **Tunnel** card displays the number of gateway tunnels down. Click the arrow › to expand the card and view the reasons for the cause of tunnel down.
Gateway	The **Gateway** card displays the number of gateways impacted by an insight. Click the arrow › to expand the card and view the most impacted gateways where the issue occurred. You can also click the drop-down list to view further details about the impacted gateways.
VPNC	The **VPNC** card displays the number of VPNC gateways on which the tunnels are down. Click the arrow › to expand the card and view the reasons for the cause of VPNC tunnel down.
Outdoor Clients	The **Outdoor Clients** card is available only for **Outdoor Clients Impacting Wi-Fi Performance** insight and it displays the percentage of avoided outdoor client minutes. Click the arrow › to expand the card and view graphical representation of the data.

Card	Description
Outdoor Minutes	The **Outdoor Minutes** card is available only for **Outdoor Clients Impacting Wi-Fi Performance** insight and it displays the percentage of avoided outdoor clients minutes and affected indoor client minutes. Click the arrow to expand the card and view graphical representation of the data.
Port	The **Port** card is available for the switch port health insights and it displays the number of ports experiencing excessive flaps or errors. Click the arrow to expand the card and view the most impacted ports where the issue occurred.
CPU	The **CPU** card is available at the device (Gateways and Switches) context and displays the number of gateways and switches impacted by high CPU utilization in the network. Click the arrow to expand the card and view graphical representation of the data.
Memory	The **Memory** card is available at the device (Gateways and Switches) context and displays the number of gateways and switches impacted by high memory utilization in the network. Click the arrow to expand the card and view graphical representation of the data.
Power	The **Power** card displays the number of power changes in access points in the network. Click the arrow to expand the card and click the drop-down list to view further details about the impacted access points.
Channel	The **Channel** card displays the number of channels changes per channel for a specific access point in the network. Click the arrow to expand the card and click the drop-down list to view further details about the impacted channels.

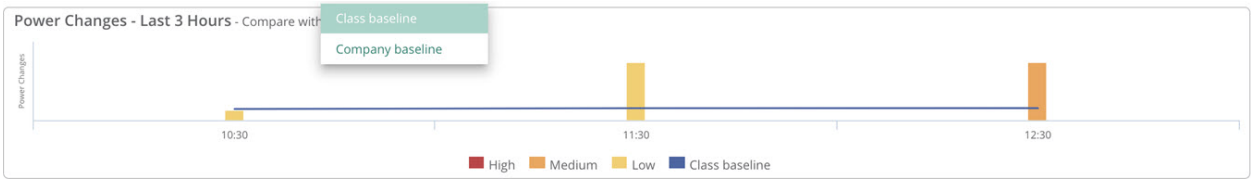
If you click on the number displayed on each card, further details specific to that card is displayed in a tabular format. The filter icon allows you to filter data in each table columns. The and icon allows you to sort the columns in ascending and descending order. Few columns are displayed by default whereas, there are few columns which does not appear in the table by default.

To customize a table, click the ellipses icon to select the required columns, or click **Reset to default** to set the table to the default columns. Click to download the card details in a CSV format.

Baselines

Baseline enables you to compare your network performance with similar peer groups. Baseline is calculated on a weekly basis and is available in the trend chart for insights in the **Site** context only. Baseline is displayed as a blue line in the trend chart. The following two baselines are available in Aruba Central:

- **Class baseline**—Provides a comparison with similar peer groups in the networks. Peer group classification is done based on various parameters such as number of access points, neighboring devices information, and so on.
- **Company baseline**—Provides a comparison of the network within the entire customer ID (CID).



Baseline is supported for the following insights:

- Clients with High MAC Authentication Failures
- Clients with High Wi-Fi Security Key-Exchange Failures
- Clients with High 802.1X Authentication Failures
- Clients with DHCP Server Connection Problems
- DNS Queries Failed to Reach or Return from the Server
- DNS Servers Rejected High Number of Queries
- Delayed DNS Request or Response
- Access Points with High CPU Utilization
- Access Points with High Memory Usage
- Access Points with High Number of Reboots
- Telemetry Information not Received from APs or Radios
- Access Points with Excessive Number of Channel Changes
- Access Points Impacted by High 2.4 GHz Usage
- Access Points Impacted by High 5 GHz Usage
- Access Point Transmit Power can be Optimized
- Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz
- Clients with Low SNR Minutes

Access Points with High Number of Reboots

The **Access Points had a high number of reboots** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about APs that have been rebooted the maximum times and is categorized under availability as the clients connected to these APs experience connectivity drops. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

The time series graph displays the number of AP reboots that occurred during the selected time period. You can hover your mouse over each bar graph to see the exact number of reboots.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 72: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience excessive reboots. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Reboots**—Number of APs that experience expressive reboots in each site.
- **APs**—Number reboots that occurred in each AP in a specific site.

Access Point

Lists the number and details of reboots observed in an AP. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **Time Series**—Pictorial graph of the AP reboots that occurred on different dates but similar timestamp.
- **FW Version**—Pictorial graph of AP reboots classified by AP firmware versions.
- **AP Model**—Pictorial graph of AP reboots classified by AP models.

Click the number displayed on the **Access Point** card, to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **AP Serial**—Serial number of the AP.
- **FW Version**—Version of the firmware running on each AP.
- **Model**—Model number of each AP.
- **Site**—Name of the site where the AP resides.
- **Reboots**—Number of reboots over time.

Access Points with Excessive Number of Channel Changes

The **Access Points had an excessive number of channel changes** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about AP radios on the network that changed channels excessively in the network. It is categorized under wireless quality as the connected clients might have to reconnect after an AP changes channel for a better network performance. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs changed channels on the network.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.
- **Channel Changes**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of channel changes per channel for a specific AP during the selected time period. You can hover your mouse on each bar graph to see the exact number of channel changes.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 73: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site
Client	Global, Site, Device
Channel	Global, Site, Device

Site

Lists the number of sites that experience excessive AP radio channel changes in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Channel Changes**—Total number of channel changes in each site.
- **Impacted Sessions**—Number of times the insight is triggered on each site.
- **Total Session**—Total number of session count in each site.
- **Impacted Radio**—Number of radios with high airtime.
- **Total Radios**—Total number of radios in each site.

Access Point

Lists the number and details of APs that experience excessive AP radio channel changes in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of the channel changes classified by AP models.
- **FW Version**—Pictorial graph of channel changes classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Serial**—Serial number of the AP.
- **Model**—Model number of each AP.
- **Band**—Bandwidth where each AP dwells.
- **Channel Changes**—Number of channel changes on each AP.
- **Impacted Sessions**—Number of times the insight is triggered on each AP.
- **Total Sessions**—Total number of session count in each AP.

Client

Lists the MAC Address, name, host name, auth ID, and the corresponding number of channel changes for each client. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Clients** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client impacted by the insight and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Times Impacted**—Number of channels changed on each client.

Channel

Number of channel changes per channel for a specific AP during the selected time period. Click the arrow › to expand the card and view the pictorial graph of the channel changes. Click the **Channel** drop-down list to view the following:

- **Band**— Pictorial graph of the channel changes based on both 2.4 GHz and 5 GHz.
- **Channel**—Pictorial graph of the number of channel changes per channel for a specific AP during the selected time period. It shows a comparison of the channel change between the peer network and AP. Click  to expand the channel data.

Click the number displayed on the **Channel** card to view a detailed description of the impacted channels:

- **From Channel**—Total number of channels.
- **Changes**—Number of channels that experienced excessive changes.

Access Points with High CPU Utilization

The **Access Points had unusually high CPU utilization** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about APs that have higher than normal CPU utilization and is categorized under availability as the clients connected to these APs experience intermittent connectivity drops. This insight displays the following information:

Time Series Graph

The time series graph displays the number of APs that experience high CPU utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number of APs.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 74: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience high CPU utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **APs**—Number of APs that experience high CPU utilization in each site.
- **Time (min)**—Time range of high CPU utilization in each site.

Access Point

Lists the number and details of APs that experience high CPU utilization in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **AP Model**—Pictorial graph of CPU utilization classified by AP models.
- **FW Version**—Pictorial graph of CPU utilization classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP.
- **AP Serial**—Serial number of the AP.
- **Firmware**—Version of the firmware running on each AP.
- **Model**—Model number of each AP.
- **Site**—Name of the site where the AP resides.
- **Time (min)**—Time range of high CPU utilization on each AP.
- **Max CPU (%)**—Percentage of high CPU utilization on each AP.

Access Points Impacted by High 2.4 GHz Usage

The **Access Points impacted by high 2.4 GHz usage** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and time of day. It is categorized under wireless quality as the connected clients experience poor Wi-Fi performance. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs experience higher airtime utilization in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

The time series graph displays the number of APs that experience high 2.4 GHz airtime utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number of APs.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 75: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site
Client	Global, Site, Device
RF Info	Global, Site, Device

Site

Lists the number of sites that experience high 2.4 GHz airtime utilization in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Duration (mins)**—Time range that an AP in each site experienced high airtime utilization.
- **Clients**—Number of clients impacted by the insight.

- **APs**—Number of APs impacted by the insight in each site.
- **Reasons**—Cause of the high 2.4 GHz airtime utilization in each site.

Access Point

Lists the number and details of APs that experience high 2.4 GHz airtime utilization in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of the high 2.4 GHz airtime utilization percentage classified by AP models.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Serial**—Serial number of the AP.
- **Consumed Airtime (mins)**—Time range of the consumed airtime in each AP.
- **Duration (mins)**—Time range that the AP experienced high airtime utilization.
- **Reasons**—Cause of the high 2.4 GHz airtime utilization in each AP.
- **Clients Impacted**—Number of clients impacted by the insight connected to each AP.
- **Avg Channel Utilization (%)**—Average percentage of the airtime utilization in each AP.
- **AP Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC Address, name, host name, auth ID, and the corresponding percentage of high 2.4 GHz airtime utilization of each client. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client impacted by the insight and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Duration (mins)**—Time range that the client experienced high airtime utilization.
- **Reason**—Cause of the high 2.4 GHz airtime utilization for each client.
- **Site**—Name of the site where the client exists.

RF Info

Number of channels impacted by high 2.4 GHz airtime utilization. Click the arrow › to view the pictorial graph of the impacted band. Click the **RF Info** drop-down list to view the following:

- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized. Click  to expand the channel data.
- **Reason**—Pictorial graph of the percentage of causes for high 2.4 GHz airtime utilization in a channel.

- **Utilization**—Pictorial graph of the airtime utilization in each AP on a specific date and time. Click  to expand the utilization data.
- **Power Distribution**—Pictorial graph of Tx Power distribution (dBm) for both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client. Click  to expand the power distribution data.
- **Hour of Day**—Pictorial graph of which hours of the day the network was most impacted by excessive AP airtime utilization. Click  to expand the hourly data.
- **SNR Percentile**—Pictorial graph of the average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 2.4 GHz band and 5 GHz band. Click  to expand the SNR percentile data.
- Click the number displayed on the **RF Info** card to view a detailed description of the impacted channels:
- **Channel**—Number of channels that experienced excessive AP airtime utilization.
- **Airtime (mins)**—Time range of the consumed airtime in each client.

Access Points Radios with Frequent Transmit Power Changes

The **Access Point radios changed their transmit power frequently** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information on AP radios that frequently changed transmission power levels in the network. It is categorized under wireless quality since the connected clients experience frequent throughput fluctuations. This insight displays the following information:

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs experience frequent transmit power changes in the network.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.

Time Series Graph

The time series graph displays the number of AP power changes in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number of power changes.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 76: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site
Power	Global, Site, Device

Site

Lists the number of sites that experience power transmit changes in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Insight**—Number of power changes occurred in each site.
- **Radio**—Number of AP radios in each site that changed transmission power level.

Access Point

Lists the number and details of APs that experience power transmit changes in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP insight.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP insight.
- **Serial**—Serial number of the AP.
- **Power Changes**—Number of power changes occurred in each AP.
- **Model**—Model number of each AP.
- **Firmware**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Power

Displays the number of power changes that occurred in APs in the network. Click the arrow › to view the pictorial graph of the impacted band. Click the **Power** drop-down list to view the following:

- **Power Changes over Time**—Pictorial graphs of power transmit changes observed across time for 2.4 GHz and 5 GHz radio. Click  to expand the power change data.
- **Power Distribution**—Pictorial graph of the percentage of time spent across power levels for the time period in the 2.4 GHz and 5 GHz band. Click  to expand the power distribution data.
- **Band**—Pictorial graph of the percent of number of changes observed in the 2.4 GHz and 5 GHz bands.
- **Variance**—Pictorial graph of the percentage of variance in transmission power across number of APs in that power variance for the 2.4 GHz and 5 GHz band. Click  to expand the variance data.

Click the number displayed on the **Power** card to view a detailed description of the impacted channels:

- **Band**—Number of power changes observed in the 2.4 GHz and 5 GHz bands.
- **Changes**—Number of power changes that occurred in each band.

Access Point Transmit Power can be Optimized

The **Access Point transmit power can be optimized** insight can be accessed only at the **Global**context. This insight generates when the transmit power is not set optimally on the radios of access points existing in the network. This insight detects that wireless clients are experiencing a poor Wi-Fi connectivity due to the transmit power settings of the access points. It is categorized under wireless quality as the clients connected to these APs can communicate with the APs well but, the APs have difficulty to communicate with the clients in return. This insight displays the following information:

- Insight Summary
- Card

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the transmit power of APs are not set optimally.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Card

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 77: *Cards*
Context

Cards	Context
Mixed	Global
Power	Global

Mixed

Number of channels in the APs impacted by transmit power setting in the network. Click the arrow › to view the pictorial graph of the impacted band. Click the **Mixed** drop-down list to view the following:

- **Band**—Pictorial graph of power changes in both the frequency bands by the AP (2.4 GHz or 5 GHz).
- **SSID**—Pictorial graph of the percent of AP dwell bands (2.4 GHz or 5 GHz) sorted by SSIDs. Click  to expand the SSID data.

Power

Displays the number of power changes that occurred in a specific access point. Click the arrow › to expand the card to view the pictorial graph of the band and power distribution in the network. Click the **Power** drop-down list, to view the following:

- **Power Distribution**—Pictorial graph of the percentage of time spent across power levels for the time period in the 2.4 GHz and 5 GHz band.
- **Band**—Graph of the percent of number of changes observed in the 2.4 GHz and 5 GHz bands.

Click the number displayed on the **Power** card, to view a detailed description of the impacted clients:

- **Band**—Band where the maximum power changes occurred.
- **Changes**—Number of power changes that occurred in each band.

Access Points Impacted by High 5 GHz Usage

The **Access Points were impacted by high 5 GHz usage** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and time of day. **Access Points were impacted by high 5 GHz usage** is categorized under wireless quality as the connected clients experience poor Wi-Fi performance. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs experience higher airtime utilization in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

The time series graph displays the number of APs that experience high 5 GHz airtime utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number of APs.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 78: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site
Client	Global, Site, Device
RF Info	Global, Site, Device

Site

Lists the number of sites that experience high 5 GHz airtime utilization in the network. Click the arrow to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Duration (mins)**—Time range that an AP in each site experienced high airtime utilization.
- **APs**—Number of APs impacted by the insight in each site.
- **Clients**—Number of clients impacted by the insight.
- **Reason**—Cause of the high 5 GHz airtime utilization in each site.

Access Point

Lists the number and details of APs that experience high 5 GHz airtime utilization in the network. Click the arrow to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of the high 5 GHz airtime utilization percentage classified by AP models. Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:
- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Serial**—Serial number of the AP.
- **Consumed Airtime (mins)**—Time range of the consumed airtime in each AP.
- **Duration (mins)**—Time range that the AP experienced high airtime utilization.
- **Reason**—Cause of the high 5 GHz airtime utilization in each AP.
- **Clients Impacted**—Number of clients impacted by the insight connected to each AP.
- **Avg Channel Utilization (%)**—Average percentage of the airtime utilization in each AP.
- **AP Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC Address, name, host name, auth ID, and the corresponding percentage of high 5 GHz airtime utilization for each client. Click the arrow to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client impacted by the insight and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Duration (mins)**—Time range that the client experienced high airtime utilization.
- **Reason**—Cause of the high 5 GHz airtime utilization for each client.
- **Site**—Name of the site where the client exists.

RF Info

Number of channels impacted by high 5 GHz airtime utilization. Click the arrow to view the pictorial graph of the impacted band. Click the **RF Info** drop-down list to view the following:

- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized. Click  to expand the channel data.
- **Reason**—Pictorial graph of the percentage of causes for high 5 GHz airtime utilization in a channel.
- **Utilization**—Pictorial graph of the airtime utilization in each AP on a specific date and time. Click  to expand the utilization data.
- **Power Distribution**—Pictorial graph of Tx Power distribution (dBm) for both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client. Click  to expand the power distribution data.
- **Hour of Day**—Pictorial graph of which hours of the day the network was most impacted by excessive AP airtime utilization. Click  to expand the hourly data.
- **SNR Percentile**—Pictorial graph of the average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 5 GHz band. Click  to expand the SNR percentile data.
- Click the number displayed on the **RF Info** card to view a detailed description of the impacted channels:
- **Channel**—Number of channels that experienced excessive AP airtime utilization.
- **Airtime (mins)**—Time range of the consumed airtime in each client.

Access Points with High Memory Usage

The **Access Points with unusually high memory usage were found** insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about APs that have higher than normal memory utilization and is categorized under availability as the clients connected to these APs experience intermittent connectivity drops. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

The time series graph displays the number of APs that experience high memory utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number of APs.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 79: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience high memory utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **APs with High Memory**—Number of APs that experience high memory utilization in each site.
- **Minutes with High Memory**—Time range of high memory utilization in each site.

Access Point

Lists the number and details of APs that experience high memory utilization in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **AP Model**—Pictorial graph of memory utilization classified by AP models.
- **FW Version**—Pictorial graph of memory utilization classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP.
- **AP Serial**—Serial number of the AP.
- **Firmware**—Version of the firmware running on each AP.
- **Model**—Model number of each AP.
- **Site**—Name of the site where the AP resides.
- **Time (min)**—Time range of high memory utilization on each AP.
- **Max Memory (%)**—Percentage of high memory utilization on each AP.

Clients with High Roaming Latency

The **Clients experienced high latency while roaming** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides reports on wireless clients that have experienced long roam times to the target AP. The threshold to detect a delayed and long client roaming is set to 50 ms and all the data and analysis pattern is perceived from the target AP issues if you access this insight from the global, site, or client context. When you access this insight from device context, data is received from the home AP issues. **Clients experienced high latency while roaming** is categorized under connectivity since it helps the network administrators to take necessary actions if there are any clients experiencing long delays to roam between APs. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

The time series graph displays the total number of roams and the percentage of high latency roams that occurred in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number and percentage of roams.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 80: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device
Roam	Global, Site, Device, Client

Site

Lists the number of sites where the clients have experience high roaming latency in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **High Latency Roams (%)**—Number and percentage of high latency roams in each site.
- **Impacted Clients Count**—Number of clients impacted with high roaming latency in each site.

Access Point

Lists the number and details of APs where the clients have experience high roaming latency. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of high roaming latency classified by AP models.
- **FW Version**—Pictorial graph of high roaming latency classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **Serial**—Serial number of the AP.
- **High Latency Roams (%)**—Number and percentage of high latency roams in each AP.
- **Clients From**—Number of clients that roamed in each AP.
- **Latency (min/avg/max) msec**—The minimum, average, and maximum latency that occurred in each AP.
- **AP MAC**—MAC address of the impacted AP and link to the specific insight at the AP context.
- **IP**—IP address of the impacted AP.
- **Model**— Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC Address, name, host name, auth ID, and the number of clients that have experience high roaming latency. Click the arrow to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted clients and link to the specific insight at the client context.
- **Client MAC**—MAC address of the impacted client and link to the specific insight at the client context.
- **High Latency Roams (%)**—Number and percentage of high latency roams in each client.
- **Top AP**— AP where the client roamed maximum as compared to other APs in the network.

Roam

Displays the percentage of client latency roams in the network. This card includes the raw telemetry feed sorted based on latency at each context.

Click the arrow to expand the **Roam** card and click the drop-down list, to view the following:

- **Latency**—Pictorial graph of latency versus concurrences. Click to expand the latency data.
- **Band**—Pictorial graph of clients roaming trends between 2.4 GHz and 5 GHz.

Click the number displayed on the **Roam** card, to view a detailed description of the impacted clients:

- **Timestamp**—Timestamp of the event received.
- **Latency (msec)**—Latency value in microsecond per client.
- **Client Name**—Name of the roaming client and link to the specific insight at the client context.
- **Client MAC**—MAC Address of the roaming client and link to the specific insight at the client context.
- **From AP Name**—Name of the home AP from the where the client roamed to the target AP.
- **To AP Name**—Name of the target AP to where the client roamed from the home AP.
- **From Channel**—Number of channel the client roamed from.
- **Roaming Type**—Type of the roam that occurred in each client.
- **From AP MAC**—MAC address of the home AP from the where the client roamed to the target AP.
- **From AP Serial**—Serial number of the home AP from the where the client roamed to the target AP.
- **To AP MAC**—MAC address of the target AP to where the client roamed from the home AP.
- **To AP Serial**—Serial number of the target AP to where the client roamed from the home AP.
- **RSSI (dBm)**—Received Signal Strength Indicator (RSSI) value of the client.
- **To Channel**—Number of channels the client roamed to.

Clients with Low SNR Minutes

The **Clients had a significant number of Low SNR minutes** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information about access points that have a low-quality signal-strength connection and is categorized under wireless quality as the clients connecting at a Low SNR have low throughput and high retransmissions. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the APs experience low-quality SNR connection in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

The time series graph displays the number of clients with low SNR uplink AP during the selected time period. You can hover your mouse on each bar graph to see the number of SNR links.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 81: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device
RF Info	Global, Site, Device

Site

Lists the number of sites where the APs and clients experience low signal connection. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **APs with Low SNR**—Number of APs with low signal connection.
- **Clients with Low SNR**—Number of clients with low signal connection.
- **Uplink Minutes of Low SNR**—Duration of uplink with low signal connection in each site.
- **Downlink Minutes of Low SNR**—Duration of downlink with low signal connection in each site.

Access Point

Lists the number and details of APs that experience low signal connection in the network. Click the arrow › to view the pictorial graph of the **Most Impacted**access points. Click the **Access Point** drop-down list, to view the following:

- **TX Power**—Pictorial graph of the percentage of Tx Power distribution (dBm) in both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the **Access Point Details** page.
- **AP MAC**—MAC address of the AP and link to the **Access Point Details** page.
- **Serial**—Serial number of the AP
- **AP Model**—Model number of each AP.
- **Clients**—Number of clients that experience low signal connection in each AP.
- **Uplink Low SNR (Total|2.4 GHz|5 GHz|min)**—Duration of uplink with low signal minutes in both bands during the time it is transmitting signal to the AP.
- **Downlink Low SNR (Total|2.4 GHz|5 GHz|min)**—Duration of downlink with low signal connection in both the bands during the time it is transmitting signal to the AP.

Client

Lists the MAC Address, name, host name, auth ID, and the number of clients experiencing low signal quality.

Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the **Client** drop-down list, to view the following:

- **Client Type**—Pictorial graph of the number and percentage of low SNR clients classified by vendors.

Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Number of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Type**—Device type of the client.
- **Uplink Minutes of Low SNR**—Duration of uplink with low signal connection in each client.
- **Uplink Low SNR (Total|2.4 GHz|5 GHz|min)**—Duration of uplink with low signal minutes in both bands during the time it is transmitting signal to the AP.
- **Downlink Low SNR (Total|2.4 GHz|5 GHz|min)**—Duration of downlink with low signal connection in both the bands during the time it is transmitting signal to the AP.
- **Site**—Name of the site where the client resides.

RF Info

Number of channels impacted by low-quality signal-strength connection in the network. Click the arrow › to view the pictorial graph of the impacted band. Click the **RF Info** drop-down list to view the following:

- **Band**— Pictorial graph of devices experiencing a low signal-quality link using 2.4 GHz or 5 GHz radio bands.
- **Good vs Bad**—Pictorial graph of the amount of time (minutes) with Low SNR (Bad) and High SNR (Good) for all the clients.

Click the number displayed on the **RF Info** card to view a detailed description of the impacted channels:

- **Band**—Number of channel changes between 2.4 GHz and 5 GHz.
- **Time (min)**—Number of power changes.

Clients with High MAC Authentication Failures

The **Clients had an unusual number of MAC authentication failures** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on excessive MAC authentication failures observed in the network and is categorized under connectivity as the users are

unable to connect to the Wi-Fi network. It also helps in order to identify the rogue users in a network. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of MAC authentication failures that occurred during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 82: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced MAC authentication failures in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Failures**—Number of failures occurred in each site.
- **Total**—Total number of MAC authentication in each site.

Access Point

Lists the number and the details of APs that faced the MAC authentication failures in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of MAC authentication failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of MAC authentication failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of MAC authentication failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **MAC**—MAC address of the access point and link to the specific insight at the AP context.
- **Failures**—Number of failures occurred in each AP.
- **Total**—Total number of MAC authentication in each AP.
- **Serial**—Serial number of the AP
- **IP**—IP address of each AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that failed MAC authentication. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Name**—Name of the impacted client and link to the specific insight at the client context.
- **MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number of failures occurred in each client.
- **Client OS**—OS type of the device.

Clients with DHCP Server Connection Problems

The **Clients had DHCP server connection problems** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on excessive client to AP DHCP failures observed in the network. This insight occurs when Wi-Fi clients attempt to acquire a DHCP IP address multiple times but fails to do so. It is insight is categorized under connectivity since the users fail to get an IP address and are unable to connect to the Wi-Fi network. It displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of DHCP failures that occurred during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 83: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device, Client
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experience DHCP server connection problems in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of DHCP requests.

Server

Lists the number of DHCP servers involved in this insight. Click the arrow › to view the pictorial graph of the**Most Impacted** sites. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of the server impacted by this insight.
- **Failures**—Number of failures occurred in each server.
- **Total**—Total number of DHCP requests.

Access Point

Lists the number and the details of the DHCP server connection problems observed in an AP. Click the arrow › to view a pictorial graph of the **Most Impacted**access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of DHCP failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of DHCP failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of DHCP failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of DHCP requests.
- **Serial**—Serial number of the AP
- **IP**—IP address of each AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Site name of the AP where the failure occurred.

Client

Lists the MAC address, host name, and auth ID of clients that failed DHCP handshake. Click the arrow  to view the pictorial graph of the **Most Impacted**clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number of failures occurred in each client.
- **Total**—Total number of DHCP requests.
- **Client OS**—OS type of the device.

Clients with High 802.1X Authentication Failures

The **Clients had excessive 802.1x authentication failures** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on excessive 802.1X authentication failures observed in the network. It is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of 802.1X authentication failures observed in the network during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 84: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device, Client
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced 802.1X authentication failures in the network. Click the arrow › to view a pictorial graph with the **Most Impacted**sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and lick to the specific insight at the site context.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of 802.1X authentication in each site.

Server

Lists the number of servers that failed 802.1X authentication in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of each server.
- **Failures**—Number of 802.1X authentication failures in each server.
- **Total**—Total number of 802.1X authentication.

Access Point

Lists the number and the details of APs that failed 802.1X authentication in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of 802.1X authentication failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of 802.1X authentication failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of 802.1X authentication failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that failed 802.1X authentication. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

Clients with High Wi-Fi Security Key-Exchange Failures

The **Clients had excessive Wi-Fi security key-exchange failures** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on excessive Wi-Fi security key-exchange failures observed in the network. When this failure occurs, users connecting to Wi-Fi using PSK or 802.1x authentication, experience higher EAPOL Key exchange failures. This insight is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes of Wi-Fi security key-exchange failure in the network.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of Wi-Fi security key-exchange failures that occurred in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number of failures. The following graph shows data trend for 3 hours in a day.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 85: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced excessive Wi-Fi security key-exchange failures in the network.

Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of failures in each site.

Access Point

Lists the number APs that experienced Wi-Fi security key-exchange failures in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **SSID**: Pictorial graph of 4-way handshake authentication failures sorted by SSIDs.
- **Model**: Pictorial graph of 4-way handshake failures classified by AP models.
- **FW Version**: Pictorial graph of 4-way handshake failures classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC Address, name, host name, and auth ID of clients that failed Wi-Fi security key-exchange authentication. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the

number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

Clients with Captive Portal Authentication Problems

The **Clients had problems authenticating with the Captive Portal** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on captive portal failures observed in the network. It is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of client captive portal failures observed in the network during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 86: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced captive portal failures in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed

description of the impacted sites:

- **Site**—Name of the site impacted by the insight.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of captive portal authentication in each site.

Access Point

Lists the number and the details of APs that failed captive portal authentication in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of captive portal authentication failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of captive portal authentication failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of captive portal authentication failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that failed captive portal authentication.

Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

Clients with High Number of Wi-Fi Association Failures

The **Clients had a high number of Wi-Fi Association failures** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on Wi-Fi association failures observed in the network. It is categorized under connectivity since the users are unable to connect to the WiFi network. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of association failures observed in the network during the selected time period. You can hover your mouse over each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 87: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites that experienced association authentication failures in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight.
- **Failures**—Number and percentage of failures occurred in each site.
- **Total**—Total number of association failures in each site.

Access Point

Lists the number and the details of APs that experienced association failures in the network. Click the arrow › to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **SSID**—Pictorial graph of the percentage of association failures sorted by SSIDs.
- **Model**—Pictorial graph of the percentage of association failures sorted by AP models.
- **FW Version**—Pictorial graph of the percentage of association failures sorted by AP firmware version.

Click the number displayed on the **Access Point** card, to view the detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP link to the specific insight at the AP context.
- **Failures**—Number and percentage of failures occurred in each AP.
- **Total**—Total number of failures in each AP.
- **Serial**—Serial number of the AP.
- **IP**—IP address of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC address, name, host name, and auth ID of clients that experienced association failures in the network. Click the arrow  to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Failures**—Number and percentage of failures occurred in each client.
- **Total**—Total number of failures in each client.
- **Client OS**—OS type of the device.

Clients who Roamed Excessively

The **Clients roamed excessively** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides reports on wireless clients that roam to the target APs more than normal from the home AP. This insight is categorized under connectivity since this helps to reduce the frequency of roaming clients in the customer network. It also helps network administrators to eliminate anonymous users and deploy additional access points in case the users get effected due to poor network performance. This insight displays the following information:

Time Series Graph

The time series graph displays the total number of roams and the percentage of excessive roams that occurred in the network during the selected time period. You can hover your mouse on each bar graph to see the exact number and percentage of roams.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 88: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site, Client
Client	Global, Site, Device

Site

Lists the number of sites where the clients have experience excessive roams in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Impacted Clients (%)**—Number and percentage of clients impacted with excessive roaming in each site.

Access Point

Lists the number and details of APs where the clients have experience excessive roams. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **Model**—Pictorial graph of excessive roams classified by AP models.
- **FW Version**—Pictorial graph of excessive roams classified by AP firmware versions.

Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **From AP**—The AP name from where the client roamed excessively.
- **Impacted Clients (%)**—Clients impacted by excessive roams in each AP.
- **AP MAC**—MAC address of the APs and link to the specific insight at the AP context.
- **Serial**—Serial number of the AP.
- **IP**—IP Address of each AP.
- **Model**— Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Client

Lists the MAC Address, name, host name, auth ID, and the number of clients that have experience high roaming latency. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the clients impacted by the insight and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client impacted by the insight and link to the specific insight at the client context.
- **Excessive Roams**—Number of excessive roams for each client.

- **Delayed Roams**—Number of delayed roams by the client.
- **Top AP**—AP where the client roamed maximum as compared to other APs in the network.

Coverage Holes Identified

The **Coverage Hole detected** insight can be accessed only at the **Global** context. This insight determines the connection status of Wi-Fi clients with the APs due to poor Wi-Fi coverage. Machine learning determines when a relatively large proportion of the client minutes that consistently have low SNR links. The exact location of the coverage hole can be identified from the location of the clients listed with poor coverage and implies that there is a need to deploy one more AP which will avoid the low SNR clients in the network. **Coverage Hole detected** is categorized under wireless quality since the clients in coverage holes have poor or intermittent Wi-Fi connectivity causing loss of productivity. This insight displays the following information:

- Insight Summary
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the clients experience poor Wi-Fi coverage in the network.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 89: *Cards Context*

Cards	Context
Site	Global
Access Point	Global
Client	Global

Site

Lists the sites where the clients experience poor Wi-Fi coverage in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites.

Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Clients**—Number of clients that experience coverage hole in each site.
- **Coverage Holes**—Total number clients that needs to be deployed in the network due to coverage holes.

Access Point

Lists the number and details of APs which has clients with poor connections due to a coverage hole in the network. This is measured by the amount of time the client experiences poor vs good connectivity. Click the arrow to view the pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list, to view the following:

- **Most Impacted by Low Uplink SNR**—Pictorial graph of APs impacted maximum by low uplink SNR.
- **Most Impacted by Low 5 GHz Downlink SNR**—Pictorial graph of APs impacted maximum by low 5 GHz downlink SNR.
- **Most Impacted by Low 2.4 GHz Downlink SNR**—Pictorial graph of APs impacted maximum by low 2.4 GHz downlink SNR.

Click the number displayed on the **Access Point** card, to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of each AP and link to the specific insight at the AP context.
- **Impacted (Time)**—Time range of the coverage hole detected in each AP.
- **Clients**—Number of clients with poor Wi-Fi coverage in each AP.
- **Coverage Hole Type**—The type of coverage hole detected in each AP.
- **AP Serial**—Serial number of each AP.
- **Firmware**—Version of the firmware running on each AP.
- **Model**—Model number of each AP.

Client

Lists the MAC Address, name, host name, auth ID, and the number of connected clients affected by poor connections determined by the total number of minutes spend in the coverage hole. Click the arrow to view the pictorial graph of the **Most Impacted** clients. Click the **Client** drop-down list, to view the following:

- **Low Uplink SNR Minutes**—Pictorial graph of clients impacted maximum by low uplink SNR minutes.
- **Low 5 GHz Downlink SNR**—Pictorial graph of clients impacted maximum by low 5 GHz downlink SNR.
- **Low 2.4 GHz Downlink SNR**—Pictorial graph of clients impacted maximum by low 2.4 GHz downlink SNR.

Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the client and link to the specific insight at the client context.
- **Impacted (Time)**—Time range of the coverage hole detected in each client.
- **Client OS**—Operating system of the client.
- **Average SNR (dB)**—Average SNR of the client on the AP.
- **Coverage Hole Type**—The type of coverage hole detected in each AP.

Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz

The **Dual-band (2.4/5 GHz) capable clients primarily used 2.4 GHz** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provide reports on Dual band capable clients

that spent more airtime on 2.4 GHz band instead of 5 GHz band. **Dual-band (2.4/5 GHz) capable clients primarily used 2.4 GHz** is categorized under wireless quality since the 2.4 GHz band has more interference, more clients, and less bandwidth capabilities than the 5 GHz band. Dual-band clients have a better user experience when they are on the 5 GHz band. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the client is excessively dwelling in the 2.4 GHz band in the network.
- **Recommendation**—Displays the recommendation against each cause to resolve the same.

Time Series Graph

The time series graph displays the percentage of clients over dwelling in the 2.4 GHz band in the network during the selected time period. You can hover your mouse on each bar graph to see the exact percentage of the dwelling time.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 90: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site
Client	Global, Site, Device

Site

Lists the number of sites where the clients are dwelling excessively in the 2.4 GHz band. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Clients Impacted**—Number of clients in each site that is excessively dwelling in the 2.4 GHz band.
- **APs Impacted**—Number of APs impacted by the insight in each site.

Access Point

Lists the number and details of APs where the clients are dwelling excessively in the 2.4 GHz band. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the number displayed on the **Access Point** card to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP.
- **Serial**—Serial number of the AP.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.
- **Total Clients**—Total number of clients connected to each AP.
- **Clients (%)**—Number of clients that is dwelling excessively on 2.4 GHz band.

Client

Lists the MAC Address, name, host name, auth ID, and the corresponding percentage of time spent for each client in the radio bands. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the **Client** drop-down list, to view the following:

- **Client Type**—Pictorial graph of the percent of clients dwelling in the 2.4 GHz band sorted by client device type.

Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Name of the client impacted by the insight.
- **Client MAC**—MAC address of the client impacted by the insight and link to the specific insight at the client context.
- **Device Type**—Clients dwelling in the 2.4 GHz band sorted by client device type.
- **Site**—Name of the site where the client resides.
- **2.4 GHz Dwell (min, %)**—Duration and percentage of time of each client dwelling in the 2.4 GHz band.
- **5 GHz Dwell (min, %)**—Duration and percentage of time of each client dwelling in the 5 GHz band.
- **Total Dwell Minutes**—Total duration of each client dwelling on both the bands.

Delayed DNS Request or Response

The **DNS request/responses were significantly delayed** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on significant delays in response from the DNS servers. It is categorized under connectivity since there is a high delay in response from the DNS server. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

The time series graph displays the number of delays from the DNS server that occurred during the selected time. You can hover your mouse on each bar graph to see the exact number of delays.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 91: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device
Access Point	Global, Site

Site

Lists the number sites that experience delays from the DNS server in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Min (ms)**—Packet latency (delay) is measured. The lowest value of delay in the measurement interval is the minimum response delay.
- **Avg (ms)**—Packet latency (delay) is measured. The average value of delay in the measurement interval is the minimum response delay.
- **Max (ms)**—Packet latency (delay) is measured. The maximum value of delay in the measurement interval is the maximum response delay.

Server

Lists the number of DNS servers that is impacted by this insight. Click the arrow › to view the pictorial graph of the **Most Impacted** servers. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of each server.
- **Avg (ms)**—Packet latency (delay) is measured. The average value of delay in the measurement interval is the minimum response delay.
- **Min (ms)**—Packet latency (delay) is measured. The lowest value of delay in the measurement interval is the minimum response delay.
- **Max (ms)**—Packet latency (delay) is measured. The maximum value of delay in the measurement interval is the maximum response delay.

Access Point

Lists the number and details of APs that has the most DNS response delays. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the number displayed on the **Access Point** card, to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **AP Serial**—Serial number of the AP.
- **Avg (ms)**—Packet latency (delay) is measured. The average value of delay in the measurement interval is the minimum response delay.

- **Min (ms)**—Packet latency (delay) is measured. The lowest value of delay in the measurement interval is the minimum response delay.
- **Max (ms)**—Packet latency (delay) is measured. The maximum value of delay in the measurement interval is the maximum response delay.
- **Servers**—Server ID where the AP resides.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

DNS Servers Rejected High Number of Queries

The **DNS server(s) rejected a high number of queries** insight can be accessed from the **Global**, **Site**, **Access Points**, and **Clients** context. This insight provides information on excessive request failures from the DNS servers. It is categorized under connectivity since there is a high number of request failures. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.
- **Failures**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

The time series graph displays the number of request failures from the DNS server that occurred during the selected time. You can hover your mouse on each bar graph to see the exact number of failures.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 92: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device
Access Point	Global, Site

Site

Lists the number sites that experience request failures from the DNS server in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Total Failures(%)**—Total number of failure packets at the site multiplied by 100.
- **Query Attempts**—Number of query attempts sent to the DNS server in a site.
- **Query Success(%)**—Percentage of successful DNS queries in a site.
- **Query Format Error**—Error in the DNS query format sent to the DNS server in a site.
- **Request Failed to Complete**—DNS request failed to complete, and the server responds with an error code.
- **Domain Name Does Not Exist**—Domain name sent to the DNS server does not exist and the server responds with an error code
- **Function Not Implemented**—Function is not implemented on the DNS server and the server responds with an error code.
- **Server Refused to Answer Query**—Server refused to answer the query and responds with an error code.

Server

Lists the number of servers that has the most number of DNS request rejections. Click the arrow › to view the pictorial graph of the **Most Impacted** servers. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of each server.
- **Total Failures(%)**—Total number and percentage of failure packets at the site multiplied by 100.
- **Query Attempts**—Number of query attempts sent to the DNS server.
- **Query Success(%)**—Percentage of successful DNS queries.
- **Query Format Error**—Error in the DNS query format sent to the DNS server in a site.
- **Request Failed to Complete**—DNS request failed to complete, and the server responds with an error code.
- **Domain Name Does Not Exist**—Domain name sent to the DNS server does not exist and the server responds with an error code
- **Function Not Implemented**—Function is not implemented on the DNS server and the server responds with an error code.
- **Server Refused to Answer Query**—Server refused to answer the query and responds with an error code.

Access Point

Lists the number and details of access points that has the most number of DNS request rejections. Click the arrow › to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **Success Rate**—Graphical representation of the total failures and total successful requests that occurred at the server.

Click the number displayed on the **Access Point** card, to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **AP Serial**—Serial number of the AP.
- **Total Failures(%)**—Total number and percentage of failure packets at the site multiplied by 100.
- **Query Attempts**—Number of query attempts sent to the DNS server in each AP.
- **Query Success(%)**—Percentage of successful DNS queries in each AP.
- **Query Format Error**—Error in the DNS query format sent to the DNS server in each AP.
- **Request Failed to Complete**—DNS request failed to complete, and the server responds with an error code.
- **Domain Name Does Not Exist**—Domain name sent to the DNS server does not exist and the server responds with an error code
- **Function Not Implemented**—Function is not implemented on the DNS server and the server responds with an error code.
- **Server Refused to Answer Query**—Server refused to answer the query and responds with an error code.
- **Site**—Name of the site where the AP resides.

Gateways with High Memory Usage

The **Gateways had high Memory usage** insight can be accessed from the **Global**, **Site**, and **Gateways** context. This insight provides information about gateways that have higher than normal memory utilization. It is categorized under availability since the clients connected to these gateways experience intermittent connectivity drops. This insight displays the following information:

Time Series Graph

The time series graph displays the percentage of impacted in the network during the selected time period. You can hover your mouse on each bar graph to see the percentage of impacted gateways.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 93: *Cards Context*

Cards	Context
Site	Global
Gateway	Global, Site
Memory	Device

Site

Lists the number of sites where the gateways experience high memory utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Number of Gateways**—Number of gateways that experience high memory utilization in each site.
- **Duration (mins)**—Amount of time (minutes) high memory utilization observed in each site.

Gateway

Lists the number and details of gateways that experience high memory utilization in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** gateways. Click the **Gateway** drop-down list, to view the following:

- **Gateway Model**—Pictorial graph of memory utilization classified by gateway models.
- **FW Version**—Pictorial graph of memory utilization classified by gateway firmware versions.
- **Mode**—Operational mode of the gateway.

Click the number displayed on the **Gateway** card to view a detailed description of the impacted gateways:

- **Serial**—Serial number of each gateway and link to the specific insight at the gateway context.
- **Gateway Name**—Name of the gateway that experience high memory utilization.
- **Mode**—Operational mode of the mode.
- **Max Memory**—Maximum memory consumed by the gateway.
- **Minutes with High Memory**—Amount of time (minutes) high memory utilization observed in each gateway.
- **Model**—Model number of each gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.

Memory

Memory card is displayed only when this insight is accessed from the device context. Click the arrow › to expand the card and view the graphical representation of the time series of memory utilization percentage in the selected gateway.

Gateways with High CPU Utilization

The **Gateways had unusually high CPU utilization** insight can be accessed from the **Global**, **Site**, and **Gateways** context. This insight provides information about gateways that have higher than normal CPU utilization. It is categorized under availability since the clients connected to these gateways experience intermittent connectivity drops. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

The time series graph displays the percentage of impacted gateways in the network during the selected time period. You can hover your mouse on each bar graph to see the percentage of impacted gateways.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 94: *Cards Context*

Cards	Context
Site	Global
Gateway	Global, Site
CPU	Device

Site

Lists the number of sites where the gateways experience high CPU utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Number of Gateways**—Number of gateways that experience high CPU utilization in each site.
- **Duration (mins)**—Amount of time (minutes) high CPU utilization observed in each site.

Gateway

Lists the number and details of gateways that experience high CPU utilization in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** gateways. Click the **Gateway** drop-down list, to view the following:

- **Gateway Model**—Pictorial graph of CPU utilization classified by gateway models.
- **FW Version**—Pictorial graph of CPU utilization classified by gateway firmware versions.
- **Mode**—Operational mode of the gateway.

Click the number displayed on the **Gateway** card to view a detailed description of the impacted gateways:

- **Serial**—Serial number of each gateway and link to the specific insight at the gateway context.
- **Gateway Name**—Name of the gateway that experience high CPU utilization.
- **Mode**—Operational mode of the gateway.
- **Max CPU**—Rate of maximum CPU utilization observed in each gateway.
- **Minutes with High CPU**—Amount of time (minutes) high CPU utilization observed in each gateway.
- **Model**—The hardware model of each gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.

CPU

CPU card is displayed only when this insight is accessed from the device context. Click the arrow › to expand the card and view the graphical representation of the time series of CPU utilization percentage in the selected gateway.

Failure to Establish Gateway Tunnels

The **Gateway tunnels failed to get established** insight can be accessed from the **Global**, **Site**, and **Gateways** context. This insight provides information about gateway tunnels that are marked down in the network. It is categorized under availability since the clients connected to these gateways experience connectivity drops.

Gateway Tunnels Down insight is available for branch and VPNC gateways in the network.

Tunnels are marked down in the network based on the following scenarios:

- If Aruba Central receives telemetry from branch gateway that a specific tunnel is down
- If Aruba Central receives telemetry from the VPNC that a specific tunnel is down
- Lack of telemetry from both branch and VPNC gateway

This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for tunnel down in the network.
- **Minutes Down**—Displays the exact number and percentage of tunnel down that occurred against each failure reason.

Time Series Graph

The time series graph displays the percentage and number of tunnels down in the network during the selected time period. You can hover your mouse on each bar graph to see the exact percentage of tunnels down.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 95: *Cards Context*

Cards	Context
Site	Global

Cards	Context
Gateway	Global, Site
VPNC	Global, Site, Device
Tunnel	Global, Site, Device

Site

Lists the number of sites where the gateways experience tunnel down. Click the arrow › to expand the card and click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight.
- **Number of Down Tunnels**—Number of tunnels down in each site that experience high memory utilization in each site.
- **Total Tunnels**—Total number of gateway tunnels in each site.
- **Number of Impacted Gateways**—Number of gateways impacted by tunnel down in each site.
- **Number of Impacted VPNC**—Number of VPNC gateways that experience tunnel down in each site.

Gateway

Lists the number and the reason for the cause of tunnel down in gateways. Click the arrow › to expand the card and click the number displayed on the **Gateway** card to view a detailed description of the impacted gateways:

- **Serial**—Serial number of each gateway and link to the **Gateway Details** page.
- **Gateway Name**—Name of the gateway that experience tunnel down.
- **Mode**—Operational mode of the gateway.
- **Number of Tunnels**—Number of tunnels down in each gateway.
- **Total Tunnels**—Total number tunnels in each gateway.
- **Duration (mins)**—Time range of tunnel down in each gateway.
- **Model**—The hardware model number of the gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.

VPNC

Displays the total number of VPNC gateways experiencing tunnel down. Click the arrow › to expand the card and view the amount of time (minutes) and the reasons for the cause of down tunnels on the VPNC gateways.

Click the number displayed on the **VPNC** card to view a detailed description of the impacted VPNC gateways:

- **Serial**—Serial number of each gateway and link to the specific insight at the gateway context.
- **Gateway Name**—Name of the gateway that experience tunnel down.
- **Mode**—Operation mode of the VPNC.
- **Total Number of Tunnels Down**—Number of tunnels down in each gateway.

- **Total Number of Tunnels**—Number of tunnels down in each gateway.
- **Number of Gateways**—Number of gateways impacted by tunnel down.
- **Number of Sites**—Number of site impacted by tunnel down.
- **Duration (mins)**—Time range of tunnel down in each gateway.
- **Model**—The hardware model number of the gateway.
- **FW Version**—Version of the firmware running on each gateway.
- **Site**—Name of the site where the gateway resides.

Tunnel

Displays the total number of gateways experiencing tunnel down. Click the arrow › to expand the card to view the amount of time (minutes) and the reasons for the cause of tunnel down in the network.

Click the number displayed on the **Tunnel** card to view a detailed description of the impacted tunnels:

- **Site**—Name of the site where the tunnel resident and link to the specific insight at the site context.
- **Gateway IP**—IP address of the impacted gateway.
- **VPNC IP**—IP address of the impacted VPNC gateway.
- **Duration (mins)**—Time range of tunnel down.
- **Gateway VLAN**—VLAN ID of the gateway.
- **VPNC VLAN**—VLAN ID of the VPNC.
- **Gateway Name**—Name of the gateway where the tunnel is down.
- **Gateway MAC**—MAC address of the impacted gateway.
- **VPNC Name**—Name of the VPNC gateway where the tunnel is down.
- **VPNC MAC**—MAC address of the impacted VPNC gateway.
- **Gateway Serial**—Serial number of the gateway and link to the specific insight at the gateway context.
- **VPNC Serial**—Serial number of VPNC gateway.

DNS Queries Failed to Reach or Return from the Server

The **DNS queries failed to reach or return from the server**insight can be accessed from the **Global**, **Site**, and **Access Points** context. This insight provides information about wireless APs that experience a higher than normal number of connection failures with the DNS server. It is categorized under connectivity since the wireless clients are unable to reach the destination URL. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the possible recommendation against each failure to resolve the same.

Time Series Graph

The time series graph displays the number of connection loss with the DNS server that occurred during the selected time. You can hover your mouse on each bar graph to see the exact number of loss.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 96: *Cards Context*

Cards	Context
Site	Global
Server	Global, Site, Device
Access Point	Global, Site

Site

Lists the number sites that experience connection loss with the DNS server in the network. Click the arrow › to view the pictorial graph of the **Most Impacted**sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Lost DNS Queries (%)**—Total count of the DNS packets that get lost in the network. DNS server does not receive these packets.
- **Total Queries**—Total number of successful DNS queries, denied DNS queries, and lost queries in the DNS server.

Server

Lists the number of servers that have higher number of DNS connection failures in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** servers. Click the number displayed on the **Server** card, to view a detailed description of the impacted servers:

- **Server IP**—IP address of each server.
- **Lost DNS Queries (%)**—Total count of the DNS packets that get lost in the network. DNS server does not receive these packets.
- **Total Queries**—Total number successful DNS queries, denied DNS queries, and lost queries in the DNS server.

Access Point

Lists the number and details of APs that have higher number of DNS connection failures in the network.

Click the arrow › to view a pictorial graph of the **Most Impacted** access points. Click the **Access Point** drop-down list to view the following:

- **Success Rate**Graphical representation of the total failures and total successful requests that occurred at the AP.

Click the number displayed on the **Access Point** card, to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **AP Serial**—Serial number of the AP.
- **Lost DNS Queries (%)**—Total count of the DNS packets that get lost in the network. DNS server does not receive these packets.
- **Total Queries**—Total number successful DNS queries, denied DNS queries, and lost queries in the DNS server.
- **Model**—Model number of each AP.
- **FW Version**—Version of the firmware running on each AP.
- **Site**—Name of the site where the AP resides.

Telemetry Information not Received from APs or Radios

The **Information (telemetry) was not received from APs/Radios** insight can be accessed from the **Global** and **Site**, and **Access Points** context. This insight provides information about AP radios that missed sending telemetry data to Aruba Central, and is categorized under availability since AI insights loses visibility of the APs. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

The time series graph displays the number of 2.4 GHz and 5 GHz radios that failed to send telemetry data during the selected time period. You can hover your mouse over each bar graph to see the exact number of missing radios.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 97: *Cards Context*

Cards	Context
Site	Global
Access Point	Global, Site

Site

Lists the number of sites where the APs experience missing telemetry. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Radios Impacted**—Number radio channels that missed telemetry data.

- **Minutes Missing**—Time range of missing telemetry in each site.
- **Hours Missing**—Hourly data of the missing telemetry in each site.

Access Point

Lists the number and details of APs that experience missing telemetry. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Click the number displayed on the **Access Point** card, to view a detailed description of the impacted access points:

- **AP Name**—Name of the access points and link to the specific insight at the AP context.
- **Total Time (HH:MM)**—Total time range (minutes/hours) of missing telemetry in both 2.4 GHz and 5 GHz bands.
- **2.4 GHz Time (HH:MM, %)**—Time range (minutes/hours) and percentage of missing telemetry in 2.4 GHz band.
- **5 GHz Time (HH:MM,%)**—Time range (minutes/hours) and percentage of missing telemetry in 5 GHz band.
- **AP MAC**—MAC address of the AP and link to the specific insight at the AP context.
- **AP Serial**—Serial number of the AP.
- **Firmware**—Version of the firmware running on each AP.
- **Model**—Model number of each AP.
- **Site**—Name of the site where the AP resides.

Outdoor Clients Impacting Wi-Fi Performance

The **Outdoor clients are impacting Wi-Fi performance** insight is used to understand which outdoor clients are affecting the performance of the indoor AP. This insight can be accessed only at the **Global** context, and is triggered when the probe SNR threshold is not set optimally. This insight is categorized under wireless quality as low SNR clients (outdoor) experience poor Wi-Fi connectivity, which in turn affects other indoor clients. This insight provides information about the optimum probe/auth SNR threshold value per AP and per SSID. It also provides the recommended configuration value for probe/auth SNR threshold below which APs ignore probe requests and authentication requests from outdoor clients.

Important Points to Note

- The outdoor clients are located far from the AP having low SNR value, whereas the indoor clients are located near the AP having high SNR value.
- Ensure that the SNR threshold value is set between 8 dBm and 16 dBm. If the value is set below 8 dBm, the system sets it back to 8 dBm. If the value is set above 16 dBm, the system sets it back to 16 dBm. If the value is set between +3 and -3, no specific recommendation is provided as there might be a few clients in the network.

This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

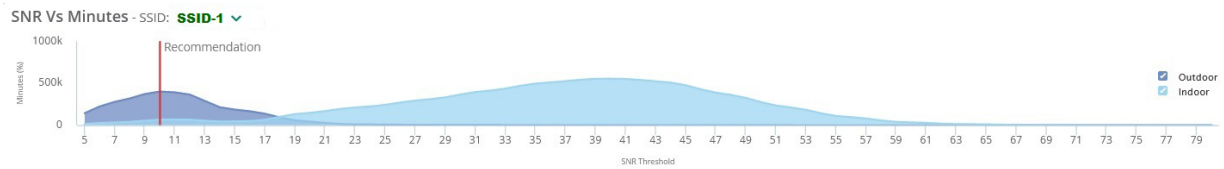
- **SSID**—The list of SSIDs impacted by outdoor clients.
- **Recommendation**—Change the Probe SNR/RSSI threshold and the Auth SNR/RSSI threshold to the recommended value to improve the performance for the indoor Wi-Fi clients.

Time Series Graph

The time series graph displays the current and the recommended threshold (dBm) for each client type in the network. To rectify the issue, the Probe SNR threshold must be set to the recommended value. This frees up airtime and AP resources for indoor users.

The following figure displays the SNR threshold graph based on the SSID selected from the drop-down list and contains the recommended SNR threshold value:

Figure 114 *Sample Probe SNR Threshold Graph*



The probe SNR threshold graph provides the following details:

- **Outdoor**—The number of outdoor minutes at that SNR.
- **Indoor**—The number of indoor minutes at that SNR.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 98: *Cards Context*

Cards	Context
Access Point	Global
Outdoor Clients	Global
Outdoor Minutes	Global

Access Point

Displays the details of APs that are impacted by outdoor clients. Click the arrow › to view the pictorial graph of the **Most Impacted** access points. Select an SSID from the **Access Point** drop-down list to view the most impacted APs. Click the number displayed on the **Access Point** card, to view a detailed description of the impacted APs:

- **AP Name**—Name of the impacted AP and link to the specific insight at the AP context.
- **SSID**—The impacted SSID name.
- **Low SNR Minutes**—The duration for which the connected clients have low SNR value.
- **Recommended Threshold**—The recommended value of the Probe SNR/RSSI Threshold and Auth SNR/RSSI Threshold.
- **Site**—Name of the site where the AP resides.

Outdoor Clients

Lists the name, MAC address, duration, SSID, client OS, and site of clients below the proposed SNR threshold. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Select an SSID from the **Outdoor Clients** drop-down list to view the most impacted clients. Click the number displayed on the **Client** card, to view a detailed description of the impacted clients:

- **Client Name**—Host name of the impacted client and link to the specific insight at the client context.
- **Client MAC**—MAC address of the impacted client and link to the specific insight at the client context.
- **Duration (mins)**—Number of minutes client was outside below the recommended Probe/Auth SNR threshold.
- **SSID**—The SSID impacted by outdoor clients.
- **Client OS**—OS type of the device.
- **Site**—Name of the site where the client resides.

Outdoor Minutes

Displays the percentage of avoided outdoor clients minutes and affected indoor client minutes in a chart.

Click the arrow › to view a pictorial graph of the **Most Impacted** outdoor minutes.

Click the number displayed on the **Outdoor Minutes** card, to view a detailed description of the impacted SSIDs:

- **SSID**—The impacted SSID name.
- **Total Traffic (%)**—The percentage of total traffic impacted.
- **Current Authentication Threshold (min-max)**—The minimum and maximum value of the current SNR/RSSI authentication threshold.
- **Recommended Auth Threshold**—The recommended value of the SNR/RSSI authentication threshold.
- **Current Probe Threshold (min-max)**—The minimum and maximum value of the current probe SNR/RSSI threshold.
- **Recommended Probe Threshold**—The recommended value of the probe SNR/RSSI threshold.
- **Outdoor Minutes Rejected if recommendation is applied to all APs**—The outdoor minutes that are rejected if recommendation is applied to all APs.
- **Indoor Minutes sacrificed if recommendation is applied to all APs**—The indoor minutes that are sacrificed if recommendation is applied to all APs.
- **Outdoor Minutes Rejected if recommendation is applied to recommended subset of APs**—The outdoor minutes that are rejected if recommendation is applied to recommended subset of APs.
- **Indoor Minutes sacrificed if recommendation is applied to recommended subset of APs**—The indoor minutes that are sacrificed if recommendation is applied to recommended subset of APs.

AOS-CX Switches with High CPU Utilization

The **CX Switches had unusually high CPU utilization** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches experiencing higher than normal CPU utilization. It is categorized under availability since the impacted switches and the associated devices experience connectivity issues. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing high CPU utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing high CPU utilization during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 99: *Cards*
Context

Cards	Context
Site	Global
Switch	Global, Site
CPU	Device

Site

Lists the number of sites where the switches experience high CPU utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** impacted sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Switches with High CPU**—Number of switches experiencing high CPU utilization in each site.
- **Minutes with High CPU**—Amount of time (minutes) high CPU utilization observed in each site.

Switch

Lists the number of switches that experience high CPU utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of the high CPU utilization sorted by switch models.
- **FW Version**—Pictorial graph of high CPU utilization sorted by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing high CPU utilization and link to the specific insight at the switch context.
- **Serial**—Serial number the switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Max CPU**—Maximum utilization of the CPU in each switch.
- **Minutes with High CPU**—Time range of high CPU utilization on each switch.
- **Model**—Model number of each switch.

- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

CPU

Lists the time series of CPU utilization percentage for a switch. Click the arrow › to expand the card and view the graphical representation of the data in the selected switch. Click the number displayed on the **CPU** card to view a detailed description of the impacted switch:

- **Switch Name**—Name of the switch experiencing high memory utilization.
- **Max CPU**—Maximum utilization of the CPU in a specific switch.
- **Total Metrics**—Total metrics of the utilization.
- **Percentage Metrics**—Percentage metrics of the utilization.
- **Model**—Model number of each switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

AOS-CX Switches with High Memory Usage

The **CX Switches had unusually high memory usage** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches experiencing higher than normal memory utilization, and is categorized under availability since the impacted switches and the associated devices experience connectivity issues. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing high memory utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing high memory utilization during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 100: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Memory	Device

Site

Lists the number of sites where the switches experience memory utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Switches with High Memory**—Number of switches experiencing high memory utilization in each site.
- **Minutes with High Memory**—Amount of time (minutes) high memory utilization observed in each site.

Switch

Lists the number of switches that experience high memory utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of the high memory utilization sorted by switch models.
- **FW Version**—Pictorial graph of high memory utilization sorted by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing high memory utilization and link to the specific insight at the switch context.
- **Serial**—Serial number the switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Max Memory**—Maximum utilization of memory in each switch.
- **Minutes with High Memory**—Time range of high memory utilization on each switch.
- **Model**—Model number of each switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Memory

Lists the time series of memory utilization percentage for a switch. Click the arrow › to expand the card and view the graphical representation of the data in the selected switch. Click the number displayed on the **Memory** card to view a detailed description of the impacted switch:

- **Switch Name**—Name of the switch experiencing high memory utilization.
- **Max Memory**—Maximum utilization of memory in a specific switch.
- **Avg Memory**—Average utilization of memory in a specific switch.
- **Total Metrics**—Total metrics of the utilization.
- **Percentage Metrics**—Percentage metrics of the utilization.
- **Model**—Model number of each switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site Name**—Name of the site where the switch exists.

AOS-CX Switch Ports with High Power-over-Ethernet Problems

The **CX Switch ports had a high number with Power-over-Ethernet problems** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that have not received required power from PoE devices connected to them. PoE issues occur in switches when power is denied, or power is demoted from the device connected to them. It is categorized under availability since the impacted switches are unable to receive sufficient power. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing power issues in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing power issues during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 101: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Wired Clients	Global, Site

Site

Lists the number of sites where switches have PoE issue. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Events**—Number of events generated pertaining to PoE failures in each site.
- **Ports**—Number of ports for which power is denied.
- **Switches**—Number of switches for which power is denied.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each site.

Switch

Lists the number of switches that experience PoE issues in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of PoE issues classified by switch models.
- **FW Version**—Pictorial graph of PoE issues classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Events**—Number of events generated pertaining to PoE failures in each switch.
- **Wired Clients**—Number of clients impacted by the PoE failures.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each switch.
- **Stack ID**—Stack ID of the impacted switch.
- **Number of Events**—Number of events generated pertaining to PoE failures in each switch.
- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Wired Clients

Lists the MAC Address, name, host name, and auth ID of the clients connected to a switch that experience PoE issues. Click the arrow › to view the pictorial graph of the **Most Impacted** clients. Click the **Wired Clients** drop-down list to view the following:

- **Model**—Pictorial graph of all the device types models connected to the impacted switch.
- **Vendor**—Pictorial graph of the device type vendors connected to the impacted switch.

Click the number displayed on the **Wired Clients** card to view a detailed description of the impacted switches:

- **Wired Client**—Name of the client.
- **Client MAC**—MAC address of the client.
- **Description**—An overview of the connected devices, including the OS type, model, and version.
- **Switch Name**—Name of the impacted switch where the client resides and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch where the client resides.
- **Port Number**—Port number of the switch the client device is connected to.
- **Power Requested/Offered**—PoE consumption for each client.
- **Reason**—Cause of the denied PoE power in each client.
- **Status**—Status of client.
- **Model**—Hardware model of the impacted switch where the client resides.
- **Vendor**—Vendor of the wired client.
- **Site**—Name of the site where the client resides.

AOS-CX Switches with High Port Errors

The **CX Switches had an unusual number of port errors** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that experience excessive port

errors confined to the Layer1 and Layer2 in the network. This insight is categorized under availability since the wired devices connected to the affected ports experience connectivity issues. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.
- **Errors**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing port errors in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing port errors during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 102: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Port	Global, Site, Device

Site

Lists the number of sites where switches have port errors. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Switches with Port Errors**—Number of the switches experiencing port errors.
- **Number of Errors**—Number of errors in each site.
- **Number of Ports**—Number of ports experiencing errors in each site.

Switch

Lists the number of switches that experience excessive port errors in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of port errors classified by switch models.
- **FW Version**—Pictorial graph of port errors classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing port errors and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Number of Errors**—Number of port errors in each switch.
- **Number of Ports**—Number of ports experiential excessive errors.
- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Port

Number of ports experiencing excessive errors. Click the arrow › to view the pictorial graph of the **Most Impacted** impacted ports. Click the number displayed on the **Port** card, to view a detailed description of the impacted ports:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Switch MAC**—MAC address of the impacted switch.
- **Port Number**—Port number of the switch.
- **Number of Errors**—Number of port errors in each port.
- **Status**—Status of the impacted switch.
- **Connected Device**—MAC address of the connected device.
- **Connected Device MAC**—MAC address of the client device.
- **Connected Device Description**—An overview of the connected devices, including the OS type, model ,and version.

AOS-CX Switches with High Port Flaps

The **CX Switches had excessive port flaps** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that experience port flaps in the network. It is categorized under availability since this causes connectivity drops and also triggers the reboot of PoE devices. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing port flaps in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing port flaps during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 103: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Port	Global, Site, Device

Site

Site card is accessible only when this insight is accessed from the global context. It lists the number of sites where switches have port flaps. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Switches with Excessive Flaps**—Number of the switches experiencing port flaps.
- **Number of Flaps**—Number of errors in each site.
- **Number of Ports**—Number of ports experiencing flaps in each site.

Switch

Lists the number of switches that experience excessive port flaps in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of port flaps classified by switch models.
- **FW Version**—Pictorial graph of port flaps classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing port flaps and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.

- **Stack ID**—Stack ID of the impacted switch.
- **Number of Flaps**—Number of port flaps in each switch.
- **Number of Ports**—Number of ports effected by excessive flaps.
- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Port

Number of ports experiencing excessive flaps. Click the arrow › to view the pictorial graph of the **Most Impacted** ports. Click the number displayed on the **Port** card, to view a detailed description of the impacted ports:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Switch MAC**—MAC address of the impacted switch.
- **Port Number**—Port number of the switch.
- **Number of Flaps**—Number of port flaps in each port.
- **Status**—Status of the impacted switch.
- **Connected Device**—MAC address of the connected device.
- **Connected Device MAC**—MAC address of the client device.
- **Connected Device Description**—An overview of the connected devices, including the OS type, Model , and Version.

AOS-Switches with High Port Errors

The **PVOS Switches had an unusual number of port errors** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that experience excessive port errors confined to the Layer1 and Layer2 in the network. This insight is categorized under availability since the wired devices connected to the affected ports experience connectivity issues. This insight displays the following information:

- Insight Summary
- Time Series Graph
- Cards

Insight Summary

The insight summary provides the following details:

- **Reason**—Displays the possible causes for which the failure occurred.
- **Recommendation**—Displays the recommendation against each failure to resolve the same.
- **Errors**—Displays the exact number and percentage of failures that occurred against each failure reason.

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing port errors in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing port errors during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 104: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Port	Global, Site, Device

Site

Lists the number of sites where switches have port errors. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Switches with Port Errors**—Number of the switches experiencing port errors.
- **Number of Errors**—Number of errors in each site.
- **Number of Ports**—Number of ports experiencing errors in each site.

Switch

Lists the number of switches that experience excessive port errors in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of port errors classified by switch models.
- **FW Version**—Pictorial graph of port errors classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing port errors and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Number of Errors**—Number of port errors in each switch.
- **Number of Ports**—Number of ports experiential excessive errors.

- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Port

Number of ports experiencing excessive errors. Click the arrow › to view the pictorial graph of the **Most Impacted** ports. Click the number displayed on the **Port** card, to view a detailed description of the impacted ports:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Switch MAC**—MAC address of the impacted switch.
- **Port Number**—Port number of the switch.
- **Number of Errors**—Number of port errors in each port.
- **Status**—Status of the impacted switch.
- **Connected Device**—MAC address of the connected device.
- **Connected Device MAC**—MAC address of the client device.
- **Connected Device Description**—An overview of the connected devices, including the OS type, model ,and version.

AOS-Switches with High Port Flaps

The **PVOS Switches had excessive port flaps** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that experience port flaps in the network. It is categorized under availability since this causes connectivity drops and also triggers the reboot of PoE devices. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing port flaps in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing port flaps during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 105: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Port	Global, Site, Device

Site

Site card is accessible only when this insight is accessed from the global context. It lists the number of sites where switches have port flaps. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Switches with Excessive Flaps**—Number of the switches experiencing port flaps.
- **Number of Flaps**—Number of errors in each site.
- **Number of Ports**—Number of ports experiencing flaps in each site.

Switch

Lists the number of switches that experience excessive port flaps in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of port flaps classified by switch models.
- **FW Version**—Pictorial graph of port flaps classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing port flaps and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Number of Flaps**—Number of port flaps in each switch.
- **Number of Ports**—Number of ports effected by excessive flaps.
- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site Name**—Name of the site where the switch exists.

Port

Number of ports experiencing excessive flaps. Click the arrow › to view the pictorial graph of the **Most Impacted** ports. Click the number displayed on the **Port** card, to view a detailed description of the impacted ports:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.

- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Switch MAC**—MAC address of the impacted switch.
- **Port Number**—Port number of the switch.
- **Number of Flaps**—Number of port flaps in each port.
- **Status**—Status of the impacted switch.
- **Connected Device**—MAC address of the connected device.
- **Connected Device MAC**—MAC address of the client device.
- **Connected Device Description**—An overview of the connected devices, including the OS type, Model , and Version.

AOS-Switches with High CPU Utilization

The **PVOS Switches had unusually high CPU utilization** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches experiencing higher than normal CPU utilization. It is categorized under availability since the impacted switches and the associated devices experience connectivity issues. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing high CPU utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing high CPU utilization during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 106: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
CPU	Device

Site

Lists the number of sites where the switches experience high CPU utilization. Click the arrow › to view the pictorial graph of the**Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Switches with High CPU**—Number of switches experiencing high CPU utilization in each site.
- **Minutes with High CPU**—Amount of time (minutes) high CPU utilization observed in each site.

Switch

Lists the number of switches that experience high CPU utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of the high CPU utilization sorted by switch models.
- **FW Version**—Pictorial graph of high CPU utilization sorted by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing high CPU utilization and link to the specific insight at the switch context.
- **Serial**—Serial number the switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Max CPU**—Maximum utilization of the CPU in each switch.
- **Minutes with High CPU**—Time range of high CPU utilization on each switch.
- **Model**—Model number of each switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

CPU

Lists the time series of CPU utilization percentage for a switch. Click the arrow › to expand the card and view the graphical representation of the data in the selected switch. Click the number displayed on the **CPU** card to view a detailed description of the impacted switch:

- **Switch Name**—Name of the switch experiencing high memory utilization.
- **Max CPU**—Maximum utilization of the CPU in a specific switch.
- **Total Metrics**—Total metrics of the utilization.
- **Percentage Metrics**—Percentage metrics of the utilization.
- **Model**—Model number of each switch.
- **Firmware**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

AOS-Switches with High Memory Usage

The **PVOS Switches had unusually high memory usage** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches experiencing higher than normal memory utilization, and is categorized under availability since the impacted switches and the associated devices experience connectivity issues. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing high memory utilization in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing high memory utilization during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 107: *Cards Context*

Cards	Context
Site	Global
Switch	Global, Site
Memory	Device

Site

Lists the number of sites where the switches experience memory utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site impacted by the insight and link to the specific insight at the site context.
- **Switches with High Memory**—Number of switches experiencing high memory utilization in each site.
- **Minutes with High Memory**—Amount of time (minutes) high memory utilization observed in each site.

Switch

Lists the number of switches that experience high memory utilization. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of the high memory utilization sorted by switch models.
- **FW Version**—Pictorial graph of high memory utilization sorted by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing high memory utilization and link to the specific insight at the switch context.
- **Serial**—Serial number the switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch.
- **Max Memory (%)**—Maximum utilization of memory in each switch.
- **Minutes with High Memory**—Time range of high memory utilization on each switch.
- **Model**—Model number of each switch.

- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Memory

Lists the time series of memory utilization percentage for a switch. Click the arrow › to expand the card and view the graphical representation of the data in the selected switch. Click the number displayed on the **Memory** card to view a detailed description of the impacted switch:

- **Switch Name**—Name of the switch experiencing high memory utilization.
- **Max Memory**—Maximum utilization of memory in a specific switch.
- **Avg Memory**—Average utilization of memory in a specific switch.
- **Total Metrics**—Total metrics of the utilization.
- **Percentage Metrics**—Percentage metrics of the utilization.
- **Model**—Model number of each switch.
- **Firmware**—Version of the firmware running on each switch.
- **Site Name**—Name of the site where the switch exists.

AOS-Switch Ports with High Power-over-Ethernet Problems

The **PVOS Switch ports had a high number with Power-over-Ethernet problems** insight can be accessed from the **Global**, **Site**, and **Switches** context. This insight provides information on the switches that have not received required power from PoE devices connected to them. PoE issues occur in switches when power is denied, or power is demoted from the device connected to them. It is categorized under availability since the impacted switches are unable to receive sufficient power. This insight displays the following information:

- Time Series Graph
- Cards

Time Series Graph

In **Global** and **Site** context the time series graph displays the count of switches experiencing power issues in the network during the selected time period. You can hover your mouse on each bar graph to see the number of impacted switches during the selected time under each severity. In the **Device** context this graph displays the severity level of the selected switch experiencing power issues during the selected time period.

Cards

The cards vary based on the context that you access the insight from. Click one of the cards to view further details:

Table 108: *Cards Context*

Cards	Context
Site	Global

Cards	Context
Switch	Global, Site
Wired Clients	Global, Site

Site

Lists the number of sites where switches have PoE issue. Click the arrow › to view the pictorial graph of the **Most Impacted** sites. Click the number displayed on the **Site** card, to view a detailed description of the impacted sites:

- **Site**—Name of the site where the impacted switch resides and link to the specific insight at the site context.
- **Events**—Number of events generated pertaining to PoE failures in each site.
- **Ports**—Number of ports for which power is denied.
- **Switches**—Number of switches for which power is denied.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each site.

Switch

Lists the number of switches that experience PoE issues in the network. Click the arrow › to view the pictorial graph of the **Most Impacted** switches. Click the **Switch** drop-down list to view the following:

- **Switch Model**—Pictorial graph of PoE issues classified by switch models.
- **FW Version**—Pictorial graph of PoE issues classified by switch firmware versions.

Click the number displayed on the **Switch** card to view a detailed description of the impacted switches:

- **Switch Name**—Name of the switch experiencing power issues and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Events**—Number of events generated pertaining to PoE failures in each switch.
- **Wired Clients**—Number of clients impacted by the PoE failures.
- **Impact (Minutes)**—Amount of time (minutes) for which power is denied in each switch.
- **Stack ID**—Stack ID of the impacted switch.
- **Number of Events**—Number of events generated pertaining to PoE failures in each switch.
- **Model**—Model number of the impacted switch.
- **FW Version**—Version of the firmware running on each switch.
- **Site**—Name of the site where the switch exists.

Wired Clients

Lists the MAC Address, name, host name, and auth ID of the clients connected to a switch that experience PoE issues. Click the arrow › to view the pictorial graph of the **Top 5** impacted clients. Click the **Wired Clients** drop-down list to view the following:

- **Model**—Pictorial graph of all the device types models connected to the impacted switch.
- **Vendor**—Pictorial graph of the device type vendors connected to the impacted switch.

Click the number displayed on the **Wired Clients** card to view a detailed description of the impacted switches:

- **Wired Client**—Name of the client.
- **Client MAC**—MAC address of the client.
- **Description**—An overview of the connected devices, including the OS type, model, and version.
- **Switch Name**—Name of the impacted switch where the client resides and link to the specific insight at the switch context.
- **Serial**—Serial number of the impacted switch and link to the specific insight at the switch context.
- **Stack ID**—Stack ID of the impacted switch where the client resides.
- **Port Number**—Port number of the switch the client device is connected to.
- **Power Requested/Offered**—PoE consumption for each client.
- **Reason**—Cause of the denied PoE power in each client.
- **Status**—Status of client.
- **Model**—Hardware model of the impacted switch where the client resides.
- **Vendor**—Vendor of the wired client.
- **Site**—Name of the site where the client resides.

Chapter 7
Managed Service Provider

Aruba Central is a SaaS platform that provides a single customer login for all cloud applications delivered by Aruba. Aruba Central in MSP mode consists of the Network Operations app and the Account Home page. The Network Operations app in Aruba Central provides a cloud-based network management platform for managing your wireless and wired networks with Aruba Instant APs and Switches. Along with device and network management functions, the Network Operations app offers value-added services such as customized guest access, client presence and service assurance analytics. In Account Home, you can manage network inventory, subscriptions, user access and other functions.

The Managed Service Provider (MSP) mode is a multi-tenant operational mode that Aruba Central accounts can be converted into, provided these accounts have subscribed to the Network Operations app. Enabling MSP mode for the Network Operations app provides additional options that an administrator can use to manage multiple independent Aruba Central accounts from a single interface.

With the MSP mode enabled, MSP administrators can provision tenant accounts, allocate devices, assign subscriptions, and monitor tenant accounts. MSP administrators can drill down to a specific tenant account and perform additional administration and configuration tasks.

Terminology

Take a few minutes to familiarize yourself with the following key terms:

Term	Description
Standard Enterprise mode	Refers to the Aruba Central deployment mode in which customers manage their respective accounts end-to-end. The Standard Enterprise mode is a single-tenant environment for a single end-customer.
MSP mode	Refers to the Aruba Central deployment mode in which service providers centrally manage and monitor multiple tenant accounts from a single management interface.
▪ Tenant accounts ▪ Customer accounts	End-customer accounts created in the MSP mode. Each tenant is an independent instance of Aruba Central.

Term	Description
MSP administrator	Refers to owners of the primary account. These users have administrator privileges to provision, manage, and monitor tenant accounts.
▪ Tenant users ▪ Customers	Refers to the owners of an individual tenant account provisioned in the Managed Service Provider mode. The MSP administrator can create a tenant account.

Getting Started with MSP Solution

Before you get started with your onboarding and provisioning operations, we recommend that you browse through the following topics to know the key capabilities of Aruba Central MSP Solution.

- Operational Modes and Interfaces
- About the Managed Service Portal User Interface

Navigate through the following steps to view help pages that describe the onboarding and provisioning procedures for MSP and tenant accounts:

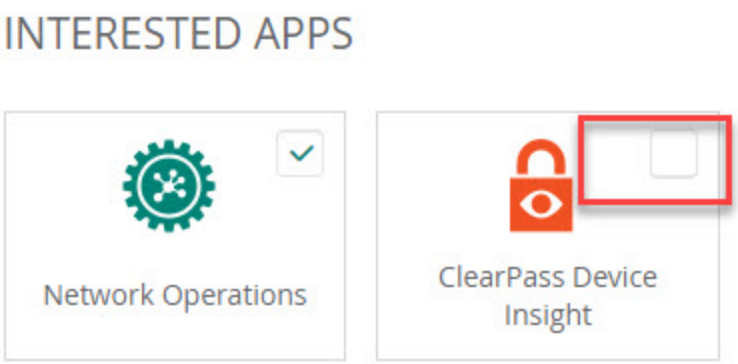
1. Set up your Aruba Central account
2. Accessing Aruba Central Portal
3. Enabling Managed Service Mode
4. Onboard devices
5. Add subscription keys
6. Create groups
7. Provision tenant accounts
8. Assign devices to tenant accounts
9. Assign subscription to devices and services
10. Configure users and roles
11. Customize tenant account view
12. Add Certificates
13. Monitor tenant accounts

Enabling Managed Service Mode

The **Enable MSP** option is only available if the following conditions are met:

- You sign into Aruba Central as an administrator.
- The Aruba Central account is only subscribed to the Network Operations app. If the account has multiple subscriptions, such as both Network Operations and ClearPass Device Insight, the **Enable MSP** option is not available.

Figure 115 *Do Not Select the ClearPass Device Insight*



- You access the **User Settings** icon from the Network Operations app and not the Account Home page.

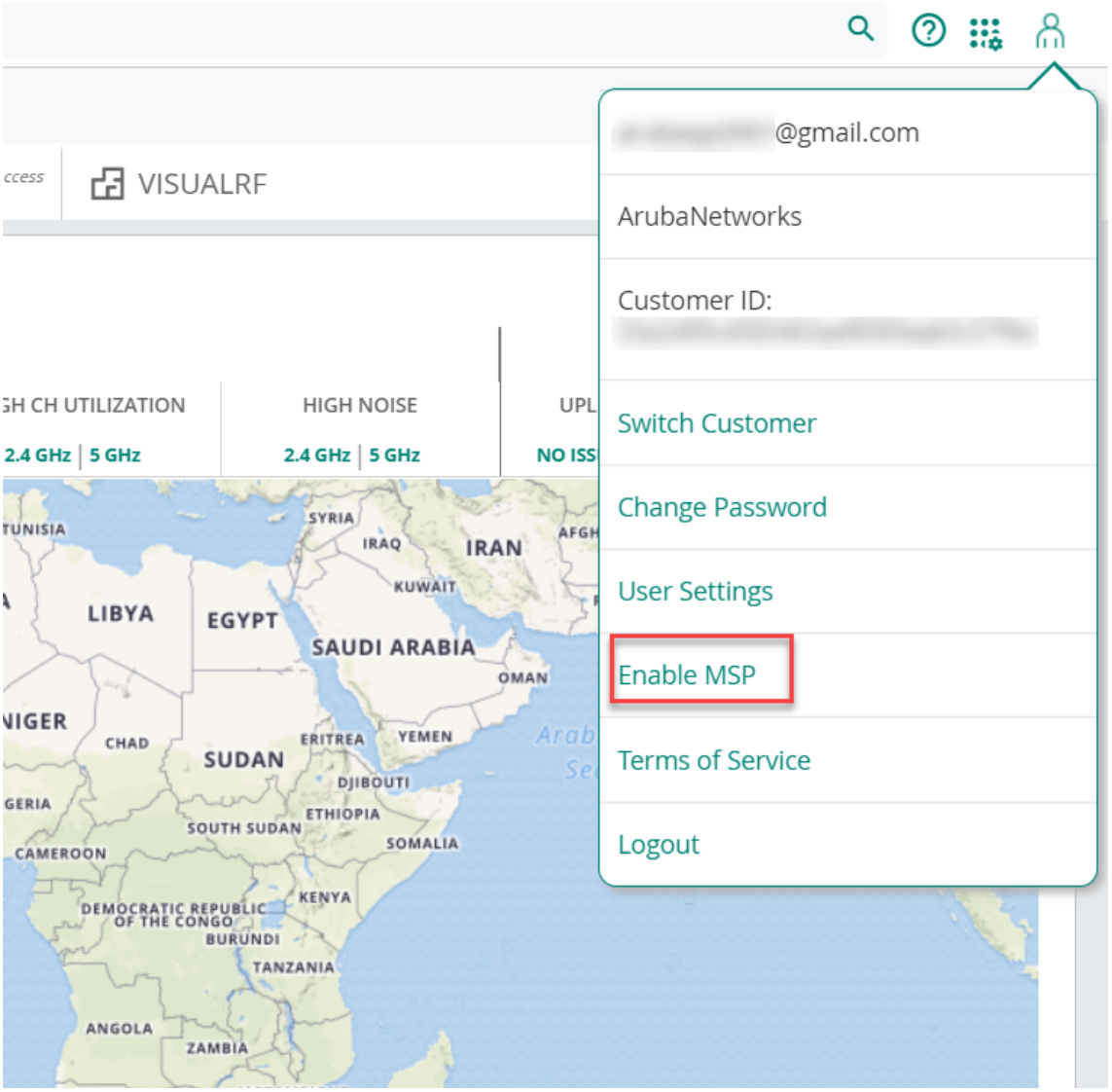
To enable MSP mode, perform the following steps:

1. Log in to your Aruba Central account as an administrator.
2. Launch the **Network Operations** app.

   If you have subscriptions to other apps, enabling MSP mode is not supported, and the **Enable MSP** option is not available. In this case, create a new Aruba Central account with the Networks Operations app and contact Aruba Technical Support to migrate devices and licenses to the new account.
3. Click the user icon.

4. Click **Enable MSP**.

Figure 116 *Click Enable MSP*



5. In the **Managed Service Mode** pop-up window, fill in the required details and click **Submit**.

   In the confirmation pop-up window, the following message is displayed if the submitted information meets the acceptance criteria: **MSP Mode is enabled for this account**.

   If the submitted information does not meet the acceptance criteria, a request denied message is displayed along with the reason on why the MSP mode is not recommended. MSP mode is not recommended and the MSP application is denied if one of the following conditions are true:

   - Your deployment of Aruba Central does not require you to deliver network management services to your end customers.
   - You are going to manage Aruba Central for your customers, however, the network devices are purchased by the customers. In this scenario, you can manage the customer accounts from the Standard Enterprise Mode by using the Switch Customer option. For more information on this deployment model, see End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2).

6. Click **OK**.

   The page is automatically redirected to the MSP Dashboard view.

If your online application is rejected because the conditions for enabling MSP were not met, and you wish to revise the provided information, the **Enable MSP** option is reset after 30 minutes for you to try again.

Disabling the Managed Service Mode

If you do not want to use **Managed Service Mode**, you can switch to the Standard Enterprise mode. Delete all tenant account data before you proceed.

To disable Managed Service mode:

1. Click the user icon.
2. Click **Disable MSP**.

   The option is grayed out if tenant account data exists.
3. In the **Managed Service Mode** pop-up window, click **Disable Managed Service Mode**.

MSP Mode Enablement Scenarios

You can convert the Standard Enterprise mode in the Network Operations app to MSP mode. Only the Network Operations app supports the MSP mode and it must be the only app running in Aruba Central for enabling the MSP mode. The following is a list of possible scenarios you might encounter while subscribing to the Network Operations app.

- **Scenario 1**: You sign up for Aruba Central to evaluate the Networks Operations app as well as the ClearPass Device Insight app. Subsequently, you wish to enable MSP mode on the Network Operations app. MSP mode conversion is not allowed in this scenario. Create another Aruba Central account with only the Network Operations app and convert this account to MSP mode. Contact Aruba Support for migrating the devices and licenses.
- **Scenario 2**: You sign up for an Aruba Central account to evaluate the ClearPass Device Insight app. After that, you also sign up for evaluating the Network Operations app in standard enterprise mode in the same account. This mode of operation is supported.
- **Scenario 3**: You sign up for an Aruba Central account to evaluate the Network Operations app. After that, you also sign up for evaluating the ClearPass Device Insight in the same Aruba Central account. If you are running the Network Operations app in the standard enterprise mode, this mode of operation is supported.

Managing MSP Licenses

Aruba Central in the Managed Service Provider (MSP) mode supports the following types of licenses for APs, switches, and gateways:

- **Foundation**—Allows you to manage and monitor the APs, switches, and gateways of your customers or tenants through the Aruba Central MSP mode. This license provides all the features included in the legacy Device Management subscription and some additional features that were available as a value- added services for APs in the earlier licensing model.
- **Advanced**—This license provides all the features of a Foundation License, with additional features related to AI Insights.

The licenses for APs, switches, and gateways cannot be used interchangeably. For example, you cannot use an AP Foundation License on a gateway. Similarly, if an Aruba 25xx Switch is in the inventory but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch. Before enabling the Auto-Assign License option for a specific device type, ensure that there are sufficient available licenses for the specific device type.

For more information on the different types of available licenses, see Aruba Central License Feature Details.

A license key is an alphanumeric string with 9 to 14 characters; for example, PQREWD6ADWERAS. Aruba Central can manage a device only if the corresponding license key of the device is added to Aruba Central. License keys can either be evaluation license keys that map to evaluation licenses or paid license keys that map to paid licenses. The evaluation license key is valid for 90 days.

To use Aruba Central for managing, profiling, analyzing, and monitoring your devices, you must ensure that you have a valid license key and that the license key is listed in the **Account Home** > **Global Settings** > **Key Management** page.

The license keys are not mapped directly to devices. Before assigning a license key to a device, the system only checks whether there are licenses available in the pool for the device.

All license keys that are added to an MSP account goes to a license pool and devices are licensed from this MSP license pool. Licenses can be assigned to devices only when the devices are already mapped to customer accounts. In the MSP mode, all the hardware and licenses are owned by the MSP. The MSP temporarily assigns devices and their corresponding licenses to customers for the duration of the managed service contract. When the contract ends, the devices and the licenses are returned back to the common pool of resources of the MSP and can be reassigned to another customer.

You can either enable automatic assignment of licenses or manually assign licenses for devices added in Aruba Central MSP mode.

Enabling Automatic License Assignments

If you, as an MSP administrator, want to enable automatic assignment of licenses to the devices mapped to your customer accounts, note the following points:

- Aruba Central assigns licenses only if the devices are mapped to a customer account.
- When a device is moved from a customer account back to the MSP pool, Aruba Central removes the license assigned to this device.
- When the automatic license assignment is enabled, Aruba Central disables the device-specific and customer-specific overrides.
- When the automatic license assignment is enabled, all the existing customers and newly created customers in the MSP account inherit the license assignment settings. Subsequently, Aruba Central assigns licenses to the customers and their respective devices.
- If you migrate from the Standard Enterprise mode to the MSP mode, Aruba Central retains your license settings.
- If the devices are no longer mapped to a customer account, MSP administrators cannot assign licenses to these devices.
- If auto-assignment is enabled and the device license expires, you are notified about the license expiry. Aruba Central checks if an equivalent license of the same tier or capacity is available and reassigns that license to the device automatically. If an equivalent license is unavailable, Aruba Central un-assigns a set of devices to match the number of expiring licenses and you are notified that the device license is updated.

You can configure automatic license assignment either during initial setup or later from the **Account Home** page.

Automatic License Assignment from the Initial Setup Wizard

To enable automatic assignment of licenses from the Initial Setup Wizard:

1. Verify that you have a valid license key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the **Assign License** tab, slide the **Auto-Assign Licenses** toggle switch to the On position.

Automatic License Assignment from Account Home

To enable automatic assignment of licenses from the **License Assignment** page:

1. On the **Account Home** page, under **Global Settings**, click **License Assignment**.

   The **License Management** page is displayed.
2. In the **Assign License** tab, slide the **Auto-Assign Licenses** toggle switch to the On position.

   All the devices in your inventory are selected for automatic assignment of licenses. You can edit the list by clearing the existing selection and re-selecting devices.

When a license assigned to a device expires, or is canceled, Aruba Central checks for the available licenses in your account and assigns an available license of the longest validity to the device. If your account does not have an adequate number of licenses, you may have to manually assign licenses to as many devices as possible. To view the license utilization details and the number of licenses available in your account, go to the **Account Home** > **Global Settings** > **Key Management** page.

Enabling Manual License Assignments

You can disable the **Auto-assign License** option and manually assign licenses to devices. Licenses can be assigned only for devices which are mapped to a customer account.

To manually assign licenses to devices or override the current assignment:

1. In the **Account Home** page, under **Global Settings**, click **License Assignment**.

   The **License Management** page is displayed.
2. Ensure that the **Auto-Assign Licenses** toggle switch is turned off.

   When you turn off the **Auto-Assign Licenses** toggle switch:
   - Automatic assignment of licenses for all the existing customers, including the MSP devices, are disabled.
   - All device licenses assigned to devices are preserved.
   - Devices must be assigned to customer accounts before assigning a license to it. If a license is assigned to a device that is not mapped to any specific customer account, Aruba Central displays the following error message: **Please assign this device to a customer before licensing it. Customer assignment can be performed in the Device Inventory page**.
3. Click one of the tabs for **Access Points**, **Switches**, or **Gateways**.

   Each of the device tabs has two sub-tabs: **Unlicensed** and **Licensed**.
4. You can use the **Customer** filter to display a specific customer.

5. In the **Unlicensed** tab, you can select one or multiple devices and click **Manage** or **Manage Assignment.**

   The **Manual License Assignment (Manual)** window is displayed.
6. From the **Choose License Type** drop-down menu, select a suitable license and click **Update** to assign a license.

   If the license update is successful, you get a notification and the device in not listed anymore under the **Unlicensed** tab.

Removing or Updating a License from a Device

You can remove a license from a device or change the license assigned to a device from the **License Assignment** window.

1. In the **Account Home** page, under **Global Settings**, click **License Assignment**.

   Ensure that the **Auto-Assign License** toggle is turned off.
2. Click one of the tabs for **Access Points**, **Switches**, or **Gateways**.

   Each of the device tabs has two sub-tabs: **Unlicensed** and **Licensed**.
3. You can use the **Customer** filter to display a specific customer.
4. In the **Licensed** tab, you can select one or multiple devices for which you want to either update or remove a license.
5. Click **Manage or Manage Assignment.**

   The **Manual License Assignment (Manual)** window is displayed.
6. You can do one of the following:
   - To remove a license, click **Unassign**.

     The devices with unassigned licenses are no longer listed in the **Licensed** tab.
   - To update to a new license, from the **Choose License Type** drop-down menu, select a suitable license and click **Update**.

     If the license update is successful, you get a notification and the **Licensed** tab displays the updated licenses.

Acknowledging License Expiry Notifications

In the **Account Home** page, under **Global Settings**, click **Key Management**. The **Key Management** page displays the expiration date for each license.

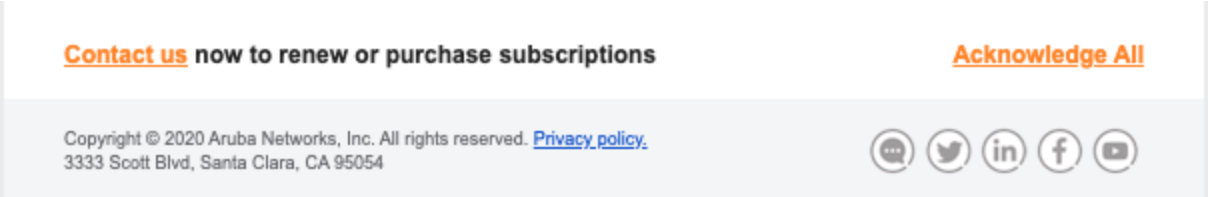
As the licenses expiration date approaches, users receive expiry notifications. The users with an evaluation license receive license expiry notifications through email 30, 15, and 1 day before the license expiry and on day 1 after the license actually expires.

The users with paid licenses receive license expiry notifications through email 90, 60, 30, 15, and 1 day before expiry and two notifications per day on day 1 and day 2 after the license expires.

Acknowledging Notifications through Email

If the user has multiple licenses, a consolidated email with the expiry notifications for all licenses is sent to the user. Users can acknowledge these notifications by clicking the **Acknowledge All** link in the email notification.

Figure 117 *Acknowledging Notifications through Email*



Acknowledging Notifications in the UI

If a license has already expired, or is about to expire within 24 hours, a license expiry notification message is displayed in a pop-up window when the user logs in to Aruba Central.

To prevent Aruba Central from generating expiry notifications, click **Acknowledge**.

Renewing Licenses

To renew your licenses, contact Aruba Sales team.

System Users and User Roles in MSP Mode

The **Users and Roles** page under **Global Settings** enables you to view, create, and modify users and roles. The **Users and Roles** page has two tabs: **Users** and **Roles**. The following topics are included:

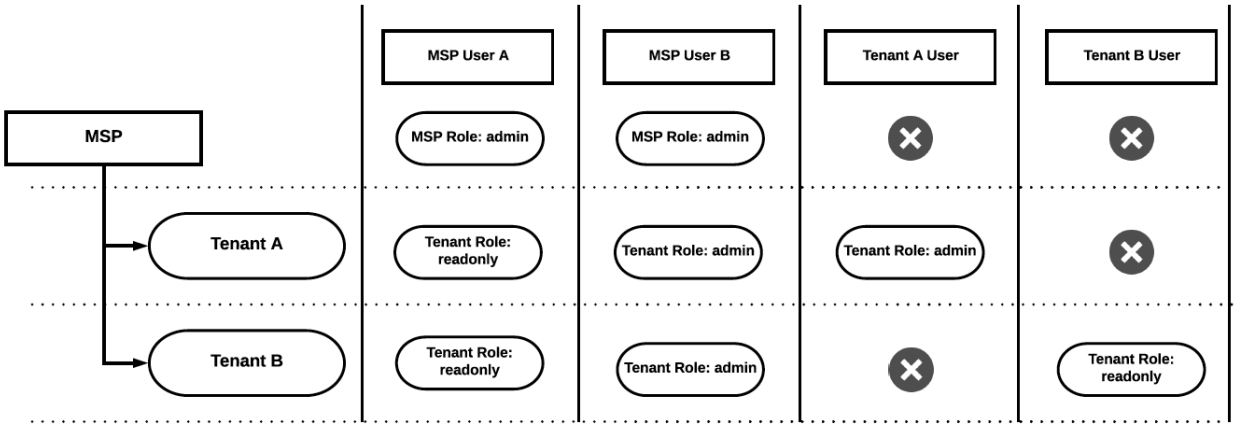
About Roles in MSP Home Account

Aruba Central MSP mode supports role-based access control. Aruba Central allows you to create predefined user roles and custom roles.

As shown in the following figure, MSP user A is mapped to two roles. MSP role **admin** gives the user administrator access to all MSP applications and the tenant role **readonly** gives the user read-only access to all tenant accounts. MSP user B is tied to MSP role **admin** and tenant role **admin**. The tenant administrator role provides the user administrator access to all tenant accounts.

Tenant user A is mapped to the **admin** role. This role gives the user administrator access to all tenant A applications. Tenant user B is mapped to the **readonly** role. This role gives the user read-only access to tenant B applications. Tenant user A and tenant user B can access only their respective accounts.

Figure 118 *MSP Role-Based Access Control*



The **Roles** tab has the following predefined roles.

Table 109: *Predefined Roles*

Application	Role	Privilege
Account Home	**admin**	Administrator for the **Account Home** page. If there are common modules between **Account Home** and other app(s), the **Account Home** role has higher precedence and the user is granted permission if the operation is initiated from the **Account Home** page.
	readwrite	Can view and modify settings in the **Account Home** page and all **Global Settings** pages. **NOTE: Note:** The '**readwrite**' role will not have modify permission for the following pages: ▪ **Users and Roles** ▪ **Single-Sign-On**
	readonly	Can view the **Account Home** page and all **Global Settings** pages.
Network Operations	**admin**	Administrator for the **Network Operations** application. Has access to **Account Home** > **Global Settings**. This is applicable only if the **Account Home** role is not set or is not conflicting.
	deny-access	Cannot view the **Network Operations** application.
	guestoperator	Has guest operator access to the **Network Operations** application. User does not have access to **Account Home** > **Global Settings**.
	readonly	Has read-only access to **Account Home** > **Global Settings** and the **Network Operations** application.
	readwrite	Has read-write access to **Account Home** > **Global Settings** and the **Network Operations** application. Has access to view and modify data using the Aruba Central UI or APIs. However, the user cannot execute APIs to: ▪ Enable or disable MSP mode. ▪ Perform operations in the following pages: ◦ **Account Home** > **Users and Roles** ◦ **Network Operations** application > **Organization** > **Labels and Sites**

Module Permissions for Roles

Aruba Central enables you to define roles with **view** or **modify** permissions. You can also **block** user access to some modules. If a module is blocked for a specific role, the corresponding pages are not displayed in the UI or can access the pages but no data is displayed and all actions are disabled for the role.

Aruba Central supports setting permissions for the following modules:

Table 110: *Permissions*

Application	Module	Description
Account Home	**Devices and Subscription**	Enables users to add devices and assign keys and subscriptions to devices in the **Account Home** page.
	Users	Enables users to define a role with access (View, Modify, or Block) to the user details in the **Users** tab in the **Users and Roles** page. To define the role, navigate to **Account Home > Global Settings > Users and Roles**.
	Roles	Enables users to define a role with access (View, Modify, or Block) to the role details in the **Roles** tab in the **Users and Roles** page. To define the role, navigate to **Account Home > Global Settings > Users and Roles**.
	SSO	Enables users to define a role with access (View, Modify, and Block) to the Single Sign On profiles details in the Users tab in the Single-Sign-On page (Account Home > Single-Sign-On). Enables users to define a role with access (View, Modify, or Block) to the **Single Sign On** profiles details in the **Single Sign On** page. To navigate to the **Single Sign On** page, go to **Account Home > Single Sign On**.
Network Operations	**MSP**	Enables users with administrator role and privileges to define user access to MSP modules such as Customer Management and Portal Customization. The MSP tenant account user does not have access to the **MSP** application. Even if a tenant account user is assigned a custom role having **MSP** application privileges: ▪ Tenant account user does have access to the **MSP** application. ▪ **MSP** will not appear in the **Account Home** > **Global Settings** > **Users and Roles** > **Roles** > **Allowed Applications** list.
	Group Management	Enables users to create, view, modify, and delete groups and assign devices to groups.
	Devices and Subscription	Users cannot edit or set permissions for this module. **Modify** and **Block** options are disabled. By default, the **View Only** permission is set.
	Network Management	Enables users to configure, troubleshoot, and monitor Aruba Central-managed networks. You can customize the permissions (view or modify or block) for the following sub-modules: ▪ Configuration ▪ Configuration Variables ▪ Privileged Configuration ▪ Firmware ▪ Troubleshooting ▪ Other Modules **NOTE:** For the Privileged Configuration, the 'Block' option disables the Admin tab (**Gateway**>**System**>**Admin**) for the user. The user management privileges are disabled for this user for gateways at the

Application	Module	Description
		device and group level.
	Guest Management	Enables users to configure cloud guest splash page profiles.
	AirGroup	Enables users to define or block user access to the AirGroup pages.
	Presence Analytics	Enables users to access the Presence Analytics app and analyze user presence data.
	Floorplans	Enables user to access Floorplans and RF heatmaps.
	Unified Communications	Enables users to access the Unified Communications pages.
	Install Manager	Enables users to manage installer profiles and site installations.
	Reports	Enables users to view and create reports.
	Other Applications	Enables users to access other applications modules such as notifications and Virtual Gateway deployment service.

Adding a Custom Role in MSP Account Home

The following are the permissions that you can associate with a custom role:

- Roles with **Modify** permission can perform add, edit, or delete actions within the specific module.
- Roles with **View Only** permission can only view the specific module.
- Roles with **Block** permission cannot view that particular module or can view the corresponding pages but no data is displayed and all actions are disabled.

To add a custom role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. Click **Add Role**. The **New Role** window is displayed.
4. Specify a name for the role.
5. From the drop-down list, select one of the following:
   - **Account Home**—To manage access to devices and subscriptions in Aruba Central.
   - **Network Operations**—To set permissions at the module level in the **Network Operations** application.
6. For Network Management and MSP modules, you can set access rights at the module level.

   To set view or edit permissions or block the users from accessing a specific module, complete the following steps:
   a. Click **Customize**.
   b. Select one of the following options for each module as required:
      - **View Only**
      - **Modify**
      - **Block**

7. Click **Save**.
8. Assign the role to a user account as required.

Viewing Role Details

To view the details of a role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab. The **Roles** tab displays the following information:
   - **Role Name**—Name of the role.
   - **Allowed Applications**—The application(s) to which the user account is subscribed to.
   - **Assigned Users**—Number of users assigned to a role.

Editing a Role

To edit a role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the edit icon.
4. In the **Edit Role <"Rolename">** window, modify the permissions set for module(s).
5. Click **Save**.

Deleting a Role

To delete a role, ensure that the role is not associated to any user and complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the delete icon.
4. Confirm role deletion in the **Confirm Action** dialog box.

About Users in MSP Account Home

In the **Account Home** page, under **Global Settings**, click **Users and Roles**. The **Users** tab is displayed. The **List of Users** table displays the following information:

- Email ID of the user.
- Type of user. The user can be system user or external user.
- Description of the user.
- MSP role
- Tenant role
- Account Home role
- Allowed groups for the user.
- Last active time of the user. If the last active time cell is blank, the user has not logged in after the product upgrade.

The **Actions** link offers the following options:

- **Resend invitation to users**—If any user has not received the email invite, you can use this link to resend invitations

- **Two-Factor Authentication (2FA)**—Enables Two-factor authentication.
- **Support Access**—Enables you to generate a new password of a specified validity to give access to a support person from Aruba.

Adding a User in MSP Account Home

To add a user, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
   The **Users and Roles** page is displayed.
2. Click **Add User**.
   The **New User** window is displayed.
3. Configure the following parameters:
   - **Username**—Email ID of the user. Enter a valid email address.
   - **Description**—Description of the user role. You can enter up to a maximum of 32 characters including alphabets, numbers, and special characters in the text field.
   - **Language**—Select a language. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
   - **Account Home**—Select a user role for the **Account Home** page.
   - **Network Operations**—Select an MSP role and Tenant role for the **Network Operations** application.
4. Click **Save**. An email invite is sent to the user with a registration link. Users can use this link to access Aruba Central.

The registration link in the email invite is valid for 15 days.

Track Progress

Click the **Track Progress** link to open the **Operations Status** page that provides the user account creation or modification status. The status can be in progress or failed. No status is displayed if the user account is successfully created.

Editing a User in MSP Account Home

To edit a user account, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
   The **Users** tab opens.
2. In the **List of Users** table, select the user and click the edit icon.
3. In the **Edit User <"Username">** window, modify description, role, or allowed groups.
4. Click **Save**.

Deleting a User in MSP Account Home

To delete a user account:

1. In the **Account Home** page, under **Global Settings**, click **Users and Roles**.
   The **Users** tab opens.

2. In the **List of Users** table, select the user and click the delete icon.
3. Confirm user deletion in the **Confirm Action** dialog box.

Viewing Audit Trail Logs for Users

Audit logs are generated when a new user is created and an existing user is modified or deleted from the Aruba Central account. It also records the login and logout activities of users.

To view audit logs for Aruba Central users:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**.

   The **Audit Trail** page is displayed.
2. To view audit logs for user addition, modification, or deletion, click the filter in the **Classification** column, and select **User Management**.
3. To filter audit logs about user activity, click the filter in the **Classification** column, and select **User Activity**.

Groups in the MSP Mode

MSP groups are UI groups mapped to the default UI groups in the tenant account. If a tenant account is associated to a specific group in the MSP mode, the configuration changes to the devices associated with this tenant account are pushed only to the **default** group in the tenant account view. However, MSP administrators can create more groups for a specific tenant by drilling down to a tenant account.

Template groups are not supported in the MSP mode. However, template groups can be defined and managed at each tenant account individually.

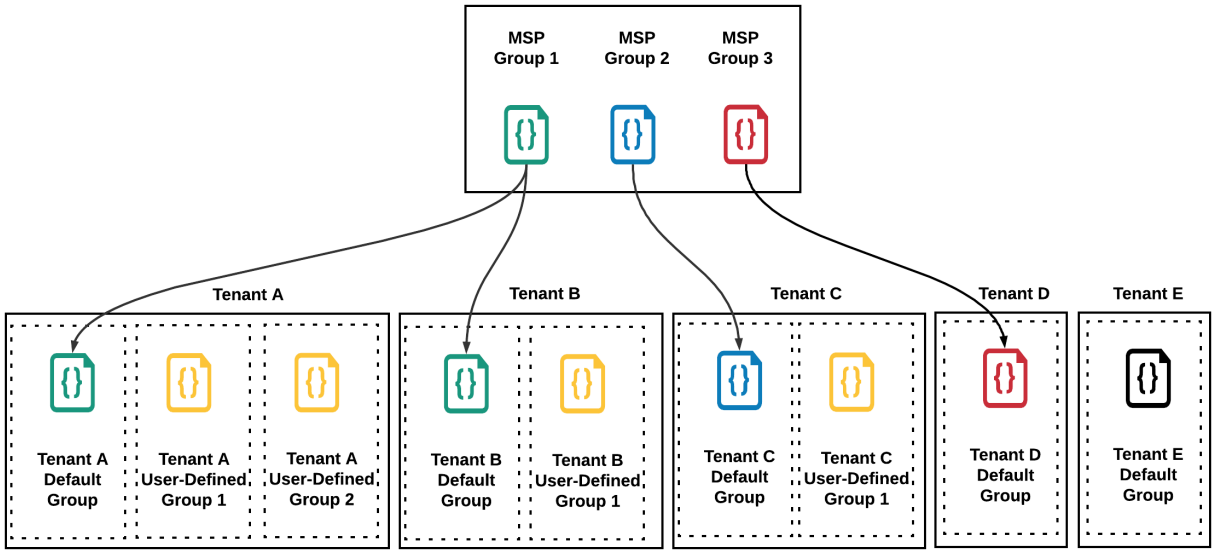
MSP Group Illustration

As shown in the following figure, tenant A and tenant B are mapped to MSP group 1. The default group configuration for these tenants is inherited from MSP group 1 configuration. Tenant A has two additional user-defined groups that are independent of MSP group 1 configuration. Tenant B has one additional user-defined group that is independent of MSP group 1 configuration.

Tenant C is mapped to MSP group 2 configuration. Its default group configuration is inherited from MSP group 2. It also has one additional user-defined group that is independent of MSP group 2 configuration.

Tenant D has only one default group and its configuration is inherited from MSP group 3. Tenant E is not mapped to any MSP group. Its default group configuration is independent of any MSP group configuration. It can have additional user-defined groups as well, if required.

Figure 119 *MSP Groups*



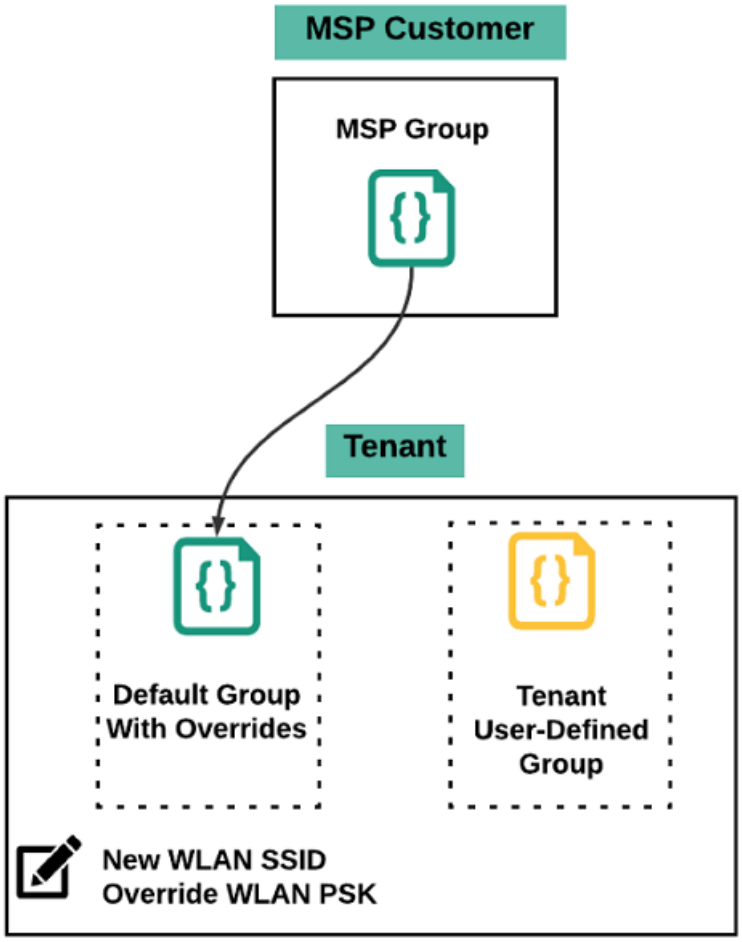
Tenant Default Group Overrides

If a tenant is mapped to an MSP group, the configuration of its default group is inherited from the MSP group it is mapped to. Once mapped, except for any newly created WLAN SSID and WLAN PSK, other configurations are overridden.

As shown in the following figure, the mentioned configuration options are allowed on a tenant default group that is mapped to an MSP group:

- Creating a new WLAN SSID.
- Overriding the WLAN PSK for a WLAN inherited from an MSP group.

Figure 120 *Default Group Overrides*



Creating an MSP UI Group

To manage device configuration using UI configuration containers in Aruba Central, you can create a UI group and assign devices.

To create an MSP UI group:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Maintain**, click **Organization** to display the **Groups** dashboard.
3. To create a new group, click **New Group**.
   The **Create New Group** pane is displayed.
4. Enter a name for the group.
5. Configure a password to restrict group access to authorized users only.
6. Click **Add Group**.

About Provisioning Tenant or Customer Accounts

After adding a device in the MSP mode, the device must be mapped to a tenant account for device management and monitoring operations.

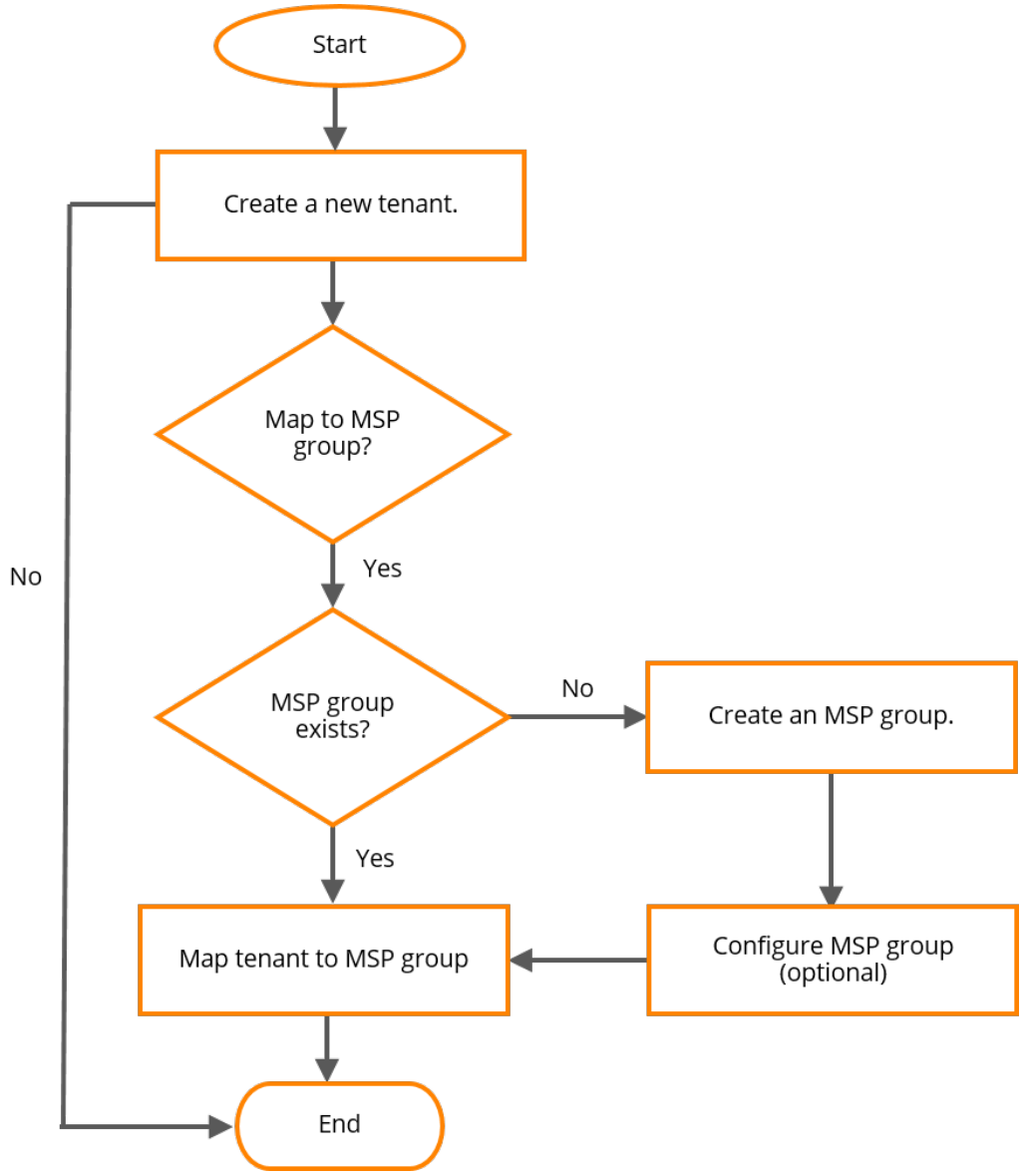
With MSP mode enabled, the MSP administrator manages the creation and deletion of tenant accounts. After a tenant account is created, the MSP administrator can add tenant users to the account. To create a tenant user, the MSP administrator must provide a valid email address for the user. A verification email is sent to this email address. Tenant users have access to their individual tenant account only. Tenant users do not have access to other tenant accounts managed by the MSP.

The group associated to the tenant account in the MSP mode shows up as the default group for tenant account users. In the MSP mode, all configuration changes made to the group associated to the tenant account are applied to the default group on the tenant account.

Flowchart for Tenant Account Mapping in MSP

The following flowchart displays a visual representation of how you can create a tenant account and map it to an MSP group.

Figure 121 *Tenant Account Mapping to an MSP Group*



Creating a Tenant Account and Mapping to an MSP Group

The following are the usage guidelines for creating a tenant account:

- If the tenant account provisioning fails, the task is marked as **Provision Failed** in the UI and **PROVISION_FAILED** in the **[GET] /msp/v1/customers** API response. To view the task status in the UI, under **Manage**, click **Overview** to display the **Dashboard** page. Click the **Customers** tab. If the provisioning fails, you can delete the tenant account and try again.
- Tenant account users can only view reports generated for the default group. The administrators of a specific tenant account can drill down to the tenant account and generate reports for the default group.
- If cloud guest provisioning fails, cloud guest features for the tenant may get impacted. In such instances, contact Aruba Central Technical Support.

To add a tenant account, complete the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview**.

   The **Dashboard** is displayed.
3. Click **Add New Customer**.

   The **Add Customer** page is displayed.
4. Enter the name of the tenant in the **Customer Name** text box. The MSP customer name can be a maximum of 70 single byte characters. All special characters, ASCII, and Unicode are allowed.
5. Enter the description of the tenant in the **Description** text box. The MSP customer description field can be a maximum of 32 single byte characters. All special characters, ASCII, and Unicode are allowed.
6. If you want to associate the tenant to a group, click the **Add to group** toggle switch.
7. From the **Group** drop-down list, select a group to which you want to assign the tenant.

The group associated to the tenant account in the MSP mode shows up as the default group for tenant account users. In the MSP mode, all configuration changes made to the group associated to the tenant account are applied to the default group on the tenant account.

8. If you want to prevent the users of the tenant account from modifying SSID settings of the device group, select the **Lock SSID** check box.
9. Click **Save**.

Viewing Tenant Account Details

To view the tenant account details, perform the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard** page.
3. Click the **Customers** tab.
4. Hover over the tenant account and click **expand**.

The customer details window displays the following sections. Click the X mark on the top right-corner of the screen to exit the window and return to the dashboard.

Summary

- **Customer ID**—Displays the subscription renewal schedule for the next 12 months. The graph plots the total count of subscriptions that are due for renewal for each month.
- **Customer Created**—Displays the count of devices that are managed in the network over a period of time.

- **MSP Group**—Displays the total number of tenants added to Aruba Central over a period of time.
- **Description**—Description of the tenant account.
- **Customer Name**—Name of the tenant account.

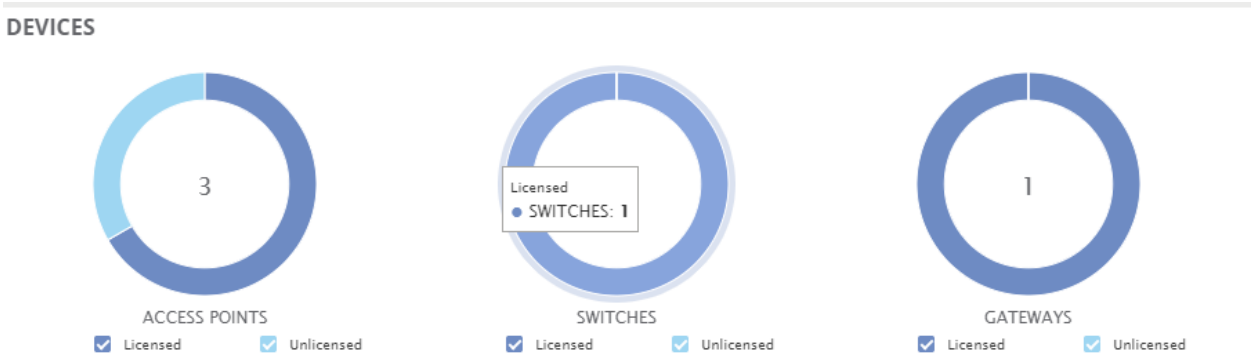
Devices

This section is a graphical representation of the devices assigned to the selected tenant account, as well as the licensed and unlicensed count for each device type.

- The section consists of three doughnut charts, each chart representing one of the following types of devices, APs, switches, and gateways.
- The number in the center of the chart indicates the total number of devices, both *licensed* and *unlicensed*, of a specific type allocated to the tenant account.
- The two colors on the ring of the doughnut indicates the number of licensed and unlicensed devices of a specific type allocated to the tenant account. You can hover over one segment of the doughnut to see the numbers corresponding to the selected segment.
- You can also deselect and reselect the **Licensed** and **Unlicensed** options for each chart.

For example, in the following image, the tenant account has three APs, one switch, and one gateway. Out of this, only one AP is unlicensed.

Figure 122 *Devices Section of the Expand Tenant Account Page*



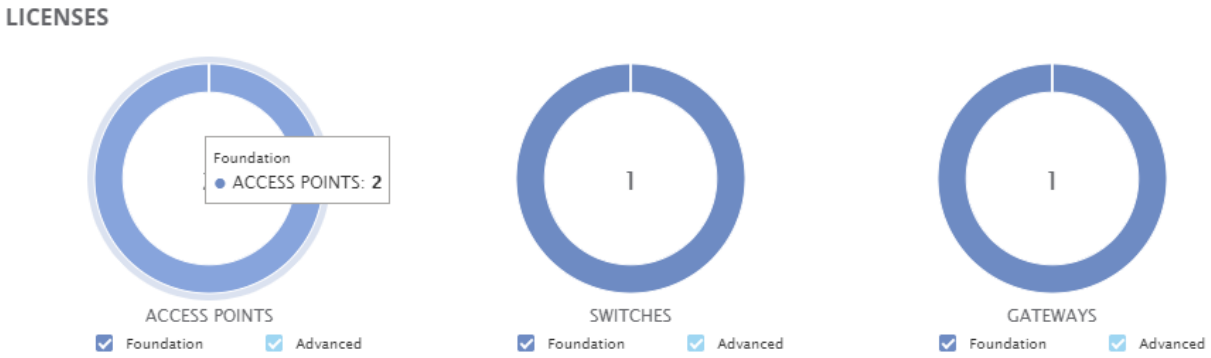
Licenses

This section is a graphical representation of the device subscriptions assigned to the devices for the selected tenant account. The section also shows the number of Foundation and Advanced licenses for each type of device.

- The section consists of three doughnut charts, each chart representing one of the following types of devices, APs, switches, and gateways.
- The number in the center of the chart indicates the total number of *licensed* devices of a specific type allocated to the tenant account.
- The two colors on the ring of the doughnut indicates the number of Advanced and Foundation licenses assigned to a device of a specific type allocated to the tenant account. You can hover over one segment of the doughnut to see the numbers corresponding to the selected segment.
- You can also deselect and reselect the **Advanced** and **Foundation** options for each chart.

For example, in the following image, the tenant account has two APs, one switch, and one gateway, each assigned with a Foundation license.

Figure 123 *Licenses Section of the Expand Tenant Account Page*



Editing a Tenant Account

When editing the group associated with the MSP customer or tenant, the default group configuration of the tenant account is also impacted. To edit a tenant account, complete the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview**.
   The **Dashboard** is displayed.
3. Hover over the tenant account that you want to edit and click **edit**.
4. Modify the account details.

NOTE

If you want to associate the tenant account to a different group, turn on the **Add to group** toggle switch and select a group.

5. Click **Save**.

Deleting a Tenant Account

To delete a tenant account, complete the following steps:

1. From the **Network Operations** app, filter **All Groups**.
2. Under **Manage**, click **Overview**.
   The **Dashboard** is displayed.
3. Hover over the tenant account that you want to delete and click **delete**.
4. Click **Yes** to confirm the action.

NOTE

If the tenant account deletion fails, the provisioning status is marked as **Delete Failed** in the UI and **DELETE_FAILED** in the **[GET] /msp/v1/customers/{customer_id}** API response. To view the task status in the UI, under **Manage**, click **Overview** to display the **Dashboard** page. Click the **Customers** tab.

Assigning Devices to Tenant Accounts

Before assigning devices to tenant accounts, ensure that you have completed the following: onboarded devices, assigned subscriptions, and provisioned tenant accounts.

To assign devices to tenant accounts, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.

   A list of devices provisioned in the MSP mode is displayed.
2. Select one or several devices from the table. To select multiple devices, press and hold the **Ctrl** key and select the devices.

   The **Assign Customer** button is displayed under the table.
3. Click **Assign Customer**.

   A window showing a list of tenant accounts provisioned in the MSP mode is displayed.
4. Select the tenant account to which you want to assign the device.

   The groups associated with the tenant accounts are displayed.
5. Click **Assign Device (s)**.
6. Click **Yes** when prompted for confirmation.

MSP Dashboard

The MSP dashboard provides a summary of hardware and subscriptions owned by the MSP and details about the tenant accounts managed by the MSP.

The hardware includes APs, switches, and gateways.

Viewing the MSP Dashboard

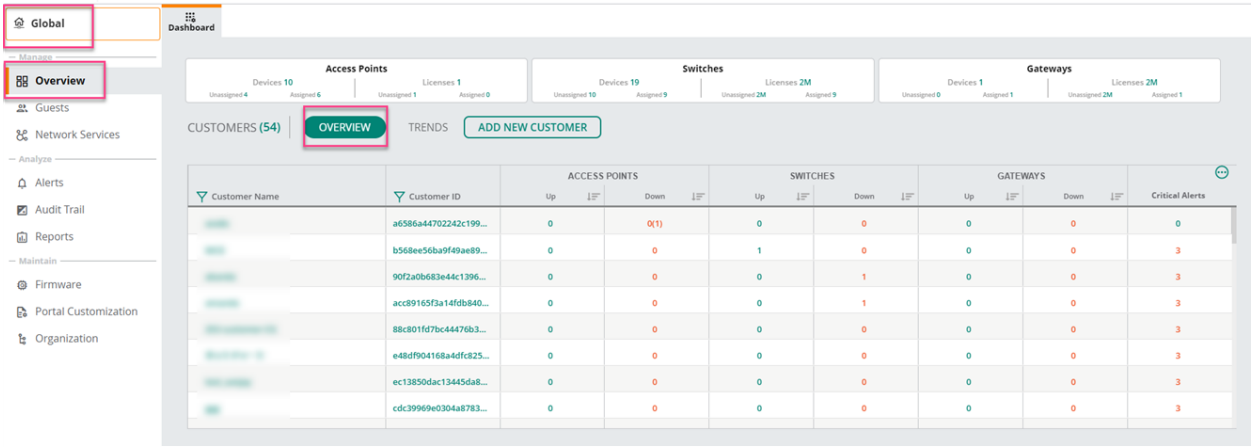
To view the MSP dashboard, perform the following steps:

1. In the **Network Operations** app, set the filter to **All Groups**.

   The filter context changes to **Global**.
2. Under **Manage**, click **Overview** to display the **Dashboard**.
   The number is parenthesis () for **Customers** indicates the total number of customers for that MSP account.
   In the following image, the total number of customers is 54.

   The **Dashboard** page includes the following sections:
   - A summary section for the dashboard—Displays the assigned and unassigned devices and the assigned and unassigned licenses for APs, switches, and gateways.
   - **Overview**—Displays the list of customers, the types of devices assigned to each customer, as well as critical alerts, if any.
   - **Trends**—Displays charts for license renewal, the number of devices under MSP management, and the number of customers added over the last year.
   - **Add New Customer**—Enables you to add a new tenant to the MSP account. Perform the steps detailed in About Provisioning Tenant or Customer Accounts.

Figure 124 *Viewing the MSP Dashboard*



Dashboard Summary

The summary section for **Dashboard** displays the total number of assigned and unassigned devices, and the total number of assigned and unassigned licenses for three categories of hardware devices that include APs, switches, and gateways. In MSP mode, you must first assign a device to a tenant account before assigning a license to the device.

The summary section includes the following details:

- **Access Points**
  - **Devices**—Number of available APs. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of the APs in the MSP inventory.
    - **Unassigned**—Number of APs that are not assigned to any tenant account. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of only the unassigned APs in the MSP inventory.
    - **Assigned**—Number of APs that are already assigned to a tenant account. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of only the assigned APs in the MSP inventory.
  - **Licenses**—Number of available licenses for APs. Click the number to navigate to **Account Home** > **License Assignment** > **Access Points** to see the details of all the licenses for APs in the MSP inventory.
    - **Unassigned**—Number of AP licenses that are not assigned to any AP. Click the number to navigate to **Account Home** > **License Assignment** > **Access Points** > **Unlicensed** to see the details of all the unassigned licenses for APs in the MSP inventory.
    - **Assigned**—Number of AP licenses that are already assigned to APs. Click the number to navigate to **Account Home** > **License Assignment** > **Access Points** > **Licensed** to see the details of all the assigned licenses for APs in the MSP inventory.
- **Switches**
  - **Devices**—Number of available switches. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of the switches in the MSP inventory.
    - **Unassigned**—Number of switches that are not assigned to any tenant account. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of the switches in the MSP inventory.

- **Assigned**—Number of switches that are already assigned to a tenant account. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of only the assigned switches in the MSP inventory.

◦ **Licenses**—Number of available licenses for switches. Click the number to navigate to **Account Home** > **License Assignment** > **Switches** to see the details of all the licenses for switches in the MSP inventory.

- **Unassigned**—Number of switch licenses that are not assigned to any switches. Click the number to navigate to **Account Home** > **License Assignment** > **Switches** > **Unlicensed** to see the details of all the unassigned licenses for switches in the MSP inventory.
- **Assigned**—Number of switch licenses that are already assigned to switches. Click the number to navigate to **Account Home** > **License Assignment** > **Switches** > **Licensed** to see the details of all the assigned licenses for switches in the MSP inventory.

■ **Gateways**

◦ **Devices**—Number of available gateways. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of the gateways in the MSP inventory.

- **Unassigned**—Number of gateways that are not assigned to any tenant account. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of only the unassigned gateways in the MSP inventory.
- **Assigned**—Number of gateways that are already assigned to a tenant account. Click the number to navigate to **Account Home** > **Device Inventory** to see the details of only the assigned gateways in the MSP inventory.

◦ **Licenses**—Number of available licenses for gateways. Click the number to navigate to **Account Home** > **License Assignment** > **Gateways** to see the details of all the licenses for gateways in the MSP inventory.

- **Unassigned**—Number of gateway licenses that are not assigned to any gateways. Click the number to navigate to **Account Home** > **License Assignment** > **Gateways** > **Unlicensed** to see the details of all the unassigned licenses for gateways in the MSP inventory.
- **Assigned**—Number of gateway licenses that are already assigned to gateways. Click the number to navigate to **Account Home** > **License Assignment** > **Gateways** > **Licensed** to see the details of all the assigned licenses for gateways in the MSP inventory.

Customer | Overview

By default, the **Customers** | **Overview** table is displayed. The table provides an overview of tenant accounts. MSP administrators can perform tasks such as drilling down to a tenant account, editing an existing tenant account, and deleting a tenant account.

■ **Customer Name**

Name of the tenant account. Click the customer name to go to the tenant account view for the customer. Hover over the tenant account name to view the following options:

◦ **expand**—Opens a new pop-up window showing the tenant account details.
For more information, see Viewing Tenant Account Details.

◦ **edit**—Opens the **Edit Customer** pop-up window.
For more information, see Editing a Tenant Account .

◦ **delete**—Opens the confirmation dialog box.
For more information, see Deleting a Tenant Account.

Hover over the icon next to the tenant account name to view the provisioning status. The status can be one of the following:

- In Progress
- Provision Failed

NOTE

Use the filter icon on the column header to filter by tenant account name.

- **Customer ID**

  Unique ID of the tenant account. The ID can be in one of the following formats:

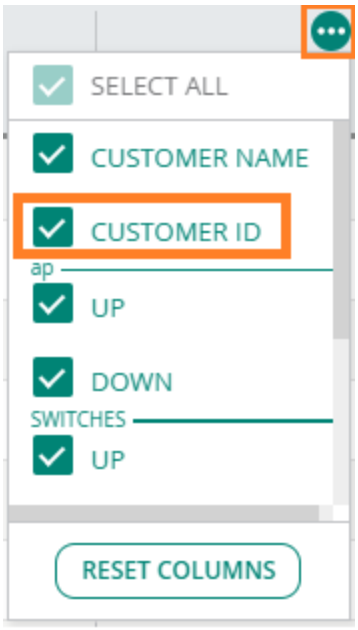
  - Numerical format
  - UUID format

  Use the column filter to search for a particular customer ID. Note that you must enter the full customer ID.

NOTE

The **Customer ID** column is not displayed in the default view. Use the column selector and select the **Customer ID** check box to add the column to the table.

Figure 125 *Selecting the Customer ID for Display*



- **Access Points**
  - **Up**—Total number of online APs. Click the number to view the list of online APs.
  - **Down**—Total number of offline APs. Click the number to view the list of offline APs.

  Click the sort icon to sort the column in ascending or descending order.

  Sometimes, the total number of APs that are displayed as **Down** for a tenant account in MSP view may not equal the total number of corresponding APs displayed as **Offline** under **Manage** > **Access Points** in the tenant account view. This discrepancy is corrected by an automatic and periodic sync between the MSP database and tenant view database. The periodic sync happens every 12 hours. The number in parentheses () indicates the number of devices that are not onboarded.
- **Switches**
  - **Up**—Total number of online switches. Click the number to view the list of online switches.
  - **Down**—Total number of offline switches. Click the number to view the list of offline switches.

Click the sort icon to sort the column in ascending or descending order.

Sometimes, the total number of switches that are displayed as **Down** for a tenant account in MSP view may not equal the total number of corresponding switches displayed as **Offline** under **Manage** > **Switches** in the tenant account view. This discrepancy is corrected by an automatic and periodic sync between the MSP database and tenant view database. The periodic sync happens every 12 hours. The number in parentheses () indicates the number of devices that are not onboarded.

The number of switches displayed in the MSP dashboard corresponds to the total number of switches available for the tenant. However, in the tenant view, a switch stack is considered as a single entity. For example, if there are two switch stacks for a tenant account, and each stack has two members, the MSP dashboard displays the count as four whereas the tenant account displays the count as two.

- **Gateways**
  - **Up**—Total number of online gateways. Click the number to view the list of online gateways.
  - **Down**—Total number of offline gateways. Click the number to view the list of offline gateways.

  Click the sort icon to sort the column in ascending or descending order.

  Sometimes, the total number of gateways that are displayed as **Down** for a tenant account in MSP view may not equal the total number of corresponding gateways displayed as **Offline** under **Manage** > **Gateways** in the tenant account view. This discrepancy is corrected by an automatic and periodic sync between the MSP database and tenant view database. The periodic sync happens every 12 hours. The number in parentheses () indicates the number of devices that are not onboarded.
- **Critical Alerts**

  Total number of critical alerts for the tenant account. Click the number to navigate to the **Alerts** page of the tenant account.

  For more information, see MSP Alerts.

Customers | Trends

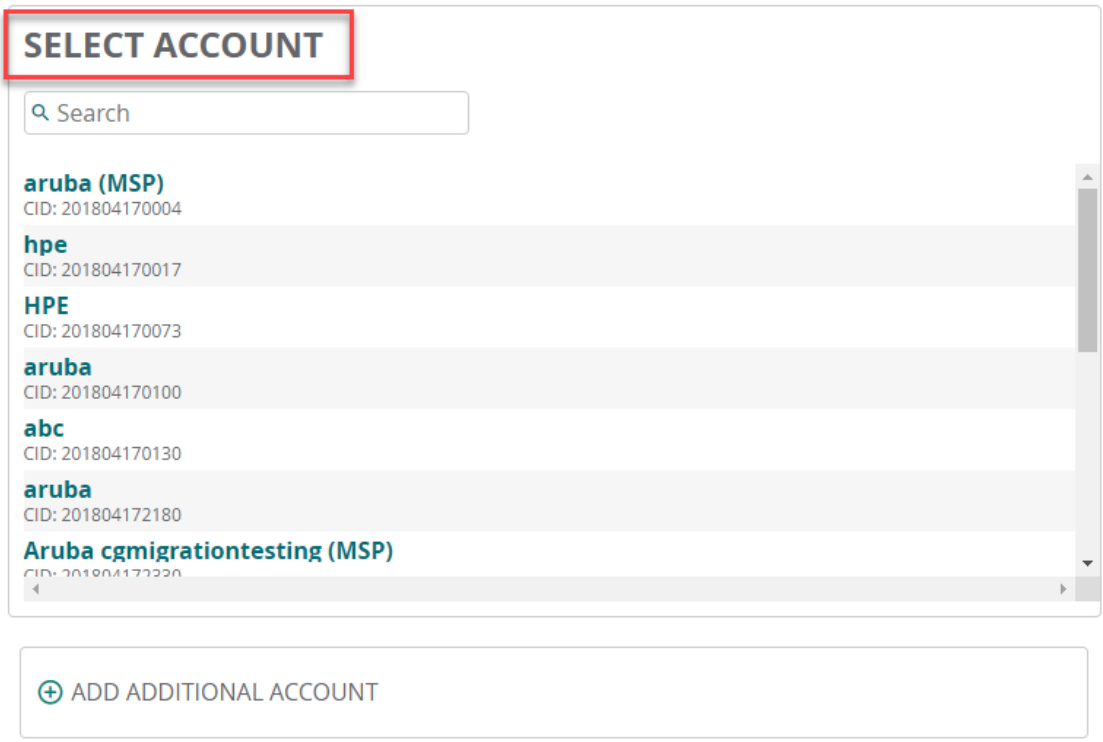
Go to **Customers** | **Trends** to view the following sections:

- **License Renewal Schedule (1 Year)**—Displays the subscription renewal schedule for the next 12 months. The entries include the license renewal date and the total count of subscriptions of each type that are due for renewal on that date.
- **Device Under Management** graph—Displays the count of devices that are managed in the network over the last 12 months. The dates are plotted on the x-axis and the number of devices on the y-axis. Hover over any part of the chart to see the number of devices the MSP is managing on that specific date.
- **Customers** graph—Displays the total number of tenants added to Aruba Central over the last 12 months. The dates are plotted on the x-axis and the number of tenants on the y-axis. Hover over any part of the chart to see the number of tenants the MSP added on that specific date. Click **Total** to view the total number of tenant accounts.

Using the Switch Customer Option

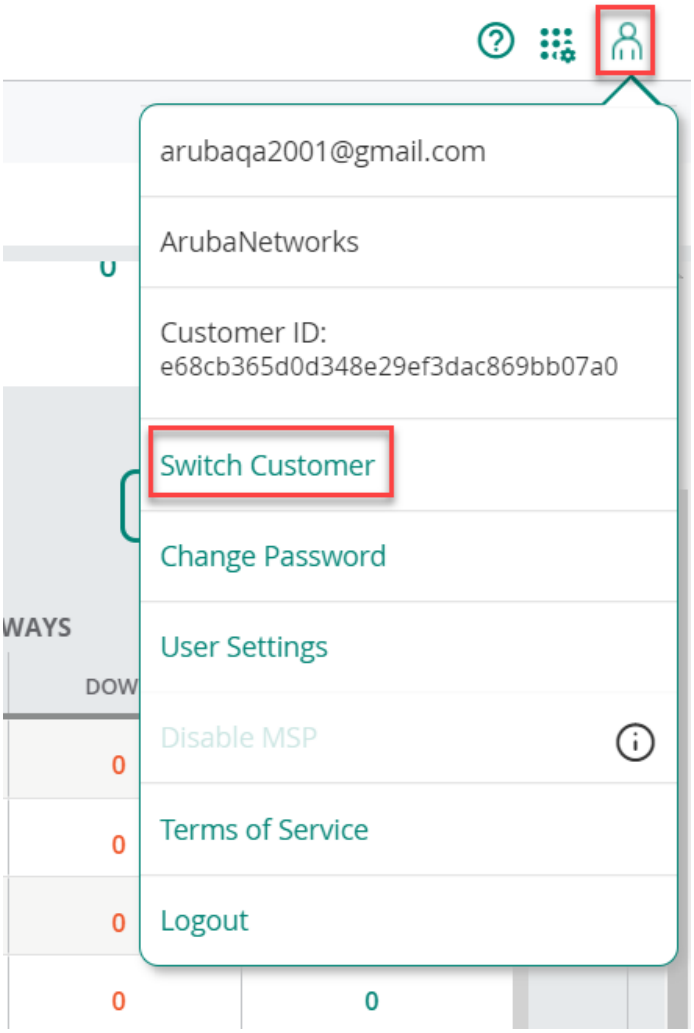
If you are an MSP administrator and if your user ID has been added to multiple tenant accounts, after you log in to Aruba Central, you must select the tenant account that you want to access.

Figure 126 *Select Account*



To select a different tenant account, click the **User** icon , select **Switch Customer**, and then select the tenant account that you want to access.

Figure 127 *Switch Customer*



MSP Certificates

You can view and add certificates in MSP.

Viewing Certificates in MSP Mode

1. In the **Network Operations** app, use the filter to select **All Groups**.
   The global dashboard is displayed for the MSP mode.
2. Under **Maintain**, click **Organization**.
3. Click the **Certificates** tab.
4. The **Certificate Store** displays the following information:

Table 111: *Certificate Store Parameters*

Date Pane Item	Description
Certificate Name	Name of the certificate.
Status	Status of the certificate as either **Active** or **Expired**.
Expiry Date	Date of expiry for the certificate.
Type	Type of certificate. For example, a server certificate.
MD5 Checksum	The Message Digest 5 (MD5) algorithm is a widely used hash function producing a 128-bit hash value from the data input. Checksum value of the certificate.
SHA-1 Checksum	The Secure Hash Algorithm 1 (SHA-1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. Checksum value of the certificate.

Uploading Certificates in the MSP Mode

MSP administrators can upload certificates to Aruba Central certificate store. They can also map the certificate usage for server and user authentication for the groups associated to a tenant account.

To upload certificates to the certificate store:

1. In the **Network Operations** app, use the filter to select **All Groups**.
   The global dashboard is displayed.
2. Under **Maintain**, click **Organization**.
3. Click the **Certificates** tab.
4. To add a new certificate to the **Certificate Store**, click the + sign.
   The **Add Certificate** dialog box is displayed.
5. Enter the certificate name in the **Name** text box.
6. Select the certificate type from the **Type** list.
7. Select the certificate format from the **Format** drop-down.
   The supported certificate formats are PEM, DER, and PKCS12.
8. For server certificates, enter and then retype the passphrase.
9. Click **Choose File** to browse to your local directory and select the certificate to upload.
10. Click **Add**.

Aruba Central allows percolation of certificates that are mapped to the MSP group, to the tenant account. When a certificate is removed from the **Device > Access Points > WLANs >Show Advanced > Security > Certificate Usage** section in the group dashboard in MSP, the respective certificate is also removed from the tenant's **Certificates Store**, if the certificate is mapped to the tenant's default group and is no longer used by the tenant. If the certificate is used by any of the tenant's non-default groups, the certificate is retained in the tenant's certificate store, even if the certificate is removed from the MSP. The **Device>Access Points> WLANs>Show Advanced >Security> Certificate Usage** menu is displayed only when you select a group from the filter.

Navigating to the Tenant Account

MSP users with administrative privileges to tenant accounts can drill down to tenant accounts.

To drill down to a specific tenant account:

1. In the **Network Operations** app, set the filter to **All Groups**.
2. Under **Manage**, click **Overview** to display the **Dashboard**.
   The **Dashboard** page includes the following sections:
   - Dashboard summary bar
   - Overview and trends for customers
3. In the **Customers | Overview** table, click the tenant account name and click **Expand**.
   The tenant account details window is displayed. Close the window.
4. To go to the tenant account, click on the tenant account name.
   The tenant account is displayed in Standard Enterprise Mode.

To return to the MSP view, click **Return to MSP View**. Aruba recommends that you not use the **Back** button of the web browser to go back to the MSP view.

Points to Note:

- The group attached to tenant account in the MSP mode shows up as a default group for the users of the tenant account.
- Configuration changes to the group attached to a tenant account in the MSP mode are applied to the default group in the interface displayed for the tenant accounts.
- The administrators can add users to a tenant account using the **Users & Roles** menu in the **Global Settings** app.
- Tenant account administrators can allow or prevent user access to specific groups by configuring custom roles.

MSP Alerts

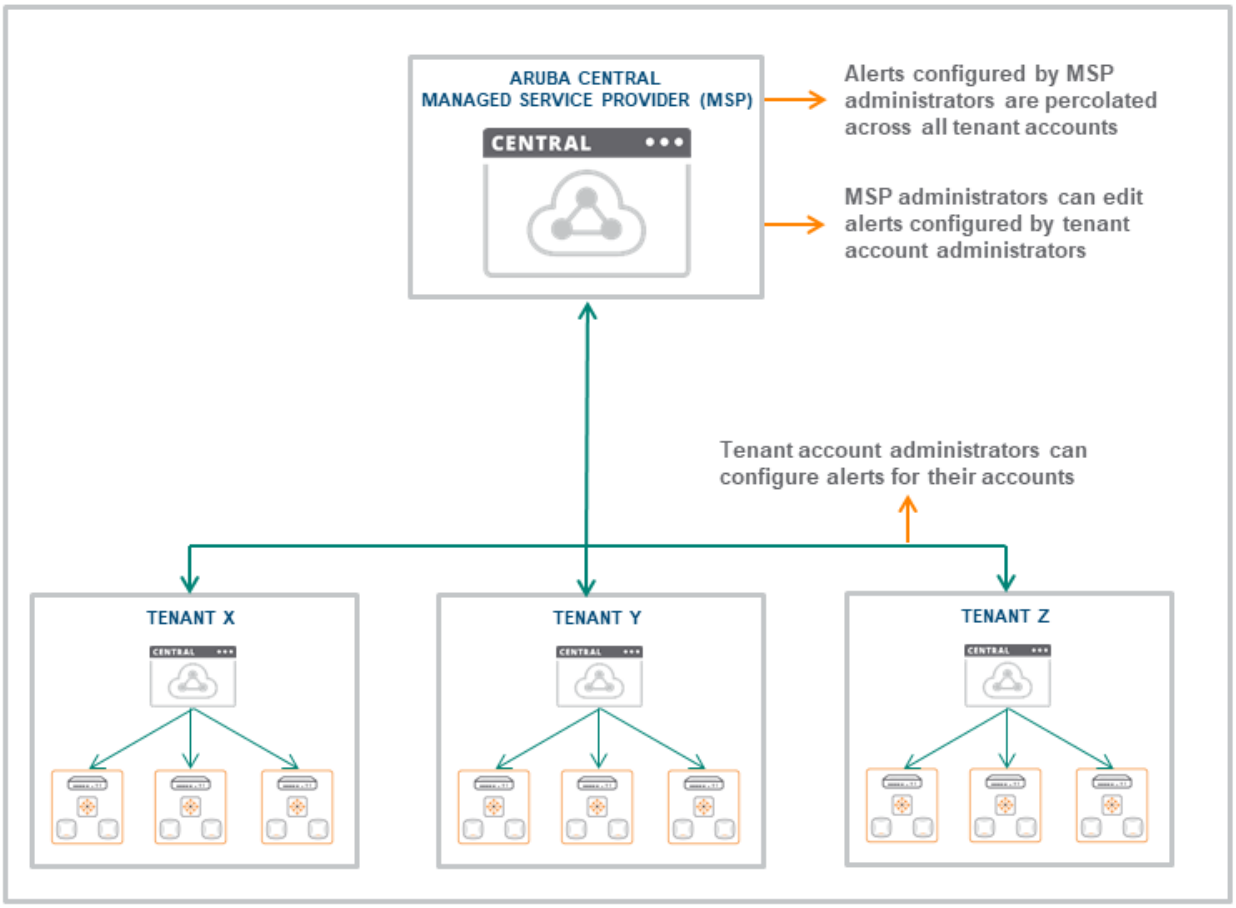
Aruba Central MSP mode enables administrators to trigger alerts when tenant provisioning, network, device, or user management events occur. An MSP administrator can configure alerts at the MSP level which percolate down to all tenant accounts managed by the MSP. For example, if the MSP administrator has configured an alert to be triggered when an AP is disconnected, the MSP is notified when an AP is disconnected in any of the tenant networks managed by the MSP. This allows for faster reactive support and makes monitoring and troubleshooting easy across multiple tenant accounts.

The MSP administrator can configure additional alerts at the tenant account level. At the tenant account level, alerts can be configured based on groups, labels, sites, or devices. Tenant account administrators can also configure additional alerts for their account. In this case, the alert is triggered only for the corresponding tenant account.

The MSP administrator can edit an alert configured by the tenant account administrator. However, the tenant account administrator cannot edit an alert created by the MSP administrator.

MSP level and tenant level alert configurations are managed separately. For example, if an alert is configured and enabled at both the MSP level and tenant level, two separate notifications are triggered for the event.

Figure 128 *MSP Alerts*



This section includes the following topics:

- Viewing MSP Alerts Dashboard
- MSP Alerts in List View
- MSP Alerts in Summary View
- MSP Alerts in Config View

Viewing MSP Alerts Dashboard

1. In the **Network Operations** app, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.

   The **Alerts** dashboard enables you to configure, view, and acknowledge alerts. The dashboard has three views:

- Alerts in **List** View
- Alerts in **Summary** View
- Alerts in **Config** View

3. The **Search** bar allows you to search for alerts by tenant account. Enter the name of the tenant account and select the tenant account from the list.
4. To view the list of alerts, click the **List** icon.
   a. The list view displays the number of alerts in the following categories:
      - **Critical**
      - **Major**
      - **Minor**
      - **Warning**
   b. Click **Acknowledge All** to acknowledge all the alerts at once.
   c. Enable the **Show Acknowledged Alerts** button to display the list of acknowledged alerts.
   d. Clicking icon enables you to customize the **Alerts** table columns or set it to the default view.
5. To view detailed graphs about the alerts, click the **Summary** icon . Select each tab, **All**, **Access Points**, **Switches**, or **Gateways** to view the graphs pertaining to each device type.
6. To configure alerts, click the **Config** icon. For more information, see xxx.

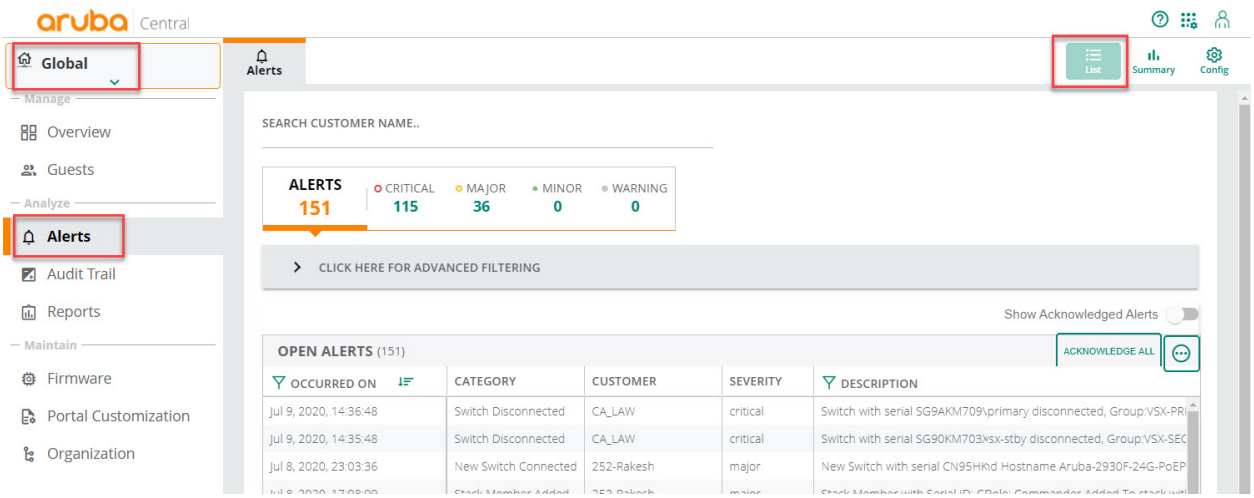
MSP Alerts in List View

The MSP Alerts page in list view displays a list of alerts for all customers associated with the MSP account.

Use the **Search Customer Name** field to filter alerts by customer name.

The Alerts summary bar displays a list of all the alerts categorized by severity level. You can click on any of the categories to display the list of alerts for that category.

Figure 129 *MSP Alerts in List View*



All the alerts are displayed in a tabular format and displays the following information:

Table 112: *Viewing the MSP Alerts in List View*

Data Pane Content	Description
Occurred On	Timestamp of the alert. Use the sort option to sort the alerts by date and time.

Data Pane Content	Description
Category	Displays the category of the alert. Use the filter option to filter the alert by category.
Label	Displays the label name of the alert.
Site	Displays the site name of the alert.
Customer	Displays the customer name of the alert.
Group	Displays the group name of the alert.
Severity	Displays the severity level of the alert. The severity can be Critical, Major, Minor, or Warning.
Description	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

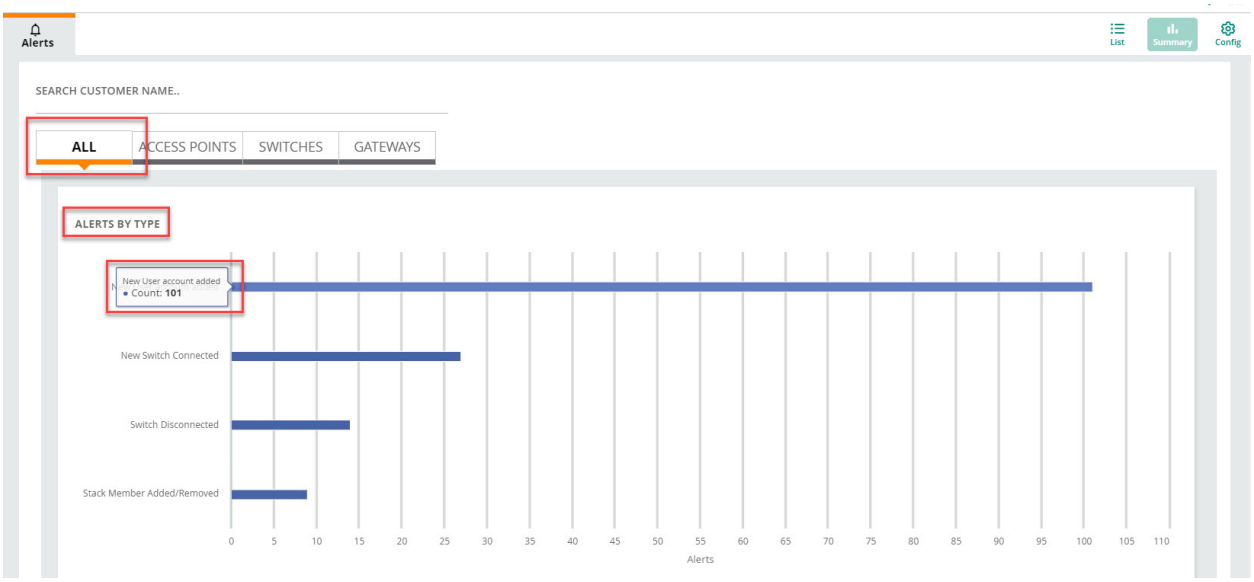
MSP Alerts in Summary View

The **Summary** view lists all the alerts in charts.

The available charts are:

- **Alerts by Type**—This horizontal bar chart plots the number of alerts versus the category of alerts. You can hover over a bar to get the exact data for the number of alerts for that category. Clicking on a bar redirects you to the list view for that category of alerts. An example is displayed in the next image.
- **Alerts by Severity**—This vertical bar chart plots the number of alerts versus the severity of alerts. You can hover over a bar to get the exact data for the number of alerts for that severity. Clicking on a bar redirects you to the list view for that severity of alerts.

Figure 130 *Alerts by Type Chart in MSP Alerts Summary View*



Select each tab, **All**, **Access Points**, **Switches**, or **Gateways** to view the graphs pertaining to each device type.

MSP Alerts in Config View

The **Alerts** page in **Config** view enables you to configure alerts. You can configure alerts at the MSP level and the tenant account level.

Configuring Alerts at the MSP Level

To configure alerts at the MSP level, complete the following steps:

1. In the **Network Operations** app, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.
3. Click the **Config** icon .

At the MSP level, you cannot configure alerts based on groups, labels, sites, or devices.

4. Use the tabs to navigate between the alert categories. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:
      - Virtual Controller Disconnected
      - Rogue AP Detected
      - New User Account Added
      - Switch Detected
      - Switch Disconnected
   b. **Notification Options**—See Alert Notification Delivery Options.
      - Click **Save**.
      - **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s).

Configuring Alerts at the Tenant Account Level

To configure alerts at the tenant account level, complete the following steps:

1. Navigate to the tenant account. See Navigating to the Tenant Account.
2. In the **Network Operations** app, set the filter to a group or a device.
3. To configure alerts, click the settings icon under **Analyze** > **Alerts & Events**. By default, the **Alerts & Events** > **User** category is displayed.
4. Use the tabs to navigate between the alert categories. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:
      - Virtual Controller Disconnected
      - Rogue AP Detected
      - New User Account Added
      - Switch Detected
      - Switch Disconnected

For a few alerts, you can configure threshold value for one or more alert severities. To set the threshold value, select the alert and in the **exceeds** text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

b. **Duration**—Enter the duration in minutes.
c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:
   - **Group**—Select a group to limit the alert to a specific group.
   - **Label**—Select a label to limit the alert to a specific label.
   - **Device**—Select a device to limit the alert to a specific device.
   - **Sites**—Select a site to limit the alert to a specific site.
d. **Notification Options**
   - **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.
   - **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list.
e. Click **Save**.
f. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the pag

Viewing Enabled Alerts

To view alerts enabled at the MSP level or tenant account level, do the following:

1. In the **Network Operations** app, filter **All Groups**.
2. Under **Analyze**, click **Alerts** to display the **Alerts** dashboard.
3. On the **Alerts** page, click **Enabled**.

   The **Enabled** tab lists the alerts that you have enabled. Click the tabs to see enabled alerts for each category.

Alert Notification Delivery Options

When you configure an alert, you can select how you want to be notified when an alert is generated. Aruba Central supports the following notification types:

- **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses; separate each value with a comma.
- **Webhook**—Select the **Webhook** check box and select the desired Webhooks from the drop-down list. Before you select this option, you must create Webhooks. For more information about creating and modifying Webhooks, see the Aruba Central Online documentation.

MSP Audit Trails

The Audit Trail page shows the logs for all the device management, configuration, and user management events triggered in Aruba Central.

You can search or filter the audit trail records based on any of the following columns:

- Occurred on (Custom Range)
- Username

- IP Address
- Category
- Description
- Target
- Source

Viewing the Audit Trail Page

To view the audit trail log details in Aruba Central MSP mode:

1. From the Network Operations app, set the filter to **All Groups**.
2. Under **Analyze**, click **Audit Trail**.
3. Adjust the time filter to get the display for the required time range.

   The Audit Trail logs are displayed for the following types of operations in the MSP:
   - Addition, modification, and deletion of tenant accounts
   - Addition, modification and deletion of users associated with a tenant account
   - Subscription assignment to devices
   - Modification of groups associated with a tenant account
   - Configuration push, override , and updates for the devices associated with a tenant account
   - Addition, modification, and deletion of MSP admin users
   - License reconciliation

The Audit Trail page in the MSP mode displays the following information:
Table 113: *Audit Trail Pane in the MSP Mode*

Parameter	Description
Occurred On	Time stamp of the events for which the audit trails are shown. Use the filter option to select a specific time range to display the events.
Username	The username of the admin user who applied the changes.
IP Address	IP address of the client device.
Category	Type of modification and the affected device management category. See Classification of Audit Trails.
Target	The group, device, or tenant account to which the changes were applied.
Source	The tenant account in which the changes occurred.
Description	A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click to view the complete details of the event. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.

Classification of Audit Trails

The audit trail is classified according to the type of modification and the affected device management category. The category can be one of the following:

- Configuration
- Firmware Management
- Reboot
- Device Management
- Templates
- User Management
- Variables
- Label Management
- MSP
- Guest
- Groups
- Subscription Management
- API Gateway
- RBAC
- Sites Management
- SAML Profile
- User Activity
- Federated User Activity
- Alert Configuration
- Install Manager
- Tools

MSP Reports

The MSP **Reports** page enables you to create reports. You can configure these reports to run on demand or periodically. You must have read and write privileges or you must be an Admin user to create reports. The **Reports** page is only applicable to the global MSP dashboard.

MSP reports are generated at the end of day, so the current day data is not available in the report. MSP reporting data is supported from version 2.5.0 onwards, the data is available only after an upgrade to version 2.5.0 or later. Data prior to the 2.5.0 upgrade is not available in the report.

Viewing the MSP Reports Page

To navigate to the **Reports** page, complete the following procedure:

1. From the **Network Operations** app, set the filter to **All Groups**.
   The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.
   The **Reports** dashboard is displayed.
   The **Reports** dashboard has the following sections:
   - **Browse**—Explore, email, download, or delete generated reports.
     Displays the number of generated reports.
     Click **Browse** to displays the **Reports** page in **List** view.
   - **Manage**—Edit or delete scheduled reports.
     Displays the number of scheduled reports.

Click **Manage** to displays the **Reports** page in **Config** view.
In the **Config** view, click + to generate a new report.

- **Create**—Creates a report that can be run instantly or periodically.
  Displays the number of report categories and the number of report types.
  Click **Create** to generate a new report. Currently, only **Device and Subscription Inventory** reports are supported in MSP.

Types of Reports

To access the **Reports** dashboard, set the filter to **All Groups** in the **Network Operations** app. Under **Analyze**, click **Reports**. Reports that are already run are listed under **Browse** > **Generated Reports**. If any report is yet to run, that report is available under **Browse** > **Scheduled Reports**.

The following table explains the parameters available in the **Device and Subscription Inventory** report.

Table 114: ***Device and Subscription Inventory*** *Report Description*

Parameter	Description
Access Points Inventory	The **Access Points Inventory** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of unassigned APs in the beginning of the time period. ■ **Purchased**—Number of APs purchased during the time period. ■ **Returned**—Number of APs returned by the tenants to the customer during the time period. ■ **Assigned**—Number of APs assigned to the tenants during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned)
Switch Inventory	The **Switch Inventory** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of unassigned switches in the beginning of the time period. ■ **Purchased**—Number of switches purchased during the time period. ■ **Returned**—Number of switches returned by the tenants to the customer during the time period. ■ **Assigned**—Number of switches assigned to the tenants during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned)
Gateway Inventory	The **Gateway Inventory** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of unassigned gateways in the beginning of the time period. ■ **Purchased**—Number of gateways purchased during the time period. ■ **Returned**—Number of gateways returned by the tenants to the customer during the time period.

Parameter	Description
	▪ **Assigned**—Number of gateways assigned to the tenants during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned)
Device Management License	The **Device Management License** page lists the following options both in table and graph form: ▪ **Opening Stock**—Total number of all licenses available in the beginning of the time period. ▪ **Purchased**—Number of licenses purchased during the time period. ▪ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ▪ **Assigned**—Number of licenses assigned to the tenants during the time period. ▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)
Gateway Foundation License	The **Gateway Foundation License** page lists the following options both in table and graph form: ▪ **Opening Stock**—Total number of licenses in the beginning of the time period. ▪ **Purchased**—Number of licenses purchased during the time period. ▪ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ▪ **Assigned**—Number of licenses assigned to the tenants during the time period. ▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)
Gateway Advanced License	The **Gateway Advanced License** page lists the following options both in table and graph form: ▪ **Opening Stock**—Total number of licenses in the beginning of the time period. ▪ **Purchased**—Number of licenses purchased during the time period. ▪ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ▪ **Assigned**—Number of licenses assigned to the tenants during the time period. ▪ **Expired**—Number of licenses that expired during the time period. ▪ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)

Parameter	Description
Gateway Base License	The **Gateway Base License** page lists the following options both in table and graph form: ■ **Opening**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)
Access Points Foundation License	The **Access Points Foundation License** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)
Access Points Advanced License	The **Access Points Advanced License** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)
Switch Foundation License	The **Switch Foundation License** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of licenses in the beginning of the time period.

Parameter	Description
	■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)
Switch Advanced License	The **Switch Advanced License** page lists the following options both in table and graph form: ■ **Opening Stock**—Total number of licenses in the beginning of the time period. ■ **Purchased**—Number of licenses purchased during the time period. ■ **Returned**—Number of licenses returned by the tenants to the customer during the time period. ■ **Assigned**—Number of licenses assigned to the tenants during the time period. ■ **Expired**—Number of licenses that expired during the time period. ■ **Closing Stock**—Total of (Opening + Purchased + Returned - Assigned -Expired)

The following table explains the parameters available in **Generated Reports** .

Table 115: ***Generated Reports*** *Description*

Parameter	Description
Title	Name of the report.
Date Run	Time when the report was last run. For **Scheduled Reports**, this is replaced by Next Run which indicates the time when the report will run in the future.
Scope	List of devices or subscription for which the report was run.
Report Type	Type of report, currently the only supported value is MSP Inventory.
Created by	Email address of the user who created the report.

The following table explains the parameters available in **Scheduled Reports**

Table 116: *Scheduled Reports* Description

Parameter	Description
Title	Name of the report.
Next Run	Time when the report will run in the future.
Status	Status of the report, whether **scheduled**, **failed**, **running**, **rerun**, or **waiting**.
Scope	List of devices or subscription for which the report was run.
Report Type	Type of report, currently the only supported value is MSP Inventory.
Recurrence	Time period of the scheduled report.
Created by	Email address of the user who created the report.

Creating a Report

The MSP **Reports** page in **Summary** view enables you to browse, manage, and create reports. To create a report, perform the following steps:

1. From the **Network Operations** app, set the filter to **All Groups**.
   The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.
   The **Reports** page is displayed.
3. In the **Reports** page, click the **Summary** icon. Click the **Create** tile.
   Else, click the **Config** view and then click the + sign in the **Scheduled Reports** page.
   The **Infrastructure** page is displayed.
4. Under **Infrastructure**, click **Device and Subscription Inventory** and then click **Next**.
5. Under **Scope**, select **All** or a combination of the other choices and then click **Next**:
   - **All**—Generates a report for all access points, gateways, switches, and subscriptions.
   - **Access Points**—Generates a report only for access points.
   - **Gateways**—Generates a report only for gateways.
   - **Switches**—Generates a report only for switches.
   - **Subscriptions**—Generates a report only for subscriptions.
6. Under **Report period**, select one of the following options and then click **Next**:
   - **Last Month**
   - **Last 3 Months**
   - **Last 6 Months**
   - **Custom Range**
7. Select one of the recurrent options:
   - **One Time (now)**
   - **One Time (later)**
   - **Every day**
   - **Every week**
   - **Every month**

8. For **Report Information**, enter the title of the report and an email address where the report will be delivered.
9. Select the format as either **PDF** or **CSV**.
10. Click **Generate**.
11. If you select **One Time** as an option in step 6, the report is available in the **Generated** view as **Generated Reports**. If the report is yet to run, the report is available under **Scheduled Reports**.

Editing a Report

To edit a report, complete the following procedure:

1. From the **Network Operations** app, set the filter to **All Groups**.
   The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.
   The **Reports** page is displayed.
3. In the **Reports** page, click the **Scheduled** view icon.
   The **Scheduled Reports** dashboard is displayed.
4. Under **Scheduled Reports**, select the report you want to edit and then click the edit icon.
   The **Infrastructure** page is displayed.
5. Under **Scope**, select one or a combination of the following choices and then click **Next**:
   - **All**—Generates a report for all access points, gateways, switches, and subscriptions.
   - **Access Points**—Generates a report only for access points.
   - **Gateways**—Generates a report only for gateways.
   - **Switches**—Generates a report only for switches.
   - **Subscriptions**—Generates a report only for subscriptions.
6. Under **Report period**, select one of the following options and then click **Next**
   - **Last Month**
   - **Last 3 Months**
   - **Last 6 Months**
   - **Custom Range**
7. Select one of the recurrent options:
   - **One Time (now)**
   - **One Time (later)**
   - **Every day**
   - **Every week**
   - **Every month**
8. For **Report Information**, enter the title of the report and an email address where the report will be delivered.
9. Select the format as either **PDF** or **CSV**.
10. Click **Generate**.
11. If you select **One Time** as an option, the report is available under **Generated Reports**. If the report is yet to run, the report is available under **Scheduled Reports**.

Viewing or Downloading a Report

To view or download a report, complete the following procedure:

1. From the **Network Operations** app, set the filter to **All Groups**.
   The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.
   The **Reports** page is displayed.
3. In the **Reports** page, click the **Generated** view icon.
   The **Generated Reports** dashboard is displayed.
4. Under **Generated Reports**, select the report you want to view or download.
   - To view the report online, click the report name.
   - To download the report, click the report and then click the download icon for either the CSV or PDF file.
   - To email the report, click the email to icon.
   - To delete the report, click the delete icon.

Deleting a Report or Multiple Reports

To delete a report or multiple reports, complete the following procedure:

1. From the **Network Operations** app, set the filter to **All Groups**.
   The **Global** dashboard is displayed.
2. Under **Analyze**, click **Reports**.
   The **Reports** page is displayed.
3. In the **Reports** page, click the **Generated** view icon.
   Reports that are already run are listed under **Generated Reports**. If any report is yet to run, that report is available under **Scheduled Reports**.
4. Select the report you want to delete and then click the delete icon.
   You can select multiple reports to delete.

Firmware Upgrades for MSP Mode

The **Firmware** menu under **Maintenance** displays a list of tenant accounts and the status of the devices assigned to the tenant accounts.

Viewing the Firmware Dashboard

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Firmware**.
3. Select one of the following tabs: **Access Points**, **Switch-MAS**, **Switch-Aruba**, or **Gateways**

The **Firmware** menu displays the **Access Points**, **Switch-MAS**, **Switch-Aruba**, and **Gateways** tabs that list all the tenants with firmware and compliance status for each of the device types.

The following table displays the Firmware dashboard for **Access Points**, the table for the other tabs are similar:

Table 117: *Firmware Dashboard Parameters for APs Tab*

Date Pane Item	Description
Customer Name	Name of the customer.
Upgrade Status	Status of the devices associated with the tenant account. This column displays one of the following: ■ Upgrading ■ Scheduling in progress ■ Downloading firmware ■ Upgrade successful, ready for reboot ■ Upgrade successful and rebooting AP ■ Upgrade in process ■ Firmware upgrade failed. Please try again. ■ Rebooting ■ Live upgrade initiating ■ Live upgrade initiated
Compliance Status	Status of compliance for the tenant. This column indicates the compliance status such as **Set**, **Not Set**, or **Compliance scheduled on <date and time>** for a specific tenant.
Manage Firmware Compliance	Enables you to plan upgrades. See Managing Firmware Compliance Based on Tenant Account.

Managing Firmware Compliance Based on Device Tabs

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Firmware**.
3. Select one of the following tabs: **Access Points**, **Switch-MAS**, **Switch-Aruba**, or **Gateways**
4. Click **Manage Firmware Compliance** at the top right.

   The **Manage Firmware Compliance** window opens.
5. Select the firmware version and the time for upgrade.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade. The **Auto Reboot** option is not available for **Access Points**.
7. Select one of the following options as required:
   - Select **Now** to set the compliance to be carried out immediately.
   - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**.
9. MSP initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

Managing Firmware Compliance Based on Tenant Account

1. In the **Network Operations** app, use the filter to select **All Groups**.
2. Under **Maintain**, click **Firmware**.
3. Select one of the following tabs: **Access Points**, **Switch-MAS**, **Switch-Aruba**, or **Gateways**

4. From the dashboard, select one or more customer name and click **Continue**.
5. The **Upgrade <Device Type> Firmware** page is displayed.

You can click the check box on the table heading of tenant details table to include all the tenants for the firmware upgrade listed in the current page. To manually upgrade firmware for specific tenants, select the check box corresponding to the tenant that requires a manual firmware upgrade in the tenant details table. Clicking the **Continue** button displays the **Upgrade <Device Type> Firmware** page. The **Filter by upgrade status** drop-down list disappears when the **Update All** button is clicked.

6. Perform the following actions:

Table 118: *Upgrade <Device Type> Firmware*

Component	Description
Firmware Version	The firmware version to which the tenant is required to be upgraded. Aruba Central considers the recommended firmware version as the default if no version is specified in the field.
Auto Reboot	Select this check box to reboot the device automatically after the download of the new version. **NOTE:** The **Auto Reboot** option is not applicable for Instant APs.
Schedule	Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time. ▪ **Now**—To set the firmware upgrade to be carried out immediately. ▪ **Later Date**—To set the firmware upgrade to take place at a later date and time. Click the **Upgrade** button to upgrade the firmware.
Cancel	Click this button to cancel the settings and go back to the **Maintenance > Firmware** page.

7. The **Firmware** page also displays the **Cancel All** button. Click **Cancel All** button to cancel the manual firmware upgrade for all the tenants in the MSP mode.

The compliance upgrade settings for the tenants and the tenant devices takes precedence over the manual firmware upgrade. The scheduled manual firmware upgrade becomes invalid when you set or schedule the compliance upgrade.

Firmware Upgrade in MSP Through NB API

Aruba Central provides an option to upgrade firmware for all the tenants mapped to the MSP through APIs in **Maintenance > API Gateway**.

To set or get the country code at group level through API:

1. In the **Account Home** page, click **API Gateway**.
2. Click **System Apps & Tokens** tab and generate a token key.
3. Download and copy the generated token.
4. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page opens.

5. On the left navigation pane, select **Firmware** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. In **Firmware Management,** the following options are displayed**:**
   - **[POST] /firmware/v1/msp/upgrade**—Upgrades firmware at the MSP level. To configure the firmware upgrade for all the tenants of a specific device type, enter the following inputs in the corresponding labels of the script

```
 {
  "firmware_scheduled_at": 0,
  "device_type": "string",
  "firmware_version": "string",
  "reboot": true,
  "exclude_groups": "string",
  "exclude_customers": "string"
}:
```

Table 119: *Firmware Upgrade at MSP level*

Label	Description
Firmware_ scheduled_ at	The time at which the firmware upgrade must be initiated. The value entered in this field is the count in seconds from the current time.
Device_ type	The type of device for which the firmware upgrade must be initiated.
Firmware_ version	The firmware version to which the device is required to be upgraded. Aruba Central takes the recommended firmware version as the default version if no version is specified in the field.
Reboot	True or false value to enable or disable the reboot of device once the firmware upgrade build is downloaded. **NOTE:** The **Reboot** option is not applicable for Instant APs.
Exclude-groups	The list of groups to be excluded from firmware upgrade.
Exclude_ customers	The list of tenants to be excluded from firmware upgrade.

   - **[POST] /firmware/v1/msp/upgrade/customers/{customer_id}**—Upgrades firmware at the tenant level. To configure the firmware upgrade for a specific tenant of a specific device type, enter the following inputs in the corresponding labels of the script

```
{
  "firmware_scheduled_at": 0,
  "device_type": "string",
  "firmware_version": "string",
  "reboot": true,
  "exclude_groups": "string"
}.
```

Table 120: *Firmware Upgrade at the Tenant level*

Label	Description
Firmware_ scheduled_ at	The time at which the firmware upgrade must be initiated. The value entered in this field is the count in seconds from the current time.
Device_ type	The type of device for which the firmware upgrade must be initiated.
Firmware_ version	The firmware version to which the device is required to be upgraded. Aruba Central takes the recommended firmware version as the default version if no version is specified in the field.
Reboot	True or false value to enable or disable the reboot of device once the firmware upgrade build is downloaded. **NOTE:** The **Reboot** option is not applicable for Instant APs.
Exclude-groups	List of groups to be excluded from firmware upgrade.

- **[POST] /firmware/v2/msp/upgrade/cancel**—Cancels a scheduled upgrade firmware of devices specified by device_type. Enter the following inputs in the corresponding labels of the script

```
{
  "device_type": "string",
  "exclude_groups": "string",
  "exclude_customers": "string"
}.
```

Table 121: *Cancel Scheduled Upgrade at MSP Level*

Label	Description
Device_type	The type of device for which the firmware upgrade schedule must be canceled.
Exclude-groups	List of groups to be excluded while canceling scheduled upgrade.
Exclude_customers	List of customer IDs to be excluded while canceling scheduled upgrade.

- **[POST] /firmware/v2/msp/upgrade/customers/{customer_id}/cancel**—Cancels a scheduled upgrade firmware of devices specified by device_type for a tenant. Enter the following inputs in the corresponding labels of the script

```
{
  "device_type": "string",
  "exclude_groups": "string"
}.
```

Table 122: *Cancel Scheduled Upgrade at the Tenant Level*

Label	Description
Device_type	The type of device for which the firmware schedule must be canceled.
Exclude-groups	List of groups to be excluded while canceling scheduled upgrade.

The following APIs that include **v1** version will be deprecated from API Gateway and is replaced with **v2** version:

- **[POST] /firmware/v1/msp/upgrade/cancel**
- **[POST] /firmware/v1/msp/upgrade/customers/{customer_id}/cancel**

Order of Precedence For Compliance

The devices in the MSP mode inherits the compliance set in the following order of precedence from highest to lowest:

- Group level
- Tenant level
- MSP level

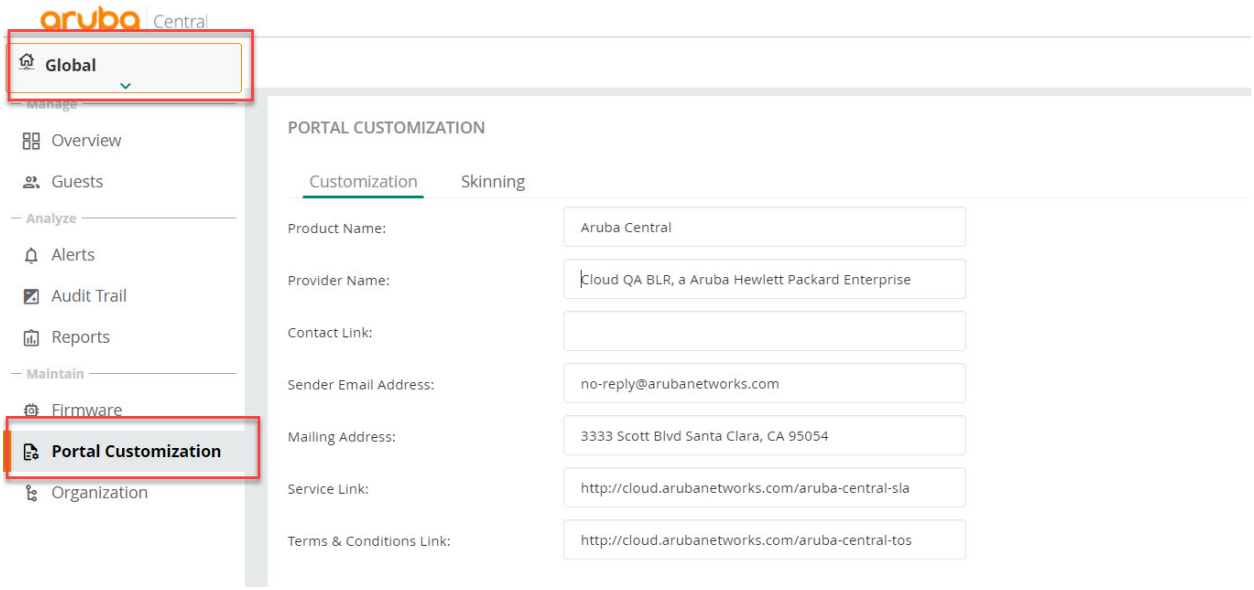
The devices in MSP mode exhibits the following behavior related to compliance settings:

- The compliance set at the group level overrides the compliance set at the tenant level or MSP level. If there is no compliance at the group level, the devices in the group inherits the compliance configured at the tenant level.
- The compliance set at the tenant level overrides the compliance set at the MSP level. If there is no compliance at the tenant level and group level, the tenant devices inherit the compliance configured at the MSP level.

Customizing the Portal in MSP Mode

The **Portal Customization** page enables you to customize the look and feel of the user interface and the email notifications sent to the customers and users. For example, you can use your company logo in the user interface and company address in the email notifications sent to the customers or users.

Figure 131 *Customizing the Portal in the Network Operations App*



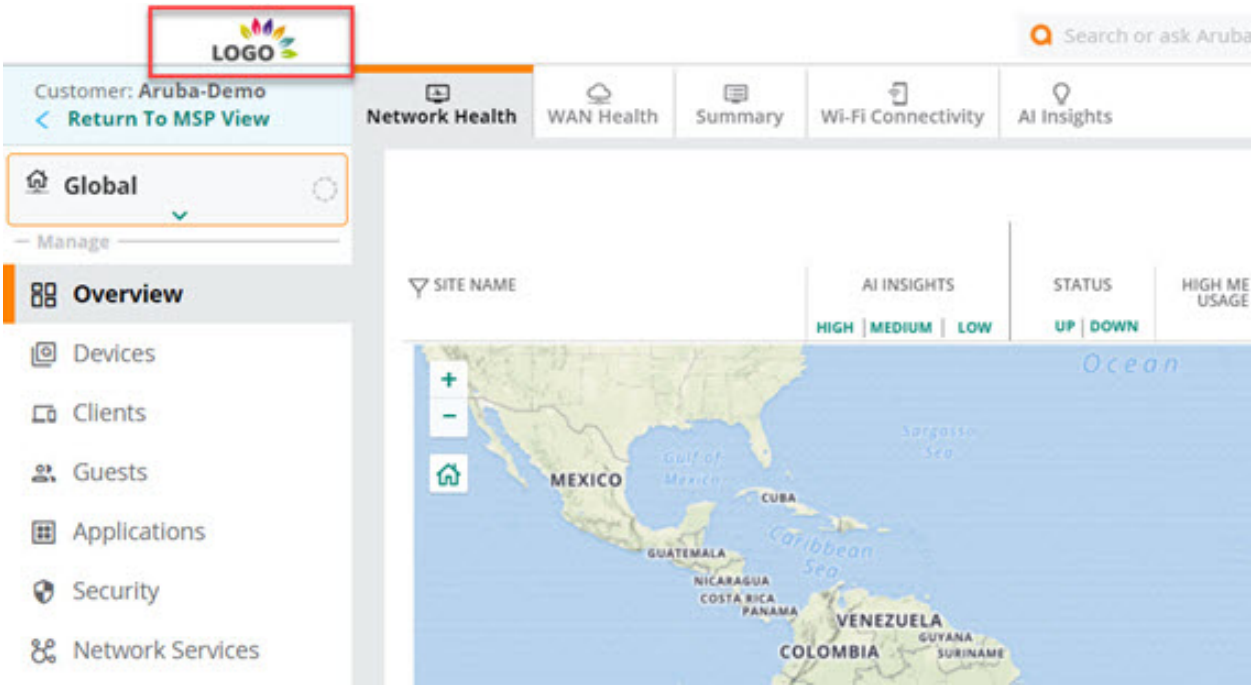
To customize the look and feel of the portal, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Portal Customization**.
3. The **Portal Customization** page is displayed.
4. Under **Customization**, configure the following information:
   - **Product Name**—Name of the product.
   - **Provider Name**—Name of the company.
   - **Contact Link**—The URL to the company website that shows the contact address of the company.
   - **Sender Email Address**—The email address from which the notifications are sent.
   - **Mailing Address**—The postal address of the company.
   - **Service Link**—The URL to the company website showing the service related information.
   - **Terms and Conditions Link**—The URL to the company website listing the terms and conditions.
5. If you want customize the logo of your portal, click **Skinning**.
6. Browse to your local directory and upload the logo image.
7. Click **Save Settings**.

The customized logo is displayed in the following pages:

- Tenant account—All the apps and pages applicable to the tenant. For more information about tenant accounts, see Provisioning Tenant Accounts.

Figure 132 *Sample Logo for a Customer Account*



- Email invite—Email invite sent while adding a new user. The email contains the registration link. For more information about adding a new user, see Adding a Custom Role in MSP Account Home.

MSP Deployment Models

The MSP mode supports multiple configuration constructs such as UI groups, template groups, local overrides, and so on. This section describes various MSP deployment models using examples. MSP supports the following deployment models:

- MSP Owns Devices and Subscriptions (Deployment Model 1)
- End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2)
- Hybrid MSP Deployment Model (Deployment Model 3)

MSP Owns Devices and Subscriptions (Deployment Model 1)

In this model, the MSP offers Network as a Service (NaaS). The MSP owns both the devices and subscriptions. The MSP acquires end-customers and manages the end-customer's network. The MSP temporarily assigns devices and subscriptions to end-customers for the duration of the managed service contract. Once the contract ends, the devices and the subscriptions are returned back to the MSP's common pool of resources and can be reassigned to another end-customer.

Setup and Provisioning

After the MSP purchases the devices and subscriptions, the MSP administrator has to do the following:

- Set up the Aruba Central account.
- Onboard devices.
- Assign device subscriptions and network services subscriptions.

MSPs can provide Network as a Service to end-customers using Aruba Central MSP mode capabilities. Aruba Central provides simplified provisioning. The **Overview** > **Dashboard** page under **Manage** in the MSP view allows you to add, view, edit, and delete tenant accounts. After adding a device, the MSP administrator must map the device to the tenant account for device management and monitoring operations.

After you create a tenant account, you can map the tenant to a group. The group associated to the tenant account in the MSP mode shows up as the default group for tenant account users. In the MSP mode, all configuration changes made to the group associated to the tenant account are applied to the default group on the tenant account.

Customizing the Portal

MSPs can customize their Aruba Central MSP portal and guest splash pages by uploading their own logo. The **Portal Customization** pane allows you to customize the look and feel of the user interface and the email notifications sent to customers and users. Aruba Central also allows MSPs to localize various pages to support a diverse customer market.

Monitoring and Reporting

Using the MSP Dashboard, MSPs can monitor and observe trends on end-customer networks.

MSPs can do the following from the MSP Dashboard:

- View total number of tenant accounts and consolidated device inventory and subscription status.
- View graphs representing the devices under management, tenant accounts added, and subscription renewal schedule
- Navigate to each tenant account.

Managing Firmware and Maintenance

MSPs can streamline and automate end-customer's network management while maintaining complete control. MSPs can perform one-click firmware updates or schedule specific updates, manage user accounts across end-customers with different levels of access and tag devices with labels to simplify firmware management and configuration.

Example Deployment Scenario

In this scenario, an MSP is offering the following wireless management services:

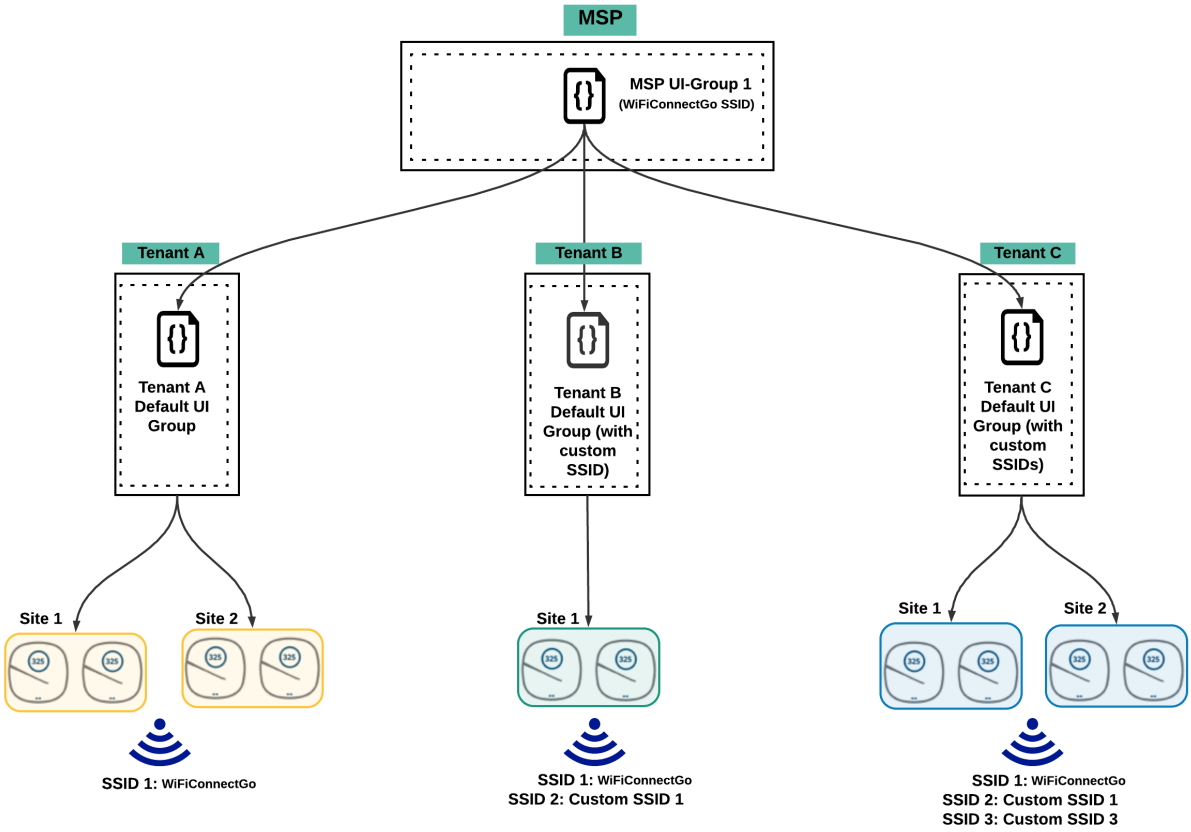
- **WiFiConnectGo**—In this program, for a monthly fee per Instant AP, customers part of this program agree to broadcast MSP's free public WiFi SSID **WiFiConnectGo**. Customers can add up to 15 additional custom SSIDs, including guest, of their own. Tenant account administrators are responsible for configuring any additional SSIDs and ongoing monitoring and maintenance. MSP is responsible for installing and bringing up the Instant AP only.
- **WiFiConnectGo-Plus**—In this program, for an additional monthly fee per Instant AP, customers part of this program need not broadcast the free public WiFi SSID **WiFiConnectGo**. Customers can add up to 15 custom SSIDs, including guest, of their own. MSP is responsible for installing Instant APs, configuring custom SSIDs, and ongoing monitoring and maintenance.

Configuring WiFiConnectGo Using Default UI Groups

Use this deployment model if your customer deployments are identical. UI groups support an inheritance model from MSP to tenant.

As shown in the following figure, MSP uses MSP UI groups to push SSID configuration to the default group in each tenant account. Tenants can choose to add additional custom SSIDs to the default group. All sites are mapped to the same default group.

Figure 133 *MSP Deployment Using Default UI Groups*

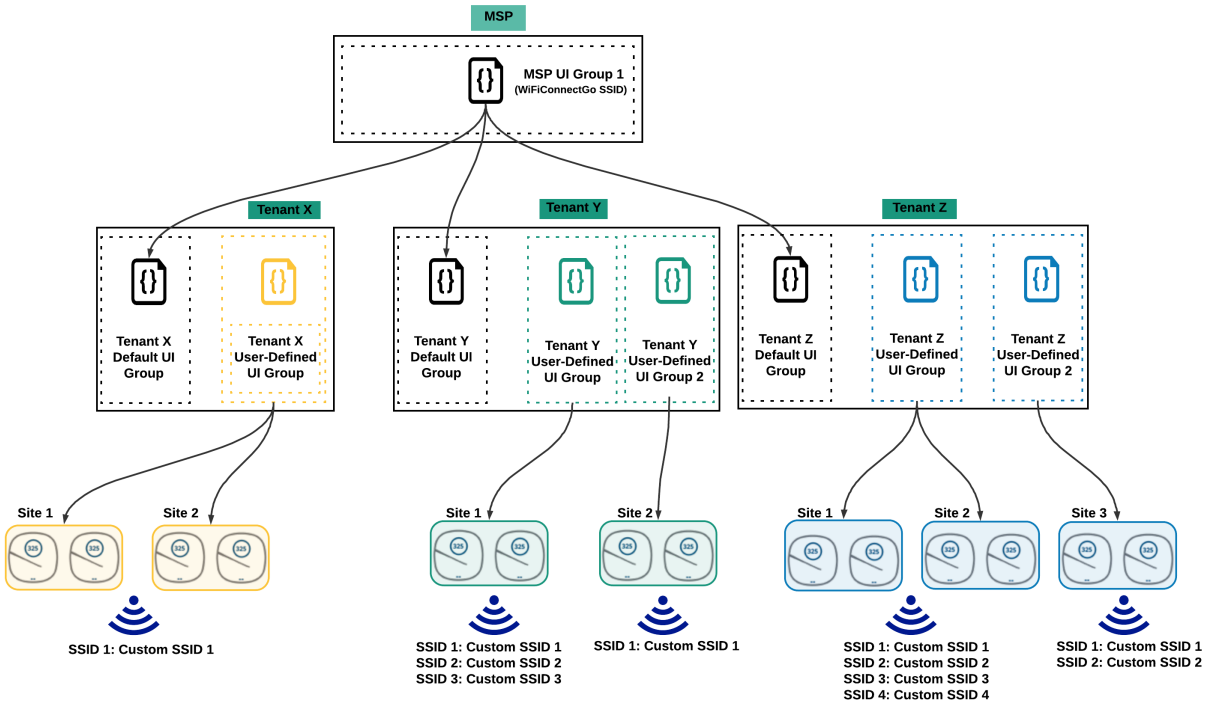


Configuring WiFiConnectGo-Plus Using User-Defined UI Groups

Use this deployment model if your customer deployments are unique and if you wish to use the Aruba Central user interface for configuring. UI groups support an inheritance model from MSP to tenant.

As shown in the following figure, each tenant has their own custom SSID configuration. In this scenario, the MSP administrator can create separate user-defined UI groups for each tenant. Sites with common SSID are mapped to the same UI group. MSP administrators can use the available UI group APIs add, modify, or remove allowed wireless configuration options.

Figure 134 *MSP Deployment Using User-Defined UI Groups*

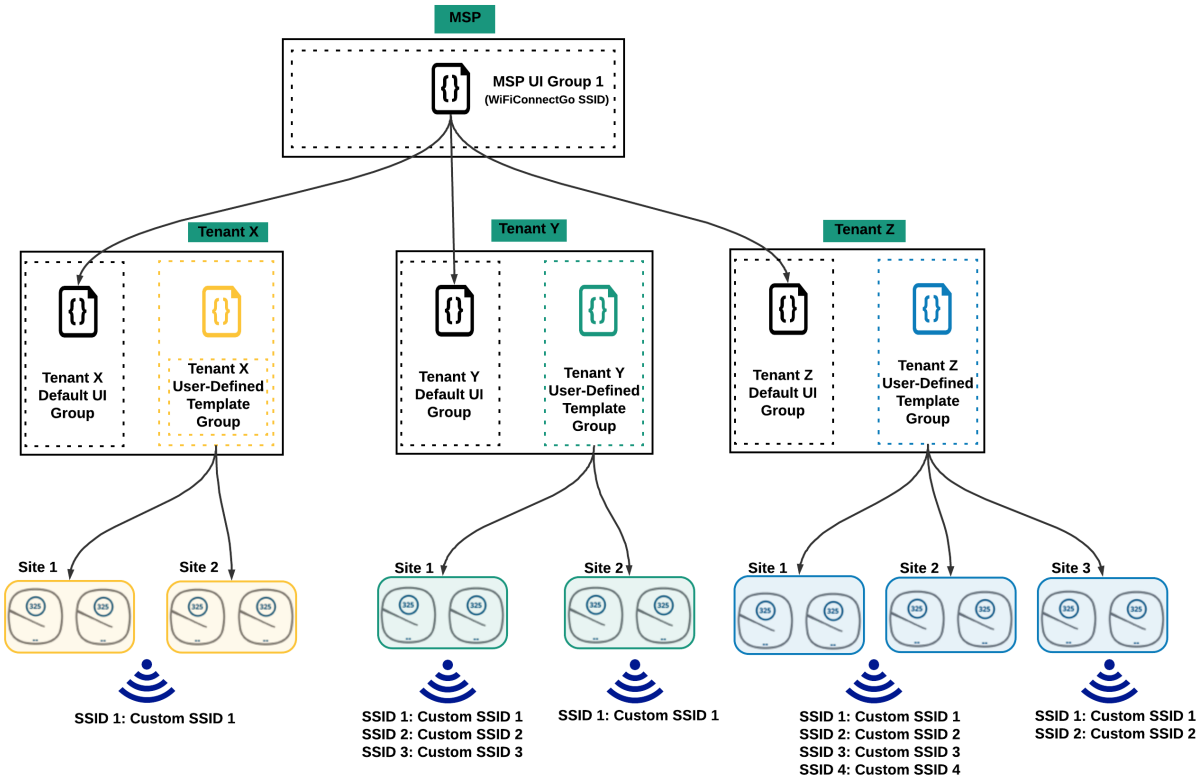


Configuring WiFiConnectGo-Plus Using Template Groups

As shown in the following figure, one template group is defined for each tenant and all devices are associated to the same group. Using the if/else conditional statements, you can push SSIDs to Instant APs selectively. MSP administrators can use the template and variable APIs to add, modify, or remove any wireless configuration.

You can use this deployment model if you wish to automate your customer deployments using Aruba CLIs and Aruba Central APIs.

Figure 135 *MSP Deployment Using Template Groups*



End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2)

NOTE

In this deployment model, the account type must be Standard Enterprise Mode. Aruba recommends that you contact your Aruba Central sales representative or the Aruba Central Support team if you are an MSP proposing this model to your end-customer.

In this model, the end-customer owns both the devices and subscriptions, but the MSP manages the end-customer's network. The end-customer can be one of the following:

- An existing Aruba customer who owns Aruba devices, but does not have an Aruba Central account.
- An existing Aruba customer who owns Aruba devices and is managing the network using Aruba Central.

In this model, to manage end-customer-owned devices and subscriptions, the MSP can use the Aruba Central Standard Enterprise mode.

The MSP need not create an Aruba Central account of their own, but can instead add their (MSP) administrator to the end-customer's Aruba Central account. The MSP administrator will only have access to each end-customer account.

Setup and Provisioning

The end-customer purchases the devices and subscriptions. The end-customer contacts the MSP to manage the network. As the devices and subscriptions are owned by the end-customer, the MSP uses the Aruba Central Standard Enterprise mode to set up and provision the tenant account.

The MSP has to request the end-customer to add the MSP administrator to their Aruba Central account. The MSP administrator can use the **Switch Customer** option to switch between end-customer accounts.

Monitoring and Reporting

As the MSP is not using the MSP mode, there is no single pane view of end-customer accounts managed by the MSP. The MSP has to monitor each end-customer individually. The MSP administrator has to use the Aruba Central Standard Enterprise mode to monitor the end-customer network.

Managing Firmware and Maintenance

The MSP has to use the **Firmware** menu under **Maintain** to view the latest supported firmware version of the device, details of the device, and the option to upgrade the device. The MSP administrator has to manage software upgrades for each end-customer individually.

Example Deployment Scenario

In this scenario, an MSP has to configure Instant APs and manage end-customer networks at two different sites. The following are the site details:

Site 1

```
Location: University Ave, Berkeley, CA
SSID Name: "WiFi_CE"
Security: WPA2-PSK
SSID Password: "password@123"
VLAN: 20
```

Site 2

```
Location: University Ave, Berkeley, CA
SSID Name: "WiFi_CE"
Security: WPA2-PSK
SSID Password: "password@123"
VLAN: 40
```

Considering the requirements, each site needs two Instant APs. The only difference between the sites is the VLAN ID.

Deployment Using User-Defined UI Groups

The MSP can configure Instant APs at both sites using user-defined UI groups. As the Wi-Fi configuration per site is different, one UI group must be created for each site.

For each site, the tenant account administrator has to do the following:

1. Create a new UI group for each site.
2. Configure the UI group with Wi-Fi settings specific to each site.
3. Map the Instant APs in each site to the respective UI group.

Points to Note:

- One user-defined UI group is created for each site.
- For any new site with a different VLAN ID, the tenant account administrator must create a new UI group.

- If a configuration change is required at all sites, the tenant account administrator must manually edit each UI group as each group is independent of the other. For example, to change the Wi-Fi SSID name from **WiFi_CE** to **WiFi_Secure_CE**, the tenant account administrator must edit UI group.

Deployment Using Template Groups

The MSP can configure Instant APs at both sites using template groups. The tenant account administrator can create a single template group for both sites with a variable file that differentiates the VLAN setting per device.

Template groups are not supported at the MSP level. However, template groups can be defined and managed at each tenant account individually.

For both sites, the tenant account administrator has to do the following:

1. Create one tenant template group.
2. Configure the newly created template group by uploading a base configuration with the **WiFi_CE** setting and a variable for the SSID VLAN.
3. Upload a variable file with unique entries for each Instant AP. For the Instant APs part of **Site 1**, the VLAN variable value is 20. For the Instant APs part of **Site 2**, the VLAN variable value is 40.
4. Map **Site 1** and **Site 2**Instant APs to the common template group.

Points to Note:

- One tenant template group is created for both sites.
- For every additional site with a different VLAN ID, the same template group can be used with a modified variable file.
- If a configuration change is required at all sites, the common template group can be updated and pushed to all sites. For example, to change the Wi-Fi SSID name from **WiFi_CE** to **WiFi_Secure_CE**, the tenant account administrator can edit the common template group and push the configuration changes to all sites.

Hybrid MSP Deployment Model (Deployment Model 3)

In this model, Aruba Central supports a hybrid deployment model for the MSP. The MSP can use the following deployment models in conjunction to manage the end-customers' network:

- MSP Owns Devices and Subscriptions (Deployment Model 1)—The MSP owns both the devices and subscriptions. The MSP acquires the tenants and uses the Aruba Central MSP mode to manage the tenant's network and monitors multiple tenant accounts using the MSP Dashboard.
- End-Customer Owns Both Devices and Subscriptions But MSP Manages (Deployment Model 2)—The MSP manages end-customer's network in which the end-customer owns both the devices and subscriptions. The MSP uses the Aruba Central Standard Enterprise mode to manage the network and the MSP administrator uses the **Switch Customer** option to navigate between different end-customer accounts.

In this deployment model if the end customer owns both devices and subscriptions, the account type must be Standard Enterprise Mode. Aruba recommends that you contact your Aruba Central sales representative or the Aruba Central Support team if you are an MSP proposing this model to your end-customer.

Frequently Asked Questions

How do I create an Aruba Central MSP account?

As MSP mode is an operational mode of the **Network Operations** app which is one of the apps in Aruba Central, the first step to create an MSP account is to create an Aruba Central account, subscribe only to the **Network Operations** app, and then enable **Managed Service Mode**.

- Sign up for Aruba Central evaluation here.
- Enable MSP mode.

Should tenants sign up for an Aruba Central account as well?

No. With MSP mode enabled, the MSP administrator manages the creation and deletion of tenant accounts. After a tenant account is created, the MSP administrator can add tenant users to the account.

To create a tenant user, the MSP administrator must provide a valid email address for the user. A verification email is sent to this email address.

Tenant users have access to their individual tenant account only. Tenant users do not have access to other tenant accounts managed by the MSP.

Who owns the hardware and subscriptions?

In the MSP mode, all the hardware and subscriptions are owned by the MSP. The MSP temporarily assigns devices and their corresponding subscriptions to tenants for the duration of the managed service contract. When the contract ends, the devices and the subscriptions are returned back to the common pool of resources of the MSP and can be reassigned to another tenant.

Can existing Aruba Central customers migrate to an MSP account?

End customers who own their own devices and subscriptions cannot transfer ownership of the devices to an MSP. However, the MSP administrator can manage the end customer network.

What are the supported devices and architectures?

MSP supports all devices and architectures supported by Aruba Central.

See Supported APs and Supported Switches.

Aruba Central support wireless, wired, and SD-WAN deployments, either independently or in combination. For example, as an MSP, you can manage the following combinations:

- Customer environments having a wireless deployment.
- Customer environments having both wired and wireless deployments.
- Customer environments having an SD-WAN deployment.

Aruba Central does not support managing gateways at the MSP level. However, gateways can be configured and managed at the tenant account level.

Which group is the default group for the tenant account?

The MSP group associated to the Tenant account shows up as the default group for Tenant account users. All configuration changes made to the “MSP group” associated to the “Tenant account” are applied to the

default group on the Tenant account.

What are predefined user roles?

The **Users & Roles** tile under **Global Settings** in the **Account Home** page allows you to configure the following types of users with system-defined roles:

User Role	Standard Enterprise Mode	MSP Mode
admin	▪ Has full access to all devices. ▪ Can provision devices and enable access to application services. ▪ Can create or update users, groups, and labels.	▪ Has full access to tenant accounts. ▪ Can create, modify, provision, and manage tenant accounts.
readwrite	▪ Has access to the groups and devices assigned in the account. ▪ Can add, modify, configure, and delete a device in the account.	Can access and modify tenant accounts.
readonly	▪ Can view the groups and devices. ▪ Can view generated reports.	Can view tenant accounts.
guestoperator	▪ Can access and modify cloud guest splash page profiles. ▪ Can configure visitor accounts for the cloud guest splash page profiles.	▪ Can access and modify cloud guest splash page profiles. ▪ Can configure visitor accounts for the cloud guest splash page profiles.

What are custom user roles?

Along with the predefined user roles, Aruba Central allows you to create custom roles with specific security requirements and access control. However, only the users with the administrator role and privileges can create, modify, clone, or delete a custom role in Aruba Central.

With custom roles, you can configure access control at the application level and specify access rights to view or modify specific application services or modules. For example, you can create a custom role that allows access to a specific applications like Guest Access or network management and assign it to a user.

You can create a custom role with specific access to MSP modules. The **MSP** application allows users with administrator role and privileges to define user access to MSP modules such as Customer Management and Portal Customization. The MSP tenant account user does not have access to the **MSP** application. Even if a tenant account user is assigned a custom role having **MSP** application privileges, the tenant account user will not have access to the **MSP** application and **MSP** will not appear in the **Global Settings** > **Users & Roles** > **Roles** > **Allowed Applications** list.

What tasks can be performed by an MSP user and tenant user?

In the MSP mode, MSP users have a superset of administration options compared to tenant users.

An MSP administrator can perform the following administrative tasks:

- Tenant account management.
- Device and subscription management across all tenants.
- Monitoring and event management across all tenants.

- Configuration management across all tenants.
- User management across all tenants.
- API management for the MSP and across all tenants.

A tenant account administrator can perform the following administrative tasks for their respective tenant account only:

- Monitoring and event management.
- Configuration management.
- User management.
- API management.

Chapter 8
Instant APs

Instant APs offer an enterprise-grade networking solution with a simple setup. The WLAN solution with Instant APs supports simplified deployment, configuration, and management of Wi-Fi networks.

Instant APs run the Aruba Instant software that virtualizes Aruba Mobility Controller capabilities on 802.11 APs and offers a feature-rich enterprise-grade Wi-Fi solution. Instant APs are often deployed as a cluster. An Instant AP cluster includes a conductor AP and set of other APs that act as member APs.

In an Instant deployment scenario, only the first AP or the conductor AP that is connected to a provisioning network is configured. All other Instant APs in the same VLAN join the conductor AP inherit the configuration changes. The Instant AP clusters are configured through a common interface called Virtual Controller. A Virtual Controller represents the combined intelligence of the Instant APs in a cluster.

Supported Deployment Modes

Aruba Instant APs can be deployed in the following modes in Aruba Central:

- Cluster mode—In this mode, several Instant APs form a cluster when connected to a provisioning network and a conductor Instant AP is elected. In the cluster mode, new Instant AP onboarded to Aruba Central can join an existing Instant AP cluster.
- Standalone mode—In this mode, individual Instant APs are provisioned in groups and managed from Aruba Central.

Configuration and Management

Network administrators can manage Instant APs through the Aruba Instant UI, Aruba Central, or AirWave management system.

For information on how to configure Instant APs using the Aruba Instant UI, see the *Aruba Instant User Guide*.

For more information on how to deploy, provision, manage, and monitor Instant APs from Aruba Central, see the following topics:

- Supported Instant APs
- Provisioning Instant APs
- Configuring Device Parameters
- Configuring Network Profiles on Instant APs
- Configuring Time-Based Services for Wireless Network Profiles
- Configuring ARM and RF Parameters on Instant APs
- Configuring IDS Parameters on APs
- Configuring Authentication and Security Profiles on Instant APs
- Configuring Instant APs for VPN Services
- Configuring DHCP Pools and Client IP Assignment Modes on Instant APs
- Configuring Services

- Configuring Uplink Interfaces on Instant APs
- Configuring Enterprise Domains
- Configuring Syslog and TFTP Servers for Logging Events
- Opening a Remote Console
- Mapping Instant AP Certificates
- Configuring APs Using Templates
- Managing Variable Files
- Viewing APs Configuration Tabs

Supported Instant APs

The following table lists the Instant AP platforms, the installation mode, the minimum supported Aruba Instant software versions, and the Instant APs supporting power draw:

Table 123: *Supported Instant AP Platforms*

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version	Power Draw Support
AP-567EX	Outdoor	Aruba Instant 8.7.1.0	No
AP-567	Outdoor	Aruba Instant 8.7.1.0	Yes
AP-565EX	Outdoor	Aruba Instant 8.7.1.0	No
AP-565	Outdoor	Aruba Instant 8.7.1.0	Yes
AP-503H	Indoor	Aruba Instant 8.7.1.0	Yes
AP 577EX	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-577	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-575EX	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-575	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-574	Outdoor	Aruba Instant 8.7.0.0	Yes
AP 518	Outdoor	Aruba Instant 8.7.0.0	Yes
AP-505H	Indoor	Aruba Instant 8.7.0.0	Yes
AP-505	Indoor	Aruba Instant 8.6.0.0	Yes
AP-504	Indoor	Aruba Instant 8.6.0.0	Yes
AP-555	Indoor	Aruba Instant 8.5.0.0	No
AP-535	Indoor	Aruba Instant 8.5.0.0	No
AP 534	Indoor	Aruba Instant 8.5.0.0	No

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version	Power Draw Support
AP 515	Indoor	Aruba Instant 8.4.0.0	Yes
AP-514	Indoor	Aruba Instant 8.4.0.0	Yes
AP-387	Outdoor	Aruba Instant 8.4.0.0	Yes
AP-303P	Indoor	Aruba Instant 8.4.0.0	No
AP-377EX	Outdoor	Aruba Instant 8.3.0.0	No
AP-377	Outdoor	Aruba Instant 8.3.0.0	Yes
AP-375EX	Outdoor	Aruba Instant 8.3.0.0	No
AP-375	Outdoor	Aruba Instant 8.3.0.0	Yes
AP-374	Outdoor	Aruba Instant 8.3.0.0	Yes
AP-345	Indoor	Aruba Instant 8.3.0.0	Yes
AP-344	Indoor	Aruba Instant 8.3.0.0	Yes
AP-318	Indoor	Aruba Instant 8.3.0.0	Yes
AP-303	Indoor	Aruba Instant 8.3.0.0	No
AP-203H	Indoor	Aruba Instant 6.5.3.0	No
AP-367	Outdoor	Aruba Instant 6.5.2.0	No
AP-365	Outdoor	Aruba Instant 6.5.2.0	No
AP-303HR	Indoor	Aruba Instant 6.5.2.0	No
AP-303H	Indoor	Aruba Instant 6.5.2.0	Yes
AP-203RP	Indoor	Aruba Instant 6.5.2.0	No
AP-203R	Indoor	Aruba Instant 6.5.2.0	No
IAP-305	Indoor	Aruba Instant 6.5.1.0-4.3.1.0	Yes
IAP-304	Indoor	Aruba Instant 6.5.1.0-4.3.1.0	Yes
IAP-207	Indoor	Aruba Instant 6.5.1.0-4.3.1.0	No
IAP-335	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	Yes
IAP-334	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	Yes
IAP-315	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	No
IAP-314	Indoor	Aruba Instant 6.5.0.0-4.3.0.0	Yes

Instant AP Platform	Installation Mode	Minimum Supported Aruba Instant Software Version	Power Draw Support
IAP-325	Indoor	Aruba Instant 6.4.4.3-4.2.2.0	No
IAP-324	Indoor	Aruba Instant 6.4.4.3-4.2.2.0	No
IAP-277	Outdoor	Aruba Instant 6.4.3.1-4.2.0.0	No
IAP-228	Indoor	Aruba Instant 6.4.3.1-4.2.0.0	No
IAP-205H	Indoor	Aruba Instant 6.4.3.1-4.2.0.0	No
IAP-215	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-214	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-205	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-204	Indoor	Aruba Instant 6.4.2.0-4.1.1.0	No
IAP-275	Outdoor	Aruba Instant 6.4.0.2-4.1.0.0	No
IAP-274	Outdoor	Aruba Instant 6.4.0.2-4.1.0.0	No
IAP-103	Indoor	Aruba Instant 6.4.0.2-4.1.0.0	No
IAP-225	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No
IAP-224	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No
IAP-115	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No
IAP-114	Indoor	Aruba Instant 6.3.1.1-4.0.0.0	No
RAP-155P	Indoor	Aruba Instant 6.2.1.0-3.3.0.0	No
RAP-155	Indoor	Aruba Instant 6.2.1.0-3.3.0.0	No
RAP-109	Indoor	Aruba Instant 6.2.0.0-3.2.0.0	No
RAP-108	Indoor	Aruba Instant 6.2.0.0-3.2.0.0	No
RAP-3WN	Indoor	Aruba Instant 6.1.3.1-3.0.0.0	No
RAP-3WNP	Indoor	Aruba Instant 6.1.3.1-3.0.0.0	No

- RAP-155, RAP-155P, IAP-214, IAP-215, IAP-224, IAP-225, IAP-228, IAP-274, IAP-275, and IAP-277 IAPs are no longer supported from Aruba Instant 8.7.0.0 onwards.
- IAP-103, RAP-108, RAP-109, IAP-114, IAP-115, IAP-204, IAP-205, and IAP-205H IAPs are no longer supported from Aruba Instant 8.3.0.0 onwards.
- By default, AP-318, AP-374, AP-375, and AP-377 IAPs have Eth1 as the uplink port and Eth0 as the downlink port. Aruba does not recommend you to upgrade these IAPs to Aruba Instant 8.5.0.0 or 8.5.0.1 firmware versions, as the upgrade process changes the uplink port from Eth1 to Eth0 port thereby making the devices unreachable.
- For more information about Aruba's End-of-life policy and the timelines for hardware and software products at the end of their lives, see: https://www.arubanetworks.com/support-services/end-of-life/.
- Data sheets and technical specifications for the supported AP platforms are available at: https://www.arubanetworks.com/products/networking/access-points/.

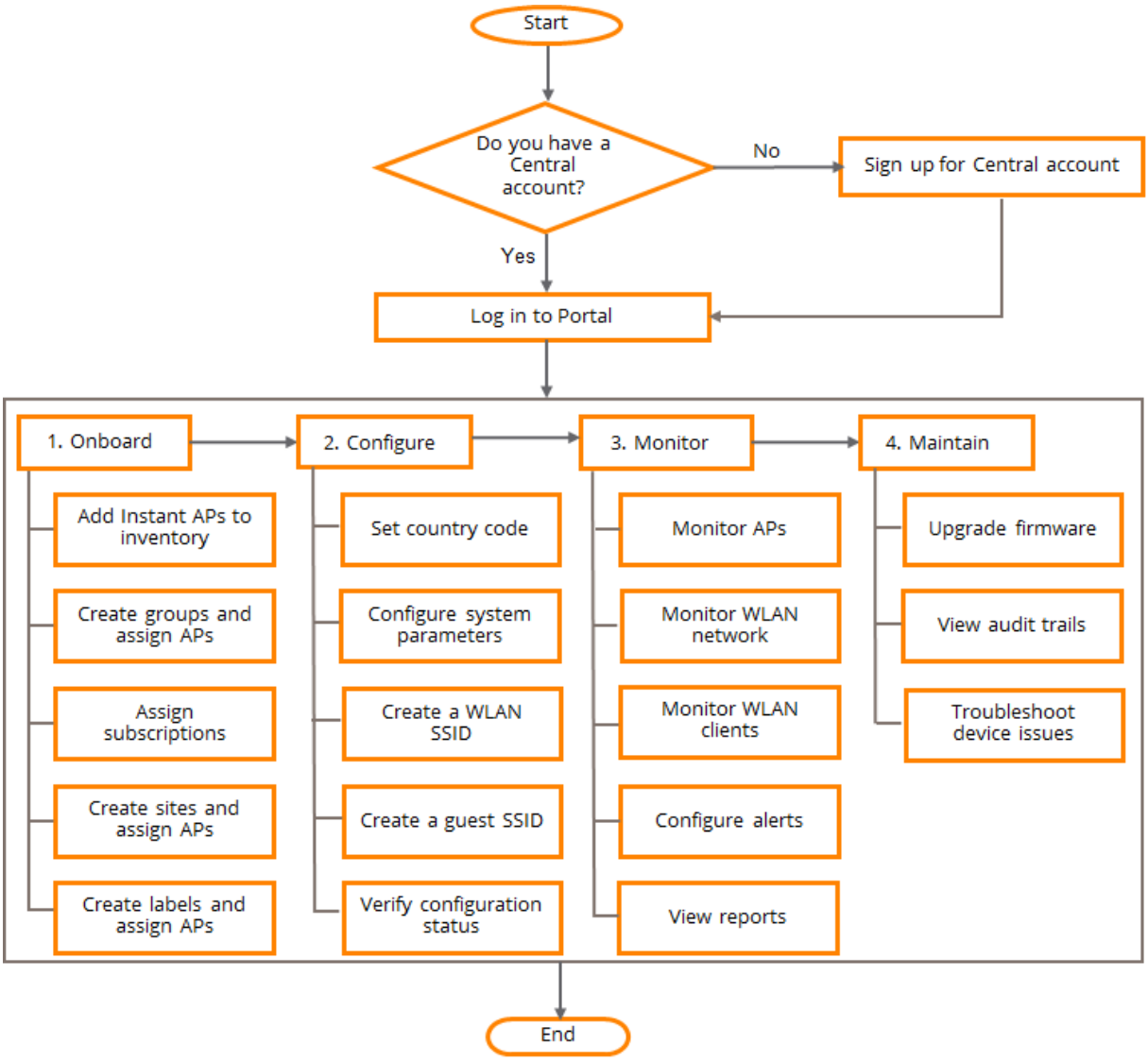
Provisioning Instant APs

The following figure illustrates the procedure for bringing up Instant APs and configuring a basic WLAN setup. To view a detailed description of the tasks, click the task link in the flowchart.

The UI-based provisioning of APs is available for Foundation and Advanced licenses for APs.

When you click a task in the flowchart, the linked topic opens in a pop-up window. After you browse through the topic, click outside the pop-up window to return to this page.

Figure 136 *Getting Started—Instant APs*



Configuring APs Using Templates

Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AP deployments.

The template-provisioning of APs is available for Foundation and Advanced licenses for APs.

To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on Aruba APs.

For template-based provisioning, APs must be assigned to a group with template-based configuration method enabled.

To create a template for the APs in a template group, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the template group under **Groups**.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.

   The tabs to configure APs in a template group are displayed.
4. In the **Templates** table, click **+** to add a new template.

   The Add Template window is displayed.
5. Under **Basic Info**, enter the following information:
   a. **Template Name**—Enter the template name.
   b. **Model**—Set the model parameter to **ALL**.
   c. **Version**—Set the model parameter to **ALL**.
6. Under **Template**, add the CLI script content.
7. Check the following guidelines before adding content to the template:
   - Ensure that the command text indentation matches the indentation in the running configuration.
   - The template allows multiple **per-ap-settings** blocks. The template must include the **per-ap-settings %_sys_lan_mac%** variable. The **per-ap-settings** block uses the variables for each AP. The general VC configuration uses variables for conductor AP to generate the final configuration from the provided template. Hence, Aruba recommends that you upload all variables for all devices in a cluster and change values as required for individual AP variables.
   - You can obtain the list of variables for **per-ap-settings** by using the `show amp-audit` command.

     The following example shows the list of variables for **per-ap-settings**.

     ```
     (Instant AP)# show amp-audit | begin per-ap
     per-ap-settings 70:3a:0e:cc:ee:60
     hostname EE:60-335-24
     rf-zone bj-qa
     ip-address 10.65.127.24 255.255.255.0 10.65.127.1 10.65.6.15 ""
     swarm-mode standalone
     wifi0-mode access
     wifi1-mode access
     g-channel 6+ 21
     a-channel 140 26
     uplink-vlan 0
     g-external-antenna 0
     a-external-antenna 0
     ap1x-peap-user peap22 282eaf1077b8d898b91ec41b5da19895
     ```

     The commands in the template are case-sensitive.

     IF ELSE ENDIF conditions are supported in the template. If the template text includes the if condition, % sign is required at the beginning and the end of the text. For example, %if guest%.

     The following example shows the template text with the IF ELSE ENDIF condition.

     ```
     wlan ssid-profile %ssid_name%
     %if disable_ssid=true%
     disable-ssid
     %endif%
     %if ssid_security=wpa2%
     opmode wpa2-aes
     ```

```
%else%
opmode opensystem
%endif%
```

Templates also support nesting of the IF ELSE END IF condition blocks.

The following example shows how to nest such blocks:

```
%if condition1=true%
routing-profile
  route 10.10.0.0 255.255.255.0 10.10.0.255
%if condition2=true%
routing-profile
  route 10.20.0.0 255.255.255.0 10.20.0.255
%else%
routing-profile
 route 10.30.0.0 255.255.255.0 10.30.0.255
%endif%
%else%
routing-profile
 route 10.40.0.0 255.255.255.0 10.40.0.255
%if condition3=true%
routing-profile
 route 10.50.0.0 255.255.255.0 10.50.0.255
%else%
routing-profile
 route 10.60.0.0 255.255.255.0 10.60.0.255
%endif%
%endif%
```

For profile configuration CLI text, for example, vlan, interface, access-list, ssid and so on, the first command must start with no white space. The subsequent local commands in given profile must start with at least one initial space (' ') or indented as shown in the following examples:

Example 1

```
 vlan 1
  name "vlan1"
  no untagged 1-24
   ip address dhcp-bootp
   exit
```

Example 2

```
%if vlan_id1%
vlan %vlan_id1%
%if vlan_id1=1%
ip address dhcp-bootp
%endif%
no untagged %_sys_vlan_1_untag_command%
exit
%endif%
```

To comment out a line in the template text, use the pound sign (#). Any template text preceded by # is ignored when processing the template.

To allow or restrict APs from joining the Instant AP cluster, Aruba Central uses the **_sys_allowed_ap_** system-defined variable. Use this variable only when allowed APs configuration is enabled. For example, **_sys_allowed_ap: "a_mac, b_mac, c_mac"**. Use this variable only once in the template.

8. Click **OK**.

- The variables configured for the Instant AP devices functioning as the VCs are replaced with the values configured at the template level.
- If any device in the cluster has any missing variables, the configuration push to those AP devices in the cluster fails. The audit trail for such instances shows the missing variables.
- You can configure the RF zone for an AP by adding the **rf-zone %rfzone%** variable in the template. Similarly, you can add the **wifi0-mode %wifi0-mode%** variable to configure a Wi-Fi0 interface of an AP to function in the access, monitor, or spectrum monitor mode.

Sample Template

The following example shows the typical contents allowed in a template file for APs:

```
virtual-controller-country %countrycode%
virtual-controller-key d2d8c79e010af35667dae85f950cf144b476ab4beba9ce5696
organization %org%
name %VCname%
virtual-controller-ip %vcip%
terminal-access
clock time zone none 00 00
rf-band all

allow-new-aps
allowed-ap 38:17:c3:cd:34:ca

hash-mgmt-password
hash-mgmt-user admin password cleartext public

syslog-level debug
syslog-level warn ap-debug

arm
 wide-bands none
 a-channels 44,44+,40,36
 g-channels 13,1+
 min-tx-power 15
 max-tx-power 127
 band-steering-mode prefer-5ghz
 air-time-fairness-mode fair-access
 channel-quality-aware-arm-disable
 client-match
 client-match nb-matching 55
 client-match calc-interval 5
 client-match slb-mode 2

wlan access-rule default_wired_port_profile
 index 0
 rule any any match any any any permit

wlan access-rule wired-SetMeUp
 index 1
 rule masterip 0.0.0.0 match tcp 80 80 permit
```

```
 rule masterip 0.0.0.0 match tcp 4343 4343 permit
 rule any any match udp 67 68 permit
 rule any any match udp 53 53 permit

wlan access-rule %ssid_name%
 index 2
 rule any any match any any any permit

wlan ssid-profile %ssid_name%
 %if disable_ssid=true%
 disable-ssid
 %endif%
 %if ssid_security=wpa2%
 opmode wpa2-aes
 %else%
 opmode opensystem
 %endif%
 type employee
 essid %ssid_name%
 wpa-passphrase %pw%
 max-authentication-failures 0
 auth-server InternalServer
 rf-band all
 captive-portal disable
 dtim-period 1
 broadcast-filter arp
 denylist
 dmo-channel-utilization-threshold 90
 local-probe-req-thresh 0
 max-clients-threshold 64
 okc
%if condition1=true%
routing-profile
  route 10.10.0.0 255.255.255.0 10.10.0.255
%if condition2=true%
routing-profile
  route 10.20.0.0 255.255.255.0 10.20.0.255
%else%
routing-profile
 route 10.30.0.0 255.255.255.0 10.30.0.255
%endif%
%else%
routing-profile
 route 10.40.0.0 255.255.255.0 10.40.0.255
%if condition3=true%
routing-profile
 route 10.50.0.0 255.255.255.0 10.50.0.255
%else%
routing-profile
 route 10.60.0.0 255.255.255.0 10.60.0.255
%endif%
%endif%

wired-port-profile wired-SetMeUp
 switchport-mode access
 allowed-vlan all
 native-vlan guest
 no shutdown
 access-rule-name wired-SetMeUp
 speed auto
 duplex auto
 no poe
```

```
 type guest
 captive-portal disable
 no dot1x

wired-port-profile default_wired_port_profile
 switchport-mode trunk
 allowed-vlan all
 native-vlan 1
 shutdown
 access-rule-name default_wired_port_profile
 speed auto
 duplex full
 no poe
 type employee
 captive-portal disable
 no dot1x


enet0-port-profile default_wired_port_profile
enet1-port-profile wired-SetMeUp

uplink
 preemption
 enforce none
 failover-internet-pkt-lost-cnt 10
 failover-internet-pkt-send-freq 30
 failover-vpn-timeout 180

cluster-security
 allow-low-assurance-devices

per-ap-settings %_sys_lan_mac%
 hostname %hostname%
 rf-zone %rfname%
 swarm-mode %mode%
 wifi0-mode %wifi0mode%
 wifi1-mode %wifi1mode%
 g-channel %gch% %gtx%
 a-channel %ach% %gtx%
```

Password Management in Configuration Templates for AP

In Aruba Central, the AP management user passwords are stored and displayed as hash instead of plain text. Password for an AP can be set using the following commands:

```
mgmt-user <user-name> <password>

mgmt-user <user-name> <password> guest-mgmt

mgmt-user <user-name> <password> read-only
```

The `mgmt-user` commands are used for APs running below Aruba InstantOS 4.3 firmware version.

The `hash-mgmt-user` commands is enabled by default on the APs provisioned in the template and UI groups. If a pre-configured AP joins Aruba Central and is moved to a new group, Aruba Central uses the **hash-mgmt-user** configuration settings and discards **mgmt-user** configuration settings, if any, on the AP. In other words, Aruba Central hashes management user passwords irrespective of the management user configuration settings running on an AP.

NOTE

The `mgmt-user` commands can only be used for APs running firmware versions equal to or above Aruba InstantOS 4.3.

Password for AP can be set using the following `hash-mgmt-user` commands:

```
hash-mgmt-user <user-name> password hash <hash-password>
hash-mgmt-user <user-name> password cleartext <cleartext-password>
hash-mgmt-user <user-name> password hash <hash-password> usertype read-only
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype read-
only
hash-mgmt-user <user-name> password hash <hash-password> usertype guest-mgmt
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype guest-
mgmt
hash-mgmt-user <user-name> password hash <hash-password> usertype local
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype local
```

- Aruba Central supports the use of hash commands with clear text, however, Aruba recommends you to use hash passwords instead of clear text passwords to avoid password disclosures.
- Aruba Central allows you to re-use the hash from one AP on another AP.

NOTE

- All AP templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates.

Viewing APs Configuration Tabs

Aruba Central now constantly displays the default tabs under the **Show Advanced** and **Hide Advanced** options in the **Devices** > **Access Points** page. When you click the **Show Advanced** or **Hide Advanced** option, a set of default configuration tabs are displayed. The respective default tabs under these two options are still displayed when you navigate out of the page, and visit the same page next time.

Following are the default tabs displayed when you navigate to **Devices** > **Access Points** page and click the **Config** icon:

- **WLANs**
- **Access Points**
- **Radios**

When you click the **Show Advanced** option, the following tabs are displayed:

- **WLANs**
- **Access Points**
- **Radios**
- **Interfaces**
- **Security**
- **VPN**

- **Services**
- **System**
- **Configuration Audit**

To view the default tabs, click **Hide Advanced**.

Navigating to Virtual Controller Configuration Dashboard

To navigate to the virtual controller configuration dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. In the **Virtual Controller** column, click on the virtual controller to navigate to the **Access Points** > **List** view of the virtual controller.
4. Click the **Config** icon.

   The default tabs to configure the virtual controller are displayed.
5. Click **Show Advanced** to view advanced configuration options.

   For more information about the various configuration options, see Deploying a Wireless Network Using Instant APs.

Deploying a Wireless Network Using Instant APs

This section describes how to configure WLAN SSIDs, radio profiles, DHCP profiles, VPN routes, security and firewall settings, uplink interfaces, and logging servers on Instant APs.

For more information on Instant AP configuration, see the following topics:

- Configuring Device Parameters
- Configuring Network Profiles on Instant APs
- Configuring Time-Based Services for Wireless Network Profiles
- Configuring ARM and RF Parameters on Instant APs
- Configuring IDS Parameters on APs
- Configuring Authentication and Security Profiles on Instant APs
- Configuring Instant APs for VPN Services
- Configuring DHCP Pools and Client IP Assignment Modes on Instant APs
- Configuring Services
- Configuring Systems
- Configuring Uplink Interfaces on Instant APs
- Configuring Mobility for Clients
- Configuring Enterprise Domains
- Configuring Syslog and TFTP Servers for Logging Events
- Viewing APs Configuration Tabs

- Opening a Remote Console
- Mapping Instant AP Certificates

Setting Country Code

The initial Wi-Fi setup of an Instant AP requires you to specify the country code for the country in which the Instant AP operates. This configuration sets the regulatory domain for the radio frequencies that the Instant AP uses. The available 20 MHz, 40 MHz, or 80 MHz channels are dependent on the specified country code.

Country Code Configuration in Aruba Central from UI

If you provision a new Instant AP without the country code, Aruba Central exhibits the following behavior:

Table 124: *Instant AP Provisioned to Aruba Central*

Country Code Configured at Instant AP	Country Code Configured in Group	Behavior
No	Yes	The country code of the group is pushed to the newly added Instant AP.
No	No	Aruba Central displays the **Country Code not set. Config not updated** message in **Audit Trail**. A notification is also displayed at the bottom of the main window to set the country code of the new Instant AP. To set the country code, perform the following actions: 1. Click **Set Country Code now** link on the notifications pane. The **Set Country Code** pop up is displayed. 2. In the **Device(s) without country code** table, click the edit icon. 3. Specify a country code from the **Country Code** drop-down list. 4. Click **Save**.

If an Instant AP has a country code and joins Aruba Central using ZTP configuration, then the country code of the Instant AP is retained. In this case, Aruba Central will not push the group country code.

Setting Country Code at a Group Level

To set the country code of the Instant AP at the group level, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The default tabs to configure the virtual controller are displayed.
4. Click **Show Advanced** to view advanced configuration options.
5. Click the **System** tab.
   The System details page is displayed.
6. Expand the **General** accordion.

7. In the **Set Country code for group** drop-down list, select the country code for the Instant AP.
8. Click **Save Settings** and then reboot the Instant AP.

- By default, the value corresponding to the **Set Country code for group** field is empty. This indicates that any Instant AP with different country codes can be a part of the group.
- When the **Set Country code for group** field is set, the field cannot revert to the default value. When the country code of the group is changed, the country code of the already connected Instant AP also will be updated.

Setting Country Code at a Device Level

To set the country code of the Instant AP at the device level, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. In the **Virtual Controller** column, click the virtual controller link to navigate to the **Access Points** > **List** view of the virtual controller.

When you click the virtual controller link in the **Virtual Controller** column, the dashboard context for the virtual controller is dispalyed.

4. Click the **Config** icon.
   The default tabs to configure the virtual controller are displayed.
5. Click **Show Advanced** to view advanced configuration options.
6. Click the **System** tab.
   The System details page is displayed.
7. Expand the **General** accordion.
8. In the **Virtual Controller** table, select a virtual controller and then click the edit icon.
9. In the **Edit IP Address** window, select the country code from the **Country Code** drop-down list.
10. Click **Ok**.
11. Click **Save Settings** and then reboot the Instant AP.

- By default, the value corresponding to the **Country code** is the country code set at the group level which can be then modified at the device level from the drop-down list. The country code of the Instant AP will always be the most recently set country code at the group level or device level.
- If there is a discrepancy in the country code configuration, Aruba Central displays it as an override in the **Configuration Audit** page.

Country Code Configuration at Group Level from API

Aruba Central provides an option to set and get the country code at group level through the APIs in **API Gateway**.

To set or get the country code at group level through API, complete the following steps:

1. In the **Account Home** page, click **API Gateway**.
   The API Gateway page is displayed.
2. Click the **Authorized Apps & Tokens** tab and generate a token key.

The token key is valid only for 2 hours from the time it was generated.

3. Download and copy the generated token.
4. In the **All Published APIs** window, click the url link listed under the **Documentation** column.
   The Central Network Management APIs page is displayed.
5. On the left navigation pane, select **Configuration** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. Click **NB UI Group Configuration**.
   The following options are displayed:
   - **Set country code at group level ([PUT]/configuration/v1/country)**—This API allows to set country code for multiple groups at once. Aruba Central currently allows country codes of up to 50 Instant AP device groups to be configured simultaneously. To set the country codes of multiple groups, enter the group names and country code as inputs corresponding to the **groups** and **country** labels respectively in the script { "groups": ["string"], "country": "string" } within the **set_ group_config_ country_ code** text box.
   - **Get country code set for group ([GET]/configuration/v1/{group}/country)**—This API allows to retrieve the country code set for a specific Instant AP group. To get the country code information of the Instant AP group, enter the name of the group for which the country code is being queried corresponding to the **country** label in the script { "country": "string"} within the **group** text box.

The APIs for setting and retrieving country code information are not available for the Instant AP devices deployed in template groups.

The following are the response messages displayed in the **Set country code at group level** and **Get country code set for group** sections:

Table 125: *Response Messages*

Set country code at group level	Get country code set for group
■ 201 - Successful operation ■ 400 - Bad Request ■ 401 - Unauthorized access, authentication required ■ 403 - Forbidden, do not have write access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress	■ 400 - Bad Request ■ 401 - Unauthorized access authentication required ■ 403 - Forbidden, do not have read access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress

For further details on APIs, see https://app1-apigw.central.arubanetworks.com/swagger/central.

Configuring Device Parameters

To configure device parameters on an access point (AP), complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select an AP group in the filter:
     a. Set the filter to a group containing at least one AP.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.
   - To select an AP in the filter:
     a. Set the filter to **Global** or a group containing at least one AP.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.
     c. Click an AP listed under **Device Name**.
        The dashboard context for the AP is displayed.
     d. Under **Manage**, click **Devices** > **Access Point**.
2. Click the **Config** icon.
   The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
   The Access Points page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Configure the parameters described below:

Table 126: *Access Points Configuration Parameters*

UI	Parameters	Description
Basic Info	**Name**	Configure a name for the Instant AP. For Instant APs running Aruba InstantOS 8.7.0.0 or later versions, you can enter up to 128 ASCII or non-ASCII characters. For Instant APs running Aruba InstantOS 8.6.0.0 or earlier versions, you can enter up to 32 ASCII or non-ASCII characters.
	AP Zone	Configure the Instant AP zone. For Instant APs running Aruba InstantOS 6.5.4.7 or later versions, and 8.3.0.0 or later versions, you can configure multiple AP zones by adding zone names as comma separated values. Aruba recommends that you do not configure zones in both SSID and in the Per AP settings of an Instant AP. If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see *Aruba Instant User Guide*.
	RF Zone	Allows you to create an RF zone for the Instant AP.

UI	Parameters	Description
		With RF zone, you can configure different power transmission settings for APs in different zones or sections of a deployment site. For example, you can configure power transmission settings to make Wi-Fi available only for the devices in specific areas of a store. You can also configure separate RF zones for the 2.4 GHz and 5 GHz radio bands for the Instant APs in a cluster. For more information, see Configuring Radio Parameters. Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors.
	Swarm Mode	Allows you to set one of the following operation modes: ■ **Cluster**—Allows an Instant AP to operate in the cluster mode. When an Instant AP operates in the cluster mode, it can form a cluster with other virtual controller Instant APs in the same VLAN. ■ **Standalone**—Allows an Instant AP to operate in the standalone mode. When an Instant AP operates in the standalone mode, it cannot join a cluster of Instant APs even if the Instant AP is in the same VLAN. ■ **Single-AP**—Allows an Instant AP to operate in the single AP mode that is specifically designed for Instant AP deployments with only one AP in the site. This mode is a type of standalone AP deployment with additional security when the AP is directly facing a WAN connection. When configured as a single AP, the AP will not send or receive management frames such as mobility packets, roaming packets, and hierarchy beacons through the uplink port. **NOTE:** After changing the AP operation mode, ensure that you reboot the Instant AP.
	LACP Mode	Allows you to set one of the following LACP modes: ■ **Active**—Allows you to enable the LACP on an Instant AP. In this mode, both the ethernet ports on the Instant AP forms a static LAG. ■ **Passive**—Allows you to set the LACP on an Instant AP in a passive mode. ■ **Disabled**—Allows you to disable the LACP on an Instant AP.
	Preferred Conductor	Select the **Preferred Conductor** check-box to provision the Instant AP as a conductor Instant AP. After provisioning the Instant AP as a conductor Instant AP, ensure that you reboot the AP.
	IP Address For Access Point	Select one of the following options: ■ **Get IP Address from DHCP server**—Allows IP to get

UI	Parameters	Description
		an IP address from the DHCP server. By default, the Instant APs obtain IP address from a DHCP server. ■ **Static**—You can also assign a static IP address to the Instant AP. To specify a static IP address for the Instant AP, complete the following steps: ■ Enter the new IP address for the Instant AP in the **IP Address** text-box. ■ Enter the subnet mask of the network in the **Netmask** text-box. ■ Enter the IP address of the default gateway in the **Default Gateway** text-box. ■ Enter the IP address of the DNS server in the **DNS Server** text-box. ■ Enter the domain name in the **Domain Name** text-box. You can configure up to two DNS servers separated by a comma. If the first DNS server goes down, the second DNS server takes control of resolving the domain name.

UI	Parameters	Description
Radio	**Dual 5G Mode**	Select the **Dual 5G Mode** check-box to enable the dual 5G mode. In the **Dual 5G Mode**, the **Mode** remains as **Access** and is non-editable. The **Dual 5G Mode** is only supported on AP-344 and AP-345 running on Aruba InstantOS 8.3.0.0. For more information, see Configuring Dual 5 GHz Radio Bands on an Instant AP.
	Split Radio	Select the **Split Radio** check-box to allow the radios of the Instant AP to operate in the tri-radio mode. The **Split Radio** is only supported on AP-555 running on Aruba InstantOS 8.5.0.0. For more information, see About Tri-Radio Mode.
	Enable Radio	Select the **Enable Radio** check-box under **2.4GHz Band** and **5 GHz Band** to enable the radio.
	Mode	From the **Mode** drop-down list, select any of the following options: ▪ **Access**—In this mode, the Instant AP serves clients, while also monitoring for rogue Instant APs in the background. ▪ **Monitor**—In this mode, the Instant AP acts as a dedicated monitor, scanning all channels for rogue Instant APs and clients. ▪ **Spectrum**—In this mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring Instant APs or from non-Wi-Fi devices such as microwaves and cordless phones. For more information, see Spectrum Scan Overview. To get accurate monitoring details and statistics, it is highly recommended to reboot the Instant APs once the Instant APs are toggled from the 2.4 or 5 GHz mode to dual 5 GHz radio mode or vice-versa. The access, spectrum, and monitor mode of the radios of an access point is available for Foundation and Advanced licenses for APs.
	Adaptive radio management assigned	You can configure a radio profile on an Instant AP either manually or by configuring the **Adaptive radio management assigned** option. **Adaptive Radio Management (ARM)** feature is enabled on Aruba Central by default. It automatically assigns appropriate channel and power settings for the Instant APs.
	Administrator assigned	You can also assign an administrator by using the **Administrator assigned** option and selecting the number of channels in the **Channel** drop-down list. In the **Transmit Power** field, enter the signal strength measured in dBm.
Installation Type	**Installation Type**	Configure the **Installation Type** of the Instant AP. The **Installation Type** drop-down consists of the following options:

UI	Parameters	Description
		▪ **Default**—Select this option to change the installation type to the default mode. ▪ **Indoor**—Select this option to change the installation type to the indoor mode. ▪ **Outdoor**—Select this option to change the installation type to the outdoor mode. The options in the **Installation Type** drop-down are listed based on the Instant AP model.
Uplink	**Uplink Management VLAN**	The uplink traffic on Instant AP is carried out through a management VLAN. However, you can configure a non-native VLAN as an uplink management VLAN. After an Instant AP is provisioned with the uplink management VLAN, all management traffic sent from the Instant AP is tagged to the management VLAN. To configure a non-native uplink VLAN, click **Uplink** and specify the VLAN in **Uplink Management VLAN**.
	Eth0 Mode	Allows you to change the Eth0 bridging mode in your wired network. The **Eth0 Mode** drop-down consists of the following options: ▪ **Uplink**—Select this option to change the Eth0 bridging mode to the uplink port. ▪ **Downlink**—Select this option to change the Eth0 bridging mode to the downlink port.
	Eth1 Mode	Allows you to change the Eth1 bridging mode in your wired network. The **Eth1 Mode** drop-down consists of the following options: ▪ **Default**—Select this option to change the Eth1 bridging mode to the default port. ▪ **Uplink**—Select this option to change the Eth1 bridging mode to the uplink port. ▪ **Downlink**—Select this option to change the Eth1 bridging mode to the downlink port.
	USB Port	Select the **USB Port** check-box if you do not want to use the cellular uplink or 3G/4G modem in your current network setup.
	PEAP User	Create the PEAP user credentials for certificate based authentication. Enter the username, password, and retype password in the **Username**, **Password**, and **Retype Password** field for creating the PEAP user.

UI	Parameters	Description
Mesh	**Mesh enable**	Select the **Mesh enable** check-box to allow mesh access points to form mesh network. The mesh feature ensures reliability and redundancy by allowing the network to continue operating even when an Instant AP is non-functional or if the device fails to connect to the network. For more information, see Configuring Mesh Instant AP
	Clusterless mesh name	Enter the name of mesh access points that do not belong to any cluster. The **Clusterless mesh name** field is disabled when the **Mesh enable** option is enabled.
	Clusterless mesh key	Enter the key of the mesh access points that do not belong to any cluster. The **Clusterless mesh key** field is disabled when the **Mesh enable** option is enabled.
	Retype	Re-enter the clusterless mesh key. The **Retype** is disabled when the **Mesh enable** option is enabled.
External Antenna	**Antenna Gain**	Enter the **Antenna Gain** values in dBi for the **2.4 GHz Antenna Gain** and the **5 GHz Antenna Gain**. For more information, see Configuring External Antenna
	Antenna Polarization Type	From the **Antenna Polarization Type** drop-down list, select any of the following: ■ **co-polarization**—Select this option for the polarization of both the transmitting and receiving antenna to be same. ■ **cross-polarization**—Select this option for the polarization of both the transmitting and receiving antenna to be different. The integrated antenna of the wireless bridge sends a radio signal that is polarized in a particular direction. The receive sensitivity of the antenna is also higher for radio signals that have the same polarization. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction.

6. Click **Save Settings** and then reboot the Instant AP.

Configuring Systems

This section describes how to configure the General, Administrator, Time-Based Services, DHCP, Layer-3 Mobility, Enterprise Domains, Logging, SNMP, WISPr, Proxy, Named VLAN Mapping, and IPM parameters on an Instant AP.

- Configuring System Parameters for an AP
- Configuring Users Accounts for the Instant AP Management Interface
- Configuring Time-Based Services for Wireless Network Profiles
- Configuring DHCP Pools and Client IP Assignment Modes on Instant APs
- Configuring Mobility for Clients
- Configuring Enterprise Domains
- Configuring Syslog and TFTP Servers for Logging Events

- Configuring SNMP Parameters
- Supported Authentication Methods
- Configuring HTTP Proxy on an Instant AP
- Configuring VLAN Name and VLAN ID
- Configuring Intelligent Power Monitoring

Configuring VLAN Name and VLAN ID

Aruba Central allows you to map VLAN name to a VLAN ID for the ease of identifying the existing VLANs.

To map a VLAN name to a VLAN ID, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **Named VLAN Mapping** accordion.
7. Click the **+** icon in the **VLAN Name to VLAN ID Mapping** pane.
   The **VLAN Name to VLAN ID Mapping** window is displayed.
8. In the **VLAN Name to VLAN ID Mapping** window, enter the **VLAN Name** and **VLAN ID**.
9. Click **OK**.
   The **VLAN Name to VLAN ID Mapping** table in the **Named VLAN Mapping** section lists all the mapped VLAN.

You can find the **Named VLAN Mapping** feature applied in the following fields of corresponding UI pages of Aruba Central:

- The **VLAN ID** field in the **VLANs** tab, when for when **Custom** for **Instant AP Assigned** and **Static** for **External DHCP server assigned** is selected during WLAN SSID creation. For more information, see Creating a Wireless Network Profile.
- The **VLAN ID** field in the **VLANs** tab, when **Custom** for **Instant AP Assigned** and **Static** for **External DHCP server assigned** is selected during wired port profile creation. For more information, see Configuring Wired Port Profiles on Instant APs.
- The **Access rules** page in the **Interfaces** > **Access** tab and the **WLANs** > **Access** tab, when you add rules for selected roles. Select **VLAN Assignment** as the rule type in the **Access rules** page to find the mapped VLAN name in the **VLAN ID** field.

You can also map VLAN ID to a VLAN name when you customize the **Client VLAN Assignment** configuration in VLANs tab during network profile creation. For more information, see VLANs Parameters.

Points to Remember

- The maximum number of **Named VLAN ID Mapping** allowed in Aruba Central is 32.
- VLAN mapping cannot be performed if the VLAN name does not exist.
- The VLAN mapping record is deleted from the **VLAN Name to VLAN ID Mapping** table when the VLAN name is deleted.
- You can only map a single VLAN id to a VLAN name.
- The VLAN name field is not case-sensitive.

Configuring External Antenna

If the Instant AP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the Instant AP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know, if the Instant AP device supports external antenna connectors, see the *Installation Guide* that is shipped along with the Instant AP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (Antenna Gain) and feeder (Coaxial Cable Loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 127: *Formula Variable Definitions*

Formula Element	Description
EIRP	Limit specific for each country of deployment.
Tx RF Power	RF power measured at RF connector of the unit.
GA	Antenna gain
FL	Feeder loss

Configuring Antenna Gain

To configure antenna gain for Instant APs with external connectors, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select an AP group in the filter:
     a. Set the filter to a group containing at least one AP.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.

- To select an AP in the filter:
  a. Set the filter to **Global** or a group containing at least one AP.
  b. Under **Manage**, click **Devices** > **Access Points**.
     A list of APs is displayed in the **List** view.
  c. Click an AP listed under **Device Name**.
     The dashboard context for the AP is displayed.
  d. Under **Manage**, click **Devices** > **Access Point**.

2. Click the **Config** icon.
   The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
   The Access Points page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click the **External Antenna** tab.
6. Enter the **Antenna Gain** values in dBi for the **2.4 GHz Antenna Gain** and the **5 GHz Antenna Gain**.
7. From the **Antenna Polarization Type** drop-down list, select any of the following:
   - **co-polarization**—Select this option for the polarization of both the transmitting and receiving antenna to be same.
   - **cross-polarization**—Select this option for the polarization of both the transmitting and receiving antenna to be different.
8. Click **Save Settings**.

After configuring the external antenna parameters, ensure that you reboot the Instant AP.

Adding an Instant AP

To add an Instant AP to Aruba Central, assign an IP address and a subscription.

After an Instant AP is connected to the network and if the **Auto Join Mode** feature is enabled, the Instant AP inherits the configuration from the virtual controller and is listed in the **Access Points** tab.

Deleting an Instant AP from the Network

To delete an Instant AP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of access points is displayed in the **List** view.
3. In the **Access Points** table, hover over the offline AP that you want to delete.
4. Click the  delete icon.

Configuring Intelligent Power Monitoring

The Intelligent Power Monitoring (IPM) feature actively measures the power utilization of an AP and dynamically adapts to the power resources. IPM allows you to define the features that must be disabled to

save power, allowing the APs to operate at a lower power consumption without hampering the performance of the related features. This feature constantly monitors the AP power consumption and adjusts the power saving IPM features within the power budget.

IPM dynamically limits the power requirement of an AP as per the available power resources. IPM applies a sequence of power reduction steps as defined by the priority definition until the AP functions within the power budget. This happens dynamically as IPM constantly monitors the AP power consumption and applies the next power reduction step in the priority list if the AP exceeds the power threshold. To manage this prioritization, you can create IPM policies to define a set of power reduction steps and associate them with a priority. The IPM policies, when applied to the AP, are based on IPM priorities, where the IPM policy can be configured to disable or reduce certain features in a specific sequence to reduce the AP power consumption below the power budget. IPM priority settings are defined by integer values, where the lower values have the highest priority and are implemented first.

The Intelligent Power Monitoring feature is available only on AP devices running Aruba InstantOS 8.6.0.3.

To configure Intelligent Power Monitoring, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **IPM** accordion.
7. Select the **IPM Activation** check box to enable IPM.
8. Click the **+** icon in the **IPM Power Reduction Steps With Priorities** pane.
   The **IPM Power Reduction Steps With Priorities** window is displayed.
9. In the **IPM Step Priority** field, enter a value from 1 to 16 to define IPM priority.
10. From the **IPM Step** drop-down list, select a setting as described in the following table:

Table 128: *Intelligent Power Monitoring Step Parameters*

Parameters	Description
cpu_throttle_25	Reduces CPU frequency to 25% of normal.
cpu_throttle_50	Reduces CPU frequency to 50% of normal.
cpu_throttle_75	Reduces CPU frequency to 75% of normal.
disable_alt_eth	Disables the second Ethernet port.

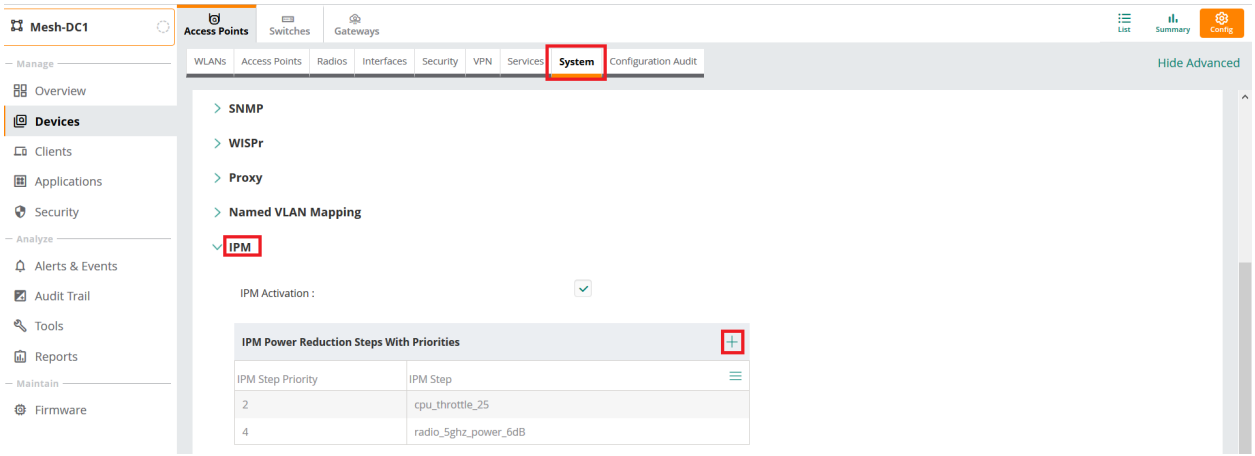
Parameters	Description
disable_pse	Disables Power Sourcing Equipment (PSE).
disable_usb	Disables USB.
radio_2ghz_chain_1	Reduces 2 GHz chains to 1x1.
radio_2ghz_chain_2	Reduces 2 GHz chains to 2x2.
radio_2ghz_chain_3	Reduces 2 GHz chains to 3x3.
radio_2ghz_power_3dB	Reduces 2 GHz radio power by 3 dB from the maximum value.
radio_2ghz_power_6dB	Reduces 2 GHz radio power by 6 dB from the maximum value.
radio_5ghz_chain_1	Reduces 5 GHz chains to 1x1.
radio_5ghz_chain_2	Reduces 5 GHz chains to 2x2.
radio_5ghz_chain_3	Reduces 5 GHz chains to 3x3.
radio_5ghz_power_3dB	Reduces 5 GHz radio power by 3 dB from the maximum value.
radio_5ghz_power_6dB	Reduces 5 GHz radio power by 6 dB from the maximum value.

11. Click **OK**.

    The **IPM Power Reduction Steps With Priorities** table in the **IPM** section lists all the IPM settings.
12. Click **Save Settings** and reboot the Instant AP for changes to take effect.

The following figure shows the IPM steps and priorities listed in the **IPM Power Reduction Steps With Priorities** table:

Figure 137 *IPM Steps and Priorities*



Setting a low-priority value for a power reduction step reduces the power level sooner than setting a high-priority value for a power reduction step. However, if the power reduction step is of the same type but different level, the smallest reduction should be allocated the lowest priority value so that the power reduction step takes place earlier. For example, the **cpu_throttle_25** or **radio_2ghz_power_3dB** parameter should have a lower priority level than the **cpu_throttle_50** or **radio_2ghz_power_6dB**, respectively, so that Intelligent Power Monitoring reduces the CPU throttle or power usage based on the priority list.

Points to Remember

- By default, Intelligent Power Monitoring is disabled.
- When enabled, IPM enables all Instant AP functionality initially. IPM then proceeds to shut down or restrict functionality if the power usage of the AP goes beyond the power budget of the Instant AP.

Configuring Dual 5 GHz Radio Bands on an Instant AP

Aruba Central provides an option to retrieve the radio numbers of Instant AP through the APIs. It also provides an option to filter AP details using radio numbers in the AP monitoring dashboard.

For regular Instant APs with non-dual band, Central automatically assigns **Radio 1** to 2.4 GHz band and **Radio 0** to 5 GHz band respectively.

To retrieve the radio numbers through API, complete the following steps:

1. In the **Account Home** page, click **API Gateway**.
   The API Gateway page is displayed.
2. Click the **APIs** tab.

   The token key is valid only for 2 hours from the time it was generated.
3. In the **All Published APIs** window, click the url link listed under the **Documentation** column.
   The Central Network Management APIs page is displayed.
4. On the left navigation pane, select **Monitoring** from the **URL** drop-down list.
5. Click **API Reference** > **AP**.
   The following APIs allow you to retrieve the radio number for the APs:

Table 129: *APIs to Get Radio Number in APs*

API	Description
[GET]/monitoring/v1/aps/{serial}/neighbouring_clients	Allows you to filter data of neighbouring clients for a specific radio number in a given time period. When there is no radio number entered in the **radio_number** field, the API filters the data of neighbouring clients for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the data of neighboring clients for a specific radio number.
[GET]/monitoring/v1/aps/rf_summary	Retrieves information on RF summary such as channel utilization and noise floor in positive, errors, drops for a given time period.

API	Description
	This API can also be used to filter RF health statistics for a specific radio number in a given time period. When there is no radio number entered in the **radio_number** field, the API filters the RF health statistics for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the RF health statistics for a specific radio number.
[GET]/monitoring/v1/aps/bandwith_usage	This API can also be used to filter out bandwidth usage data for a specific radio number in a given time period. When there is no radio number entered in the **radio_number** field, the API filters the bandwidth usage for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the bandwidth usage for a specific radio number.

6. On the left navigation pane, click **API Reference** > **Client**.

   The following APIs allow you to retrieve the radio number for the total number of clients connected:

Table 130: *APIs to Get Radio Number in Connected Clients*

API	Description
[GET]/monitoring/v1/clients/count	This API is used to filter out the data for connected clients for a specific radio number of AP in a given time period. When there is no radio number entered in the **radio_number** field, the API filters the clients count for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the total count of clients for a specific radio number.

For further details on APIs, see https://app1-apigw.central.arubanetworks.com/swagger/central.

Support for Dual 5 GHz AP

Aruba Central supports automatic opmode selection for dual 5 GHz AP. When the opmode is set to automatic, AirMatch determines whether to convert a radio in an AP to 5 GHz operation instead of the 2.4 GHz and 5 GHz dual band operation. Automatic is the default dual 5G mode where Airmatch detects what is an optimal mode for the radios – dual band or dual 5G and updates the running opmode without requiring an AP reboot between the mode changes.

Manual setting of dual band and dual 5G is possible and the manual setting overrides the automatic mode and explicitly enables or disables the dual 5G mode. In this scenario, the AP immediately switches to the specified mode without a reboot and AirMatch maintains the specified channel and power assignments in the specified mode.

Automatic mode is not supported on AP-344. By default, AP-344 assumes the automatic mode to be the same as dual 5G disabled and operates in the dual band mode. To switch AP-344 to dual 5G mode, select the **Dual 5G Mode** check-box.

To configure automatic opmode selection for dual 5 GHz AP, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select an AP group in the filter:
     a. Set the filter to a group containing at least one AP.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.
   - To select an AP in the filter:
     a. Set the filter to **Global** or a group containing at least one AP.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.
     c. Click an AP listed under **Device Name**.
        The dashboard context for the AP is displayed.
     d. Under **Manage**, click **Devices** > **Access Point**.
2. Click the **Config** icon.
   The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
   The Access Points page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click the **Radio** tab.
6. Set **Dual 5G Mode** to **Automatic**.
7. Optionally, specify the manual channel by setting **Channel Assignment** to **Manual**.
8. Optionally, specify the transmit power by setting **Transmit Power Assignment** to **Manual**.
9. Click **Save Settings**.

Configuring System Parameters for an AP

To configure system parameters for an AP, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.

6. Click the **General** accordion and configure the following parameters:

Table 131: *System Parameters*

Data Pane Item	Description
Virtual Controller	This parameter configuration is only applicable for APs that operate in a cluster deployment environment. To configure the virtual controller name and IP address, click edit icon and update the name and IP address. The IP address serves as a static IP address for the multi-AP network. When configured, this IP address is automatically provisioned on a shadow interface on the AP that takes the role of a virtual controller. The AP sends three ARP messages with the static IP address and its MAC address to update the network ARP cache. ■ **Name**—Name of the virtual controller. ■ **IP address**—IPv4 address configured for the virtual controller. The IPv4 address uses the 0.0.0.0 notation. ■ **IPv6 address**—IPv6 address configured for the virtual controller. You can configure IPv6 address for the virtual controller only if the Allow IPv6 Management feature is enabled. IPv6 is the latest version of IP that is suitable for large-scale IP networks. IPv6 supports a 128-bit address to allow 2128, or approximately 3.4×1038 addresses while IPv4 supports only 232 addresses. The IP address of the IPv6 host is always represented as eight groups of four hexadecimal digits separated by colons. For example *2001:0db8:0a0b:12f0:0000:0000:0000:0001*. However, the IPv6 notation can be abbreviated to compress one or more groups of zeroes or to compress leading or trailing zeroes; for example *2001:db8:a0b:12f0::0:0:1*.
Set Country code for group	To configure a country code for the AP at the group level, select the country code from the **Set Country code for group** drop-down list. By default, no country code is configured for the AP device groups. When a country code is configured for the group, it takes precedence over the country code setting configured t the device level.
Timezone	To configure a time zone, select a time zone from the **Timezone** drop-down list. If the selected time zone supports DST, the UI displays the "**The selected country observes Daylight Savings Time**" message.
Preferred Band	Assign a preferred band by selecting an appropriate option from the **Preferred Band** drop-down list. Reboot the AP after modifying the radio profile for changes to take effect.
NTP Server	This parameter allows you to configure NTP servers for the Instant AP. Up to four NTP servers can be configured for the AP, each one separated by a comma. To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to: ■ Trace and track security gaps, network usage, and troubleshoot network issues. ■ Validate certificates. ■ Map an event on one network element to a corresponding event on another. ■ Maintain accurate time for billing services and similar. ■ NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the AP clock to set the correct time. If NTP server is not configured in the AP network, an AP reboot may lead to variation in time data.

Table 131: *System Parameters*

Data Pane Item	Description
	By default, the AP tries to connect to **pool.ntp.org** to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server **pool.ntp.org** is used if no NTP server is configured or provisioned through DHCP option 42. To configure an NTP server, enter the IP address or the URL of the NTP server and reboot the AP to apply the configuration changes.
Virtual Controller Netmask **Virtual Controller Gateway** **Virtual Controller DNS** **Virtual Controller VLAN**	This parameter configuration is only applicable for APs that operate in a cluster deployment environment. The IP configured for the virtual controller can be in the same subnet as AP or can be in a different subnet. Ensure that you configure the virtual controller VLAN, gateway, and subnet mask details only if the virtual controller IP is in a different subnet. Ensure that virtual controller VLAN is not the same as native VLAN of the AP.
DHCP Option 82 XML	The **DHCP Option 82 XML** is not applicable for cloud APs. **DHCP Option 82 XML** can be customized to cater to the requirements of any ISP using the conductor AP. To facilitate customization using a XML definition, multiple parameters for Circuit ID and Remote ID options of DHCP Option 82 XML are introduced. The XML file is used as the input and is validated against an XSD file in the conductor AP. The format in the XML file is parsed and stored in the DHCP relay which is used to insert Option 82 related values in the DHCP request packets sent from the client to the server. From the drop-down list, select one of the following XML files: ▪ **default_dhcpopt82_1.xml** ▪ **default_dhcpopt82_2.xml** For more information, see Configuring DHCP Scopes on Instant APs.
Dynamic CPU Utilization	APs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If an AP is overloaded, prioritize the platform resources across different functions. Typically, the APs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified. To configure dynamic CPU management, select any of the following options from **Dynamic CPU Utilization**. ▪ **Automatic**—When selected, the CPU management is enabled or disabled automatically during run-time. This decision is based on real time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option. ▪ **Always Disabled in all APs**—When selected, this setting disables CPU management on all APs, typically for small networks. This setting protects user experience. ▪ **Always Enabled in all APs**—When selected, the client and network management functions are protected. This setting helps in large networks with high client density.

Table 131: *System Parameters*

Data Pane Item	Description
Auto-Join Mode	When enabled, APs can automatically discover the virtual controller and join the network. The **Auto-Join Mode** feature is enabled by default.
APs allowed for Auto-Join Mode	Displays the number of APs allowed for **Auto-Join Mode**. ■ Click **View Allowed APs** to view the details of AP allowed for Auto-Join mode. ■ Click **Hide Allowed APs** to hide the details of AP allowed for Auto-Join mode. When **Auto-Join Mode** is enabled, the APs are automatically discovered and are allowed to join the cluster. When the **Auto-Join Mode** is disabled on the AP, the list of allowed APs on Aruba Central may not be synchronized or up-to-date. In such cases, you can manually add a list of APs that can join the AP cluster in the Aruba Central UI. To manually add the list of allowed AP devices, complete the following steps: 1. Under **View Allowed APs**, click **+** in the **Allowed APs** pane. 2. In the **Add Allowed AP** window, enter the MAC address of the AP in the **MAC Address field**. 3. Click **Save**.
Allow IPv6 Management	Enables IPv6 address configuration for the virtual controller. You can configure an IPv6 address for a virtual controller IP only when **Allow IPv6 Management** feature is enabled.
Uplink switch native VLAN	Allows you to specify a VLAN ID, to prevent the AP from sending tagged frames for clients connected on the SSID that uses the same VLAN as the native VLAN of the switch. By default, the AP considers the native VLAN of the upstream switch, to which it is connected, as the VLAN ID 1.
Terminal Access	When enabled, the users can access the AP CLI through SSH.
Login Session Timeout	Allows you to set a timeout for login session.
Console Access	When enabled, the users can access AP through the console port.
WebUI Access	If an AP is connected to Aruba Central, you can use this option to disable AP Web UI access and any communication via HTTPS or SSH. If you enable this feature, you can manage the AP only from Aruba Central.
Telnet Server	When enabled, the users can start a Telnet session with the AP CLI.
LED Display	Enables or disables the LED display for all APs in a cluster. The LED display is always enabled during the AP reboot.
Extended SSID	**Extended SSID** is enabled by default in the factory default settings of APs. This disables mesh in the factory default settings. For AP devices that support Aruba Instant 8.4.0.0 firmware versions and above, you can configure up to 14 SSIDs. By enabling **Extended SSID**, you can create up to 16 networks.
Advanced Zone	Turn on the **Advanced Zone** toggle switch to broadcast the same ESSIDs on APs that are part of the same AP zone in a cluster. **NOTE:** When the advanced-zone feature is enabled and a zone is already

Table 131: *System Parameters*

Data Pane Item	Description
	configured with 16 SSIDs, ensure to remove the zone from two WLAN SSID profiles if you want to disable extended SSID.
Deny Inter User Bridging	If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter-user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. To disable inter-user bridging, turn off the **Deny Inter User Bridging** toggle switch.
Deny Local Routing	If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same AP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision. To disable local routing, move the slider to the right.
Dynamic RADIUS Proxy	If your network has separate RADIUS authentication servers (local and centralized servers) for user authentication, you may want to enable **Dynamic RADIUS proxy** to route traffic to a specific RADIUS server. When **Dynamic RADIUS proxy** is enabled, the IP address of the virtual controller is used for communication with external RADIUS servers. To enable **Dynamic RADIUS Proxy**, you must configure an IP address for the Virtual Controller and set it as a NAS client in the RADIUS server profile.
Dynamic TACACS Proxy	If you want to route traffic to different TACACS servers, enable **Dynamic TACACS Proxy**. When enabled, the AP cluster uses the IP address of the Virtual Controller for communication with external TACACS servers. If an IP address is not configured for the Virtual Controller, the IP address of the bridge interface is used for communication between the AP and TACACS servers. However, if a VPN tunnel exists between the Instant AP and TACACS server, the IP address of the tunnel interface is used.
Cluster Security	This parameter is required to be set only for APs that operate in a cluster deployment environment. Enables or disables the cluster security feature. When enabled, the control plane communication between the AP cluster nodes is secured. The **Disallow Non-DTLS Members** toggle switch appears. Turn on the toggle switch to allow member APs to join a DTLS enabled cluster. For secure communication between the cluster nodes, the Internet connection must be available, or at least a local NTP server must be configured. After enabling or disabling cluster security, ensure that the configuration is synchronized across all devices in the cluster, and then reboot the cluster. The **Disallow Non-DTLS Members** feature is only supported in AP devices supporting Aruba Instant 8.4.0.0 firmware versions and above.
Low Assurance PKI	Turn on the toggle switch to allow low assurance devices that use non-TPM chip, in the network. To enable the cluster security feature, turn on the **Low Assurance PKI** toggle switch. For more information on *Low Assurance PKI*, refer to *Cluster Security* section in *Aruba Instant User Guide*. The **Low Assurance PKI** toggle switch is supported in AP devices running Aruba Instant 6.5.3.0 firmware versions and later.

Table 131: *System Parameters*

Data Pane Item	Description
Mobility Access Switch Integration	Turn on the toggle switch to enable LLDP protocol for **Mobility Access Switch integration**. With this protocol, APs can instruct the switch to turn off ports where rogue access points are connected, as well as take actions such as increasing PoE priority and automatically configuring VLANs on ports where APs are connected.
URL Visibility	Turn on the toggle switch to enable URL data logging for client HTTP and HTTPS sessions and allows APs to extract URL information and periodically log them on ALE for DPI and application analytics.
Restrict uplink port to specified VLANs	Turn on the toggle switch to restrict the uplink port to the specified VLANs.
VOIP QOS Trust	Turn on the toggle switch to enable the RTP traffic based on the DSCP value set by the end user device.

7. Click **Save Settings**.

Enabling 802.1X Authentication on Uplink Ports of an AP

If your network requires all wired devices to authenticate using **PEAP** or **TLS** protocol, you must enable 802.1X authentication type on uplink ports of an AP, so that the APs are granted access only after completing the authentication as a valid client.

To enable 802.1X authentication on uplink ports using **PEAP** or **TLS** protocol, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Expand the **AP1X** section.
   - To set **PEAP** based authentication, select **PEAP** in the **AP1X Type** drop-down list.

If you select **PEAP** protocol, ensure that the **PEAP User** is configured on the uplink port by selecting an AP group and navigating to **Uplink** section in the **Access Points** tab.

   - To set **TLS** based authentication:
     a. Select **TLS** in the **AP1X Type** drop-down list.
     b. Select **User** in the **Certificate Type** drop-down list.

8. Select the **Validate Server** check-box to validate the server credentials using server certificate. Ensure that the server certificates for validating server credentials are available in the Instant AP database.
9. Click **Save Settings**.

Configuring HTTP Proxy on an Instant AP

If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the Instant AP to download the image from the cloud server. After setting up the HTTP proxy settings, the Instant AP connects to the Activate server, Aruba Central, or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an Instant AP) by providing their host name or IP address under **Exception**. Aruba Central allows the user to configure HTTP proxy on an Instant AP.

To configure HTTP proxy on Instant AP through Aruba Central, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **Proxy** accordion and specify the following:
   a. Enter the HTTP proxy server IP address in the **Server** text-box.
   b. Enter the port number in the **Port** text-box.
7. Click **Save Settings**.

Aruba Central displays the **Username**, **Password**, and **Retype Password** fields under **System** > **Proxy** for Instant AP running Aruba Instant 8.3.0.0. The Instant APs with the Aruba InstantOS 8.3.0.0 firmware require user credentials for proxy server authentication.

Configuring Network Profiles on Instant APs

This section describes the following procedures:

- Configuring Wireless Network Profiles on Instant APs
- Configuring Wireless Networks for Guest Users on Instant APs
- Configuring Wired Port Profiles on Instant APs
- Configuring Wired Networks for Guest Users on Instant APs
- Editing a Wireless Network Profile
- Deleting a Network Profile

Configuring Wireless Network Profiles on Instant APs

You can configure up to 14 SSIDs. By enabling **Extended SSID** in the **System** > **General** accordion, you can create up to 16 networks.

NOTE

If more than 16 SSIDs are assigned to a zone and the extended zone option is disabled, an error message is displayed.

This section describes the following topics:

- Creating a Wireless Network Profile
- Configuring VLAN Settings for Wireless Network
- Configuring Security Settings for Wireless Network
- Configuring ACLs for User Access to a Wireless Network
- Viewing Wireless SSID Summary

Creating a Wireless Network Profile

To configure WLAN settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **WLANs** tab, click **+ Add SSID**.
   The Create a New Network pane is displayed.
6. In **General** tab, enter a name that is used to identify the network in the **Name (SSID)** text-box.
7. Under **Advanced Settings**, configure the following parameters:

Table 132: *Advanced Settings Parameters*

Parameter	Description
Broadcast/Multicast	
Broadcast filtering	Select any of the following values: ■ **All**—The Instant AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ■ **ARP**—The Instant AP drops broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. Additionally, it converts ARP requests to unicast and sends frames directly to the associated clients. By default, the Instant AP is configured to ARP mode. ■ **Unicast ARP Only**—This option enables Instant AP to convert ARP requests to unicast frames thereby sending them to the associated clients. ■ **Disabled**—The Instant AP forwards all the broadcast and multicast traffic is forwarded to the wireless interfaces.

Parameter	Description
DTIM Interval	The **DTIM Interval** indicates the DTIM period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the Instant AP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode. Range is 1 to 10 beacons. The default value is 1, which means the client checks for buffered data on the Instant AP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast Transmission Optimization	Select the check-box if you want the Instant AP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent up to a rate of 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This option is disabled by default.
Dynamic Multicast Optimization (DMO)	Select the check-box to allow Instant AP to convert multicast streams into unicast streams over the wireless link. Enabling DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the Instant AP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the Instant AP sends multicast traffic over the wireless link. **NOTE:** This option will be enabled only when **Dynamic Multicast Optimization** is enabled.
Transmit Rates (Legacy Only)	
2.4 GHz	If the 2.4 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps.
5 GHz	If the 5 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Zone	
Zone	Specify the zone for the SSID. If a zone is configured in the SSID, only the Instant AP in that zone broadcasts this SSID. If there are no Instant APs in the zone, SSID is broadcast. If the Instant AP cluster has devices running Aruba Instant firmware versions 6.5.4.7 or later, and 8.3.0.0 or later, you can configure multiple AP zones by adding zone names as comma separated values. **NOTE:** Aruba recommends that you do not configure zones in both SSID and in the device specific settings of an Instant AP. If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see *Aruba Instant User Guide*.
Bandwidth Control	

Parameter	Description
Airtime	Select this to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage.
Downstream	Enter the downstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the **Per User** check-box. **NOTE:** The bandwidth limit set in this method is implemented at the device level and not cluster level.
Upstream	Enter the upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the Per user check-box. **NOTE:** The bandwidth limit set in this method is implemented at the device level and not cluster level.
Each Radio	Select this to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. The value ranges from 1 through 65535.
Enable 11n	When this option is selected, there is no disabling of High-Throughput (HT) on 802.11n devices for the 5 GHz radio band. If HT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, HT is enabled on all SSIDs. **NOTE:** If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear this check-box to disable VHT on these devices.
Enable 11ac	When this option is selected, VHT is enabled on the 802.11ac devices for the 5 GHz radio band. If VHT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs. **NOTE:** If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear this check-box to disable VHT on these devices.
Enable 11ax	When this option is selected, VHT is enabled on the 802.11ax devices. If VHT is enabled for a radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs.
WiFi Multimedia	
Background Wifi Multimedia Share	Allocates bandwidth for background traffic such as file downloads or print jobs. Specify the appropriate DSCP mapping values within a range of 0–63 for the background traffic in the corresponding DSCP mapping text-box. Enter up to 8 values with no white space and no duplicate single DHCP mapping value.
Best Effort Wifi Multimedia Share	Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. Specify the appropriate DSCP mapping values within a range of 0–63 for the best effort traffic in the corresponding DSCP mapping text-box.
Video Wifi Multimedia Share	Allocates bandwidth for video traffic generated from video streaming. Specify the appropriate DSCP mapping values within a range of 0–63 for the video traffic in the corresponding DSCP mapping text-box.

Parameter	Description
Voice Wifi Multimedia Share	Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication. Specify the appropriate DSCP mapping values within a range of 0–63 for the voice traffic in the corresponding DSCP mapping text-box. **NOTE:** In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for **Best Effort Wifi Multimedia** share and **Voice Wifi Multimedia Share** to allocate a higher bandwidth to clients transmitting best effort and voice traffic.
Traffic Specification (TSPEC)	Select this check-box to set if you want the TSPEC for the wireless network. The term TSPEC is used in wireless networks supporting the IEEE 802.11e Quality of Service standard. It defines a series of parameters, characteristics and Quality of Service expectations of a traffic flow.
TSPEC Bandwidth	Enter the bandwidth for the TSPEC.
Spectralink Voice Protocol (SVP)	Select this check-box to opt for SVP protocol.
WiFi Multimedia Power Save (U-APSD)	Select this check-box to enable WiFi Multimedia Power Save (U-APSD). The U-APSD is a power saving mechanism that is an optional part of the IEEE amendment 802.11e, QoS.
Miscellaneous	
Band	Select a value to specify the band at which the network transmits radio signals in the **Band** drop-down list. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
Content Filtering	Select this check-box to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Primary Usage	Based on the type of network profile, select one of the following options: ▪ **Mixed Traffic**—Select this option to create an employee or guest network profile. The employee network is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods. Employees can access the protected data of an enterprise through the employee network after successful authentication. The guest network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The VC assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify the encryption settings when configuring a guest network. ▪ **Voice Only**—Select this option to configure a network profile for devices that provide only voice services such as handsets or applications that require voice traffic prioritization. **NOTE:** When a client is associated with the voice network, all data traffic is marked and placed into the high priority queue in QoS.

Parameter	Description
Inactivity timeout	Specify an interval for session timeout in seconds, minutes, or hours. If a client session is inactive for the specified duration, the session expires and the user is required to log in again. You can specify a value within the range of 60–86,400 seconds (24 hours) for a client session. The default value is 1000 seconds.
Hide SSID	Select this check-box if you do not want the SSID to be visible to users.
Disable Network	Select this check-box if you want to disable the SSID. When selected, the SSID is disabled, but is not removed from the network. By default, all SSIDs are enabled.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0–255. The default value is 64.
Local Probe Request Threshold	Specify a threshold value to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests if required. You can specify a RSSI value within range of 0–100 dB.
Min RSSI for auth request	Enter the minimum RSSI threshold for authentication requests.
Deauth inactive clients	Select this option to allow the Instant AP to send a de-authentication frame to the inactive client and the clear client entry.
Can be used without uplink	Select this check-box if you do not want the SSID profile to use the uplink.
Deny inter user bridging	Disables bridging traffic between two clients connected to the same SSID on the same VLAN. When this option is enabled, the clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
Enable SSID when	Select an option from the drop-down list and specify the time period.
Disable SSID when	Select an option from the drop-down list and specify the time period.
Deny Intra VLAN Traffic	Disables intra VLAN traffic to enable the client isolation and disable all peer-to-peer communication. Client isolation disables inter-client communication by allowing only client to gateway traffic from clients to flow in the network. All other traffic from the client that is not destined to the gateway or configured servers will not be forwarded by the Instant AP. This feature enhances the security of the network and protects it from vulnerabilities. For more information, see Configuring Client Isolation.
Management Frame Protection	Turn on the **Management Frames Protection** toggle switch to provide high network security by maintaining data confidentiality of management frames. The Management Frame Protection (MFP) establishes encryption keys between the client and Instant AP using 802.11i framework. For more information, see Configuring Management Frames Protection.
Fine Timing Measurement (802.11mc) Responder Mode	Turn on the toggle switch to enable the fine timing measurement (802.11mc) responder mode.
Time Range Profiles	

Parameter	Description
Time Range Profiles	Ensure that the NTP server connection is active. Select a time range profile from the **Time Range Profiles** list and apply a status form the drop-down list. Click **+ New Time Range Profile** to create a new time range profile. For more information, see Configuring Time-Based Services for Wireless Network Profiles.

Configuring VLAN Settings for Wireless Network

To configure VLANs settings for an SSID, complete the following steps:

1. In the **VLANs** tab, select any of the following options for **Client IP Assignment**:
   - **Instant AP assigned**—When selected, the client obtains the IP address from the VC.
   - **External DHCP server assigned**—When selected, the client obtains the IP address from the network.

2. Based on the type of client IP assignment mode selected, configure the following parameters:

Table 133: *VLANs Parameters*

Parameter	Description
Instant AP assigned	When this option is selected, the client obtains the IP address from the virtual controller. The virtual controller creates a private subnet and VLAN on the Instant AP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP Pools and Client IP Assignment Modes on Instant APs. If this option is selected, specify any of the following options in **Client VLAN Assignment**: ■ **Internal VLAN**—Assigns IP address to the client in the same subnet as the Instant APs. By default, the client VLAN is assigned to the native VLAN on the wired network. ■ **Custom**—Allows you to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. When this option is selected, select the scope from the **VLAN ID** drop-down list.
External DHCP server assigned	When this option is selected, specify any of the following options in **Client VLAN Assignment**: ■ **Static**—In **VLAN ID**, specify a VLAN ID for a single VLAN(s). If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID. ◦ To show or hide the Named VLANs, click **Show Named VLANs**. Click **Show Named VLANs** to view the Named VLAN table. To add a new Named VLAN, complete the following steps: a. Click **+Add Named VLAN**. The **Add Named VLAN** window is displayed. b. Enter the **VLAN Name** and **VLAN** details, and then click **OK**. ■ **Dynamic**—Assigns the VLANs dynamically from a DHCP server. ◦ To add a new VLAN assignment rule, complete the following steps: a. Click **+ Add Rule** in the **VLAN Assignment Rules** window. The **New VLAN Assignment Rule** page is displayed. b. Enter the **Attribute**, **Operator**, **String**, and **VLAN** details, and then click **OK**. ◦ To delete a VLAN assignment rule, select a rule in the **VLAN Assignment Rules** window, and then click the delete icon. ◦ To show or hide the Named VLANs, click **Show Named VLANs**. Click **Show Named VLANs** to view the Named VLAN table. To add a new Named VLAN, complete the following steps: a. Click **+Add Named VLAN**. The **Add Named VLAN** window is displayed. b. Enter the **VLAN Name** and **VLAN** details, and then click **OK**. ◦ To delete, select a Named VLAN in the Named VLAN table, and then click the delete icon. ■ **Native VLAN**—Assigns the client VLAN is assigned to the native VLAN.

3. Click **Next**.

Configuring Security Settings for Wireless Network

To configure security settings for mixed traffic or voice network, complete the following steps:

1. In the **Security** tab, specify any one of the following options in the **Security Level**:
   - **Enterprise**—On selecting **Enterprise** security level, the authentication options applicable to the network are displayed.
   - **Personal**—On selecting **Personal** security level, the authentication options applicable to the personalized network are displayed.
   - **Captive Portal**—On selecting **Captive Portal** security level, the authentication options applicable to the captive portal is displayed. For more information on captive portal, see Configuring Wireless Networks for Guest Users on Instant APs.
   - **Open**—On selecting **Open** security level, the authentication options applicable to an open network are displayed.

The default security setting for a network profile is **Personal**.

2. Based on the security level specified, configure the following basic parameters:

Table 134: *Basic WLAN Security Parameters*

Data Pane Item	Description
Key Management	For **Enterprise** security level, select an encryption key from **Key Management** drop-down list: ■ **WPA-2 Enterprise**—Select this option to use WPA-2 security. The WPA-2 Enterprise requires user authentication and requires the use of a RADIUS server for authentication. ■ **WPA Enterprise**—Select this option to use both WPA Enterprise. ■ **Both (WPA-2 & WPA)**—Select this option to use both WPA-2 and WPA security. ■ **Dynamic- WEP with 802.1X**—If you do not want to use a session key from the RADIUS Server to derive pairwise unicast keys, turn on the **Use Session Key for LEAP** toggle switch. This is required for old printers that use dynamic WEP through LEAP authentication. The **Use Session Key for LEAP** feature is **Disabled** by default. ■ **WPA-3 Enterprise(CNSA)**—Select this option to use WPA-3 security employing CNSA encryption. ■ **WPA-3 Enterprise(CCM 128)**—Select this option to use WPA-3 security employing CCM encryption operation mode limited to encrypting 128 bits of plain text. ■ **WPA-3 Enterprise(GCM 256)**—Select this option to use WPA-3 security employing GCM encryption operation mode limited to encrypting 256 bits of plain text. **NOTE:** When any of the aforementioned encryption types is selected and if 802.1x authentication method is configured, ensure that the **Opportunistic key caching (OKC)** and **802.11r** toggle switches under **Advanced Settings** are turned on. This enables OKC and 802.11r protocols and allows faster roaming of clients without the need for a complete 802.1x authentication. You can configure both OKC and 802.11r roaming only for the **Enterprise** security level.
	For **Personal** security level, select an encryption key from **Key Management** drop-down list: ■ For **WPA-2 Personal**, **WPA Personal**, **Both (WPA-2&WPA)**, and **WPA-3 Personal** keys, specify the following parameters:

Data Pane Item	Description
	a. **Passphrase Format**—Select a passphrase format. The options available are 8-63 alphanumeric characters and 64 hexadecimal characters. b. **Passphrase**—Enter a passphrase. c. **Retype**—Retype the passphrase to confirm. ■ For **Static WEP**, specify the following parameters: a. **WEP Key Size**—Select an appropriate value for WEP key size from the drop-down list. Select an appropriate value from the **Tx Key** drop-down list. b. **WEP Key**—Enter an appropriate WEP key. c. **Retype WEP Key**—Retype the WEP key to confirm. ■ For **MPSK-AES**, select a primary server from the drop-down list. ■ For **MPSK-LOCAL**, select a Mpsk Local server from the drop-down list.
	For **Captive Portal** security level, select an encryption key from **Key Management** drop-down list: ■ For **WPA-2 Personal**, **WPA Personal**, **Both (WPA-2&WPA)**, and **WPA-3 Personal** keys, specify the following parameters: a. **Passphrase Format**—Select a passphrase format. The options available are 8-63 alphanumeric characters and 64 hexadecimal characters. b. **Passphrase**—Enter a passphrase. c. **Retype**—Retype the passphrase to confirm. ■ For **Static WEP**, specify the following parameters: a. **WEP Key Size**—Select an appropriate value for WEP key size from the drop-down list. Select an appropriate value from the **Tx Key** drop-down list. b. **WEP Key**—Enter an appropriate WEP key. c. **Retype WEP Key**—Retype the WEP key to confirm. For information on configuring captive portal, see Configuring Wireless Networks for Guest Users on Instant APs.
	For **Open** security level, the **Key Management** includes **Open** and **Enhanced Open** options.
EAP offload	This option is applicable to **Enterprise** security levels only. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, turn on the **EAP offload** toggle switch. Enabling **EAP offload** can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the Instant AP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the Instant AP acts as a relay for this exchange. When EAP Offload is enabled, the Instant AP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the Instant AP and the authentication server. Instant supports the configuration of primary and backup authentication servers in an EAP termination-enabled SSID. If you are using LDAP for authentication, ensure that Instant AP termination is configured to support EAP.
Authentication Server	Configure the following parameters: ■ **MAC Authentication**—Turn on the **MAC Authentication** toggle switch to allow

Data Pane Item	Description
	MAC address based authentication for **Personal**, **Captive Portal**, and **Open** security levels. ▪ **Primary Server**—Set a primary authentication server. The **Primary Server** option appears only for Enterprise security level, internal and external captive portal types. Select one of the following options from the drop-down list: ▪ **Internal Server**—To use an internal server, select **Internal Server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. To add a new server, click **+**. For information on configuring external servers, see Configuring External Authentication Servers for APs. Aruba Central allows you to configure an external RADIUS server, TACACS or LDAP server, and External Captive Portal for user authentication. ▪ **Secondary Server**—To add another server for authentication, configure another authentication server. ▪ **Authentication Survivability**—If an external server is configured for authentication, you can enable authentication survivability. Specify a value in hours for **Cache Timeout** to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours. By default, authentication survivability is disabled. ▪ **Load Balancing**—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring External Authentication Servers for APs.
Users	Click **Users** to add the users. The registered users of **Employee** type will be able to access the users of **Enterprise** network. To add a new user, click **+ Add User** and enter the new user in the **Add User**pane. The **Primary Server** option appears only for **Enterprise** security level, **Internal Captive Portal**, and **External Captive Portal**.

3. Based on the security level specified, specify the following parameters in the **Advanced Settings** section:

Table 135: *Advanced WLAN Security Parameters*

Data pane item	Description
Use Session Key for LEAP	Turn on the toggle switch to use the session key for Lightweight Extensible Authentication Protocol. This option is available only for **Enterprise** level.
MAC Authentication for Enterprise Networks	To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the toggle switch to enable **MAC Authentication**. For **Enterprise** security level, the following options are available: ▪ **Perform MAC authentication before 802.1X**—Select this to use 802.1X authentication only when the MAC authentication is successful. ▪ **MAC Authentication Fail-Through**—On selecting this, the 802.1X authentication is attempted when the MAC authentication fails.

Data pane item	Description
	■ If **MAC Authentication** is enabled, configure the following parameters: ■ **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled. ■ **Uppercase Support**—Turn on the toggle switch to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Reauth Interval	Specify a value for **Reauth Interval**. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients. If the re-authentication interval is configured: ■ On an SSID performing L2 authentication (MAC or 802.1X authentication): When re-authentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful re-authentication. If re-authentication fails, the client retains the pre-authentication role. ■ On an SSID performing both L2 and L3 authentication (MAC with captive portal authentication): When re-authentication succeeds, the client retains the role that is already assigned. If re-authentication fails, a pre-authentication role is assigned to the client. ■ On an SSID performing only L3 authentication (captive portal authentication): When re-authentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access.
Denylisting	By default, this option is disabled. To enable denylisting of the clients with a specific number of authentication failures, select **Denylisting** and specify a value for **Max Authentication Failures**. The users who fail to authenticate the number of times specified in **Max Authentication Failures** field are dynamically denylisted. By default, the **Denylisting** option is disabled.
Enforce DHCP	Enforces WLAN SSID on Instant AP clients. When DHCP is enforced: ■ A layer-2 user entry is created when a client associates with an Instant AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the Instant APs, the DHCP state and the client IP address is synchronized with the new Instant AP.
WPA3 Transition	Enable this option to allow transition from WPA3 to WPA2 and vice versa. The WPA3 Transition appears only when WPA3 is selected in the **Key Management** for **Personal**, **Captive Portal**, and **Open** level.

Data pane item	Description
Legacy Support	Enable this option to allow backward compatibility of encryption modes in networks. The **Legacy Support** appears only when WPA3 is selected in the **Key Management** for **Personal**, **Captive Portal**, and **Open** level.
Use IP for Calling Station ID	Enable this option to configure client IP address as calling station ID. When this option is enabled, the following options are displayed: ▪ **Called Station ID Type**—Select any of the following options for configuring called station ID: ◦ **Access Point Group**—Uses the VC ID as the called station ID. ◦ **Access Point Name**—Uses the host name of the Instant AP as the called station ID. ◦ **VLAN ID**—Uses the VLAN ID of as the called station ID. ◦ **IP Address**—Uses the IP address of the Instant AP as the called station ID. ◦ **MAC address**—Uses the MAC address of the Instant AP as the called station ID. ▪ **Called Station ID Include SSID**—Appends the SSID name to the called station ID. **NOTE:** The **Called Station ID Type** detail can be configured even if the **Use IP for Calling Station ID** is set to disabled. ▪ **Called Station ID Delimiter**—Sets delimiter at the end of the called station ID. ▪ **Max Authentication Failures**—Sets a value for the maximum allowed authentication failures.
Delimiter Character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
Uppercase Support	Select this option to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Fast Roaming	Enable the following fast roaming features as per your requirement: ▪ **Opportunistic Key Caching (OKC)**—Turn on the **Opportunistic key caching (OKC)** toggle switch to reduce the time needed for authentication. When OKC is enabled, multiple APs can share Pairwise Master Keys (PMKs) and use these keys when clients roam to a neighboring AP. **NOTE:** The **Opportunistic key caching (OKC)** toggle switch is disabled by default when you select any of the encryption types from the **Key Management** drop-down list. ▪ **802.11k**—Turn on the **802.11k** toggle switch to enable 802.11k roaming. The 802.11k protocol enables Instant APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, Instant APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. ▪ **802.11v**—Turn on the **802.11v** toggle switch to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows the client

Data pane item	Description
	devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best AP to transition to as they roam. ■ **802.11r**—Turn on the **802.11r** toggle switch to enable 802.11r roaming. Selecting this option enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. **NOTE:** For **Enterprise** security level, the **802.11r** toggle switch is disabled by default when you select **WPA2 Enterprise** or **Both (WPA2 & WPA)** encryption types from the **Key Management** drop-down list. However, the **802.11r** toggle switch is not available when you select the remaining encryption types from the **Key Management** drop-down list. Once you enable the **802.11r**, the following field is displayed: ■ **MDID**—In the **MDID** text-box, enter the mobility domain identifier to configure a mobility domain identifier. In a network of standalone Instant APs within the same management VLAN, 802.11r roaming does not work. This is because the mobility domain identifiers do not match across Instant APs. They are auto-generated based on a virtual controller key. You can set a mobility domain identifier for 802.11r SSIDs. For standalone Instant APs in the same management VLAN, 802.11r roaming works only when the mobility domain identifier is configured with the same value.

4. Click **Next**.

Configuring ACLs for User Access to a Wireless Network

You can configure up to 64 access rules for a wireless network profile. To configure access rules for a network, complete the following steps:

1. In the **Access** tab, turn on the **Downloadable Role** toggle switch to allow downloading of pre-existing user roles. For more information, see Configuring Downloadable Roles.

- The **Downloadable Role** feature is optional. The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
- At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see Authentication Servers for Instant APs

2. Click the action corresponding to the server. The **Edit Server** page is displayed.

Viewing Wireless SSID Summary

In the **Summary** tab, the **Network Summary** page displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs. Click **Save Settings** to complete the network profile creation and save

the settings.

Configuring Client Isolation

Aruba Central supports the **Client Isolation** feature isolates clients from one another and disables all peer-to-peer communication within the network. Client isolation disables inter-client communication by allowing only client to gateway traffic from clients to flow in the network. All other traffic from the client that is not destined to the gateway or configured servers will not be forwarded by the Instant AP.

This feature enhances the security of the network and protects it from vulnerabilities. **Client Isolation** can only be configured through the CLI. When **Client Isolation** is configured, the Instant AP learns the IP, subnet mask, MAC, and other essential information of the gateway and the DNS server. A subnet table of trusted destinations is then populated with this information. Wired servers used in the network should be manually configured into this subnet table to serve clients. The destination MAC of data packets sent by the client is validated against this subnet table and only the data packets destined to the trusted addresses in the subnet table are forwarded by the Instant AP. All other data packets are dropped.

Client Isolation feature is supported only in IPv4 networks. This feature does not support **AirGroup** and affects **Chromecast** and **Airplay** services.

Enabling Client Isolation for Wireless Networks in Aruba Central

To enable the Client Isolation feature, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **WLANs** page, click **+ Add SSID**.
   The Create a New Network page is displayed.
6. Click **Advanced Settings** and expand **Miscellaneous**.
7. Turn on the **Deny Intra VLAN Traffic** toggle switch.
8. Click **Next**.

Configuring Management Frames Protection

Aruba Central supports the Management Frame Protection (MFP) feature in networks that include Aruba Instant 8.5.0.0 firmware version and later. This feature protects networks against forged management frames spoofed from other devices that might otherwise disrupt a valid user session.

The MFP increases the security by providing data confidentiality of management frames. MFP uses 802.11i framework that establishes encryption keys between the client and Instant AP.

Enabling Management Frames Protection for Wireless Networks in Aruba Central

To enable the MFP feature, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **WLANs**page, click **+ Add SSID**. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. In the **General** tab, click **Advanced Settings**.
7. Expand **Miscellaneous**.
8. Turn on the **Management Frames Protection** toggle switch to enable the MFP feature.
9. Click **Next**.
10. Click **Save Settings**.

The MFP configuration is a per-SSID configuration. The MFP feature can be enabled only on WPA2-PSK and WPA2-Enterprise SSIDs. The 802.11r fast roaming option will not take effect when the MFP is enabled.

Configuring Wireless Networks for Guest Users on Instant APs

Instant APs support the captive portal authentication method in which a webpage is presented to the guest users, when they try to access the Internet in hotels, conference centers, or Wi-Fi hotspots. The webpage also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The captive portal solution for an Instant AP cluster consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against internal database of the AP.
- The SSID broadcast by the Instant AP.

The Instant AP administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal webpage prompts the user to authenticate with a user name and password.

Splash Page Profiles

Instant APs support the following types of splash page profiles:

- **Internal Captive portal**—Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
  - **Internal Authenticated**—When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.

- **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.

- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.
- **None**—Select to disable the captive portal authentication.

To create splash page profiles, see the following sections:

- Creating a Wireless Network Profile for Guest Users
- Configuring an Internal Captive Portal Splash Page Profile
- Configuring an External Captive Portal Splash Page Profile
- Configuring a Cloud Guest Splash Page Profile
- Configuring a Cloud Guest Splash Page Profile
- Configuring ACLs for Guest User Access
- Configuring Captive Portal Roles for an SSID
- Disabling Captive Portal Authentication

Creating a Wireless Network Profile for Guest Users

To create an SSID for guest users, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **WLANs** page, click **+ Add SSID**.
   The Create a New Network pane is displayed.
6. Under **General**, enter a network name in the **Name (SSID)** text-box.
7. If configuring a wireless guest profile, set the required WLAN configuration parameters described in Table 1.
8. Click **Next**.
   The VLANs details are displayed.
9. Under **VLANs**, select any of the following options for **Client IP Assignment**:

Table 136: *VLANs Assignment*

Parameter	Description
Instant AP assigned	When this option is selected, the client obtains the IP address from the virtual controller. The virtual controller creates a private subnet and VLAN on the Instant AP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP Pools and Client IP Assignment Modes on Instant APs. If this option is selected, specify any of the following options in **Client VLAN Assignment**: ■ **Internal VLAN**—Assigns IP address to the client in the same subnet as the Instant APs. By default, the client VLAN is assigned to the native VLAN on the wired network. ■ **Custom**—Allows you to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. When this option is selected, select the scope from the **VLAN ID** drop-down list.
External DHCP server assigned	When this option is selected, specify any of the following options in **Client VLAN Assignment**: ■ **Static**—In **VLAN ID**, specify a VLAN ID for a single VLAN(s). If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID. ◦ To show or hide the Named VLANs, click **Show Named VLANs**. Click **Show Named VLANs** to view the Named VLAN table. To add a new Named VLAN, complete the following steps: a. Click **+Add Named VLAN**. The **Add Named VLAN** window is displayed. b. Enter the **VLAN Name** and **VLAN** details, and then click **OK**. ■ **Dynamic**—Assigns the VLANs dynamically from a DHCP server. ◦ To add a new VLAN assignment rule, complete the following steps: a. Click **+ Add Rule** in the **VLAN Assignment Rules** window. The **New VLAN Assignment Rule** page is displayed. b. Enter the **Attribute**, **Operator**, **String**, and **VLAN** details, and then click **OK**. ◦ To delete a VLAN assignment rule, select a rule in the **VLAN Assignment Rules** window, and then click the delete icon. ◦ To show or hide the Named VLANs, click **Show Named VLANs**. Click **Show Named VLANs** to view the Named VLAN table. To add a new Named VLAN, complete the following steps: a. Click **+Add Named VLAN**. The **Add Named VLAN** window is displayed. b. Enter the **VLAN Name** and **VLAN** details, and then click **OK**. ◦ To delete, select a Named VLAN in the Named VLAN table, and then click the delete icon. ■ **Native VLAN**—Assigns the client VLAN is assigned to the native VLAN. For more information, see Configuring VLAN Assignment Rule.

Configuring an Internal Captive Portal Splash Page Profile

To configure an internal captive portal profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a guest SSID, and then click the edit icon.
6. Under **Security** tab, in the **Security Level**, select **Captive Portal** and configure the following parameters:

Table 137: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Captive Portal Type	Select **Internal** from the drop-down list.
Captive Portal Location	Select **Acknowledged** or **Authenticated** from the drop-down list.
Customize Captive Portal	Under **Splash Page**, when **Customize Captive Portal** is clicked, use the editor to specify text and colors for the initial page that is displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (**Authenticated** or **Acknowledged**) for which you are customizing the splash page design. Complete the following steps to customize the splash page design. ▪ **Top banner title**—Enter a title for the banner. ▪ **Header fill color**—Specify a background color for the header. ▪ **Welcome text**—To change the welcome text, click the first square box in the splash page, enter the required text in the **Welcome text** box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ▪ **Policy text**—To change the policy text, click the second square in the splash page, enter the required text in the **Policy text** box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ▪ **Page fill color**—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ▪ **Redirect URL**—To redirect users to another URL, specify a URL in **Redirect URL**. ▪ **Logo image**—To upload a custom logo, click **Choose File**to upload. Ensure that the image file size does not exceed 16 KB. To delete an image, click **Delete Logo**. To preview the captive portal page, click **preview_splash_page**.

Table 137: *Internal Captive Portal Configuration Parameters*

Parameter	Description
	To configure a captive portal proxy server or global proxy server to match your browser configuration, enter the IP address and port number in the **Captive-portal proxy server IP** and **Captive Portal Proxy Server Port** fields.
Encryption	By default, this field is disabled. Turn on the toggle switch to enable and configure the following encryption parameters: a. **Key Management**—Specify an encryption and authentication key. b. **Passphrase format**—Specify a passphrase format. c. **Passphrase**—Enter a passphrase. d. **Retype**—Retype the passphrase to confirm.
Key Management	Select **Open** or **Enhanced Open** from the drop-down list.
Advanced Settings	
Captive Portal Proxy Server IP	Specify the IP address of the Captive Portal proxy server.
Captive Portal Proxy Server Port	Specify the port number of the Captive Portal proxy server.
MAC Authentication	Configure the following parameters: ▪ **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the **MAC Authentication** toggle switch. ▪ **Secondary Server**—To add another server for authentication, configure another authentication server. ▪ **Load Balancing**—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients. To use an internal server, select **Internal Server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. To add a new server, click **+**. For information on configuring external servers, see Configuring External Authentication Servers for APs.
Reauth Interval	Specify a value for **Reauth Interval**. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.
Accounting	Select an accounting mode for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client disconnects. This is applicable for WLAN SSIDs only.

Table 137: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Denylisting	If you are configuring a wireless network profile, turn on the **Denylisting** toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Max Authentication Failures	If you are configuring a wireless network profile, turn on the **Denylisting** toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Enforce DHCP	If you are configuring a wireless network profile, turn on the **Denylisting** toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
WPA3 Transition	If you are configuring a wireless network profile, turn on the **Denylisting** toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Called Station ID Include SSID	If you are configuring a wireless network profile, turn on the **Denylisting** toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Uppercase Support	If you are configuring a wireless network profile, turn on the **Denylisting** toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Disable if uplink type is	To exclude uplink(s), expand **Disable if uplink type is**, and turn on the toggle switch for the uplink type(s). For example, **Ethernet**, **Wi-Fi**, and **3G/4G**.

7. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles and associate these profiles with an SSID or a wired profile. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.

5. In the **Wireless SSIDs** table, select a guest SSID, and then click the edit icon.
6. Under **Security** tab, in the **Security Level**, select **Captive Portal**.
7. Select the **Splash Page** type as **External**.
8. If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive Portal Proxy Server IP** and **Captive Portal Proxy Server Port** fields.
9. Select a captive portal profile. To add a new profile, click **+** and configure the following parameters:

Table 138: *External Captive Portal Profile Configuration Parameters*

Data Pane Item	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: ▪ **Radius Authentication**—Select this option to enable user authentication against a RADIUS server. ▪ **Authentication Text**—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or Hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL of the external captive portal server.
Port	Enter the port number that is used for communicating with the external captive portal server.
Use HTTPS	Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected.
Captive Portal Failure	This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select **Deny Internet** to prevent guest users from using the network, or **Allow Internet** to access the network.
Server Offload	Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server.
Prevent Frame Overlay	Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
Automatic URL Allowlisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically allowlisted.
Auth Text	If the **External Authentication splash** page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

10. Click **Save**.
11. On the external captive portal splash page configuration page, specify encryption settings if required.

12. Specify the following authentication parameters under **Advanced Settings**:
    - **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the **MAC Authentication** toggle switch.
    - **Primary Server**—Sets a primary authentication server.
        - To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users.
        - To add a new server, click **+**. For information on configuring external servers, see Configuring External Authentication Servers for APs.
    - **Secondary Server**—To add another server for authentication, configure another authentication server.
    - **Load Balancing**—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers.
13. If required, under **Walled Garden**, create a list of domains that are denylisted and also a allowlist of websites that the users connected to this splash page profile can access.
14. To exclude uplink, select an uplink type.
15. If MAC authentication is enabled, you can configure the following parameters:
    - **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
    - **Uppercase Support**—Turn on the toggle switch to enable to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
16. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, Instant APs periodically re-authenticate all associated and authenticated clients.
17. If required, enable denylisting. Set a threshold for denylisting clients based on the number of failed authentication attempts.
18. Click **Save Settings**.

Configuring a Cloud Guest Splash Page Profile

To create a cloud guest network profile, see Configuring a Guest Splash Page Profile

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest splash page profile for the guest SSID, ensure that the Cloud Guest splash Page profile is configured through the **Guest Access** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.

   The tabs to configure the APs are displayed.

4. Click the **WLANs** tab.

   The WLANs details page is displayed.
5. Under **WLANs** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
6. Click the **Security** tab.
   a. Under **Splash Page**, select **Cloud Guest** from the **Captive Portal Type** drop-down list.
   b. Select the splash page profile name from the **Guest Captive Portal Profile** list, and then click **Next**.
   c. To enable encryption, turn on the **Encryption** toggle switch and configure the following encryption parameters:
      i. **Key Management**—Specify an encryption and authentication key.
      ii. **Passphrase format**—Specify a passphrase format.
      iii. **Passphrase**—Enter a passphrase.
      iv. **Retype**—Retype the passphrase to confirm.
   d. To exclude uplink, expand **Disable if uplink type is** and select an uplink type. For example, **Ethernet**, **Wi-Fi**, and **3G/4G**.
   e. Click **Next**.
7. Click **Save Settings**.

When you clone an existing group, the unshared splash page profile in the existing group is not cloned to the new group. In the existing group, if an unshared splash page is associated with a guest network, then the splash page value is empty in the guest network of the new group.

Configuring ACLs for Guest User Access

To configure access rules for a guest network, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.

   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.

   The WLANs details page is displayed.
5. Under **WLANs** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
6. Click the **Access** tab.
7. Under **Access rules**, select any of the following types of access control:
   - **Unrestricted**—Select this to set unrestricted access to the network.
   - **Network Based**—Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule, complete the following steps:

a. Click **+** and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
b. Click **Save**.

- **Role Based**—Select **Role Based** to enable access based on user roles.

For role-based access control, complete the following steps:

1. To create a user role:
   a. Click **+ Add Role** in **Role** pane.
   b. Enter a name for the new role and click **OK**.
2. To create access rules for a specific user role:
   a. Click **+ Add Rule** in **Access Rules for Selected Roles**, and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
   b. Click **Save**.
3. To create a role assignment rule:
   a. Under **Role Assignment Rules**, click **+ Add Role Assignment**. The **New Role Assignment Rule** pane is displayed.
   b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.
   c. Click **Save**.
4. To assign pre-authentication role, select the **Assign Pre-Authentication Role** check-box and select a pre-authentication role from the drop-down list.
5. Click **Save Settings**.

Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce captive portal authentication for SSIDs with 802.1X authentication enabled. You can configure rules to provide access to an external captive portal, internal captive portal, so that some of the clients using this SSID can derive the captive portal role.

The following conditions apply to the 802.1X and captive portal authentication configuration:

- If captive portal settings are not configured for a user role, the captive portal settings configured for an SSID are applied to the client's profile.
- If captive portal settings are not configured for a SSID, the captive portal settings configured for a user role are applied to the client's profile.
- If captive portal settings are configured for both SSID and user role, the captive portal settings configured for a user role are applied to the profile of the client.

To create a captive portal role for the **Internal** and **External** splash page types:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.

5. Under **WLANs** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
6. Click the **Access** tab.
7. Under **Access rules**, select **Role Based**.
8. Click **+ Add Rule** in **Access Rules for Selected Roles**.
9. In the **Add Rules** window, specify the following parameters.

Table 139: *Access Rule Configuration Parameters*

Data Pane Item	Description
Rule Type	Select **Captive Portal** from the drop-down list.
Splash Page Type	Select a splash page type from the drop-down list.
Internal	If **Internal** is selected as **Splash Page Type** drop-down list, complete the following steps: ■ **Top banner title**—Enter a title for the banner. To preview the page with the new banner title, click **Preview** splash page. ■ **Header fill color**—Specify a background color for the header. ■ **Welcome text**—To change the welcome text, click the first square box in the splash page, enter the required text in the **Welcome text** box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ■ **Policy text**—To change the policy text, click the second square in the splash page, enter the required text in the **Policy text** box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ■ **Page fill color**—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ **Redirect URL**—To redirect users to another URL, specify a URL in **Redirect URL**. ■ **Logo image**—To upload a custom logo, click **Choose File**to upload. Ensure that the image file size does not exceed 16 KB. To delete an image, click **Delete Logo**. To preview the captive portal page, click **preview_splash_page**.
External	If **External** is selected as **Splash Page Type** drop-down list, complete the following steps: ■ **Captive Portal Profile**—Select a profile from the drop-down list. To create a profile, click the **+** icon and enter the following information in the **External Captive Portal** window. ■ **Name**—Enter a name for the profile. ■ **Authentication Type**—From the drop-down list, select either **RADIUS Authentication** (to enable user authentication against a RADIUS server) or **Authentication Text** (to specify the authentication text to returned by the external server after a successful user authentication). ■ **IP OR Hostname**—Enter the IP address or the hostname of the external splash page server. ■ **URL**—Enter the URL for the external splash page server. ■ **Port**—Enter the port number for communicating with the external splash page server. ■ **Captive Portal Failure**—This field allows you to configure Internet access for the guest clients when the external captive portal server is not available. From the drop-down list,

Table 139: *Access Rule Configuration Parameters*

Data Pane Item	Description
	select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available. ▪ **Automatic URL Allowlisting**—Turn on the toggle switch to enable or disable automatic allowlisting of URLs. On selecting this for the external captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically allowlisted. The automatic URL allowlisting is disabled by default. ▪ **Server offload**—Turn on the toggle switch to offload the server. ▪ **Prevent Frame Overlay**—Turn on the toggle switch to prevent frame overlay. ▪ **Use VC IP in Redirect URL**—Turn on the toggle switch to use the virtual controller IP address as a redirect URL. ▪ **Auth TEXT**—Indicates the authentication text returned by the external server after a successful user authentication. ▪ **Redirect URL**—Specify a redirect URL to redirect the users to another URL. To edit a profile, click the edit icon and modify the parameters in the **External Captive Portal** window.

10. Click **Save**. The enforce captive portal rule is created and listed as an access rule.
11. Click **Save Settings**.

The client can connect to this SSID after authenticating with user name and password. After the user logs in successfully, the captive portal role is assigned to the client.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a guest SSID, and then click the edit icon.
6. Under **Security** tab, in the **Security Level**, select **Captive Portal**.
7. Under **Splash Page**, select **None** from the **Captive Portal Type** drop-down list.
8. Click **Save Settings**.

Configuring Wired Networks for Guest Users on Instant APs

Instant APs support the captive portal authentication method in which a webpage is presented to the guest users, when they try to access the Internet in hotels, conference centres, or Wi-Fi hotspots. The webpage

also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The captive portal solution for an Instant AP cluster consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against internal database of the AP.
- The SSID broadcast by the Instant AP.

The Instant AP administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal webpage prompts the user to authenticate with a user name and password.

Splash Page Profiles

Instant APs support the following types of splash page profiles:

- **Internal Captive portal**—Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
  - **Internal Authenticated**—When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
  - **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.
- **None**—Select to disable the captive portal authentication.

For information on how to create splash page profiles, see the following sections:

- Creating a Wired Network Profile for Guest Users
- Configuring an Internal Captive Portal Splash Page Profile
- Configuring an External Captive Portal Splash Page Profile
- Configuring a Cloud Guest Splash Page Profile
- Disabling Captive Portal Authentication

Creating a Wired Network Profile for Guest Users

To create a wired SSID for guest access, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.

4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Wired** accordion.
7. To create a new wired SSID profile, click **+ Add Port Profile**.
   The **Create a New Network** pane is displayed.
8. Under **General**, enter the following information:
   a. **Name**—Enter a name.
   b. **ports**—Select port(s) form the drop-down list.
9. Click **Next** to configure the **VLANs** settings.
   The VLANs details are displayed.
10. In the **VLANs** tab, select a type of mode from the **Mode** drop-down list.
11. Select any of the following options for **Client IP Assignment**:

Table 140: *VLANs Parameters*

Parameter	Description
Instant AP assigned	Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client. If this option is selected, specify any of the following options in **Client VLAN Assignment**: ▪ **Default**—When the client VLAN must be assigned to the native VLAN on the network. ▪ **Custom**—To customize the client VLAN assignment to a specific VLAN, or a range of VLANs.
External DHCP server assigned	Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

Configuring an Internal Captive Portal Splash Page Profile

To configure internal captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Ports** > **Security** page.

Table 141: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Captive Portal Type	Select any of the following from the drop-down list: ■ **Internal - Authenticated**—When **Internal Authenticated** is selected, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. ■ **Internal - Acknowledged**—When **Internal Acknowledged** is selected, the guest users are required to accept the terms and conditions to access the Internet. ■ **External**—When **External** is selected, the guest users are required to enter the proxy server details such as IP address and captive portal proxy server port details. Also enter the details in **Walled Garden**, and **Advanced** section. ■ **Cloud Guest**—When **Cloud Guest** is selected, the guest users are required to select the **Guest Captive Portal Profile**. ■ **None**—Select this option if you do not want to set any splash page.
Captive Portal Location	Select **Acknowledged** or **Authenticated** from the drop-down list.
Splash Page Properties	**Policy text** for which you are customizing the splash page design. Perform the following steps to customize the splash page design. ■ **Top Banner Title**—Enter a title for the banner. To preview the page with the new banner title, click **Preview Splash Page**. ■ **Header fill color**—Specify a background color for the header. ■ **Welcome Text**—To change the welcome text, click the first square box in the splash page, enter the required text in the **Welcome Text** box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ■ **Policy Text**—To change the policy text, click the second square in the splash page, enter the required text in the **Policy Text** box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ■ **Page Fill Color**—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ **Redirect URL**—To redirect users to another URL, specify a URL in **Redirect URL**. ■ **Logo Image**—To upload a custom logo, click **Upload**, browse the image file, and click **upload image**. Ensure that the image file size does not exceed 16 KB. To delete an image, click **Delete**. To preview the captive portal page, click **Preview** splash page. To configure a captive portal proxy server or global proxy server to match your browser configuration, enter the IP address and port number in the **Captive-portal proxy server IP** and **Captive Portal Proxy Server Port** fields.
Encryption	By default, this field is disabled. Turn on the toggle switch to enable and configure the following encryption parameters:

Table 141: *Internal Captive Portal Configuration Parameters*

Parameter	Description
	a. **Key Management**—Specify an encryption and authentication key. b. **Passphrase format**—Specify a passphrase format. c. **Passphrase**—Enter a passphrase and retype to confirm.
Authentication	Configure the following parameters: ▪ **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the **MAC Authentication** toggle switch. ▪ **Secondary Server**—To add another server for authentication, configure another authentication server. ▪ **Load Balancing**—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients. To use an internal server, select **Internal Server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. To add a new server, click **+**. For information on configuring external servers, see Configuring External Authentication Servers for APs.
Users	Create and manage users in the captive portal network. Only registered users of type **Guest Employee** will be able to access this network.
Advanced Settings > **MAC Authentication**	To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the **MAC Authentication** toggle switch.
Advanced Settings > **Reauth Interval**	Specify a value for **Reauth Interval**. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.
Advanced Settings > **Denylisting**	If you are configuring a wireless network profile, turn on the **Denylisting** toggle switch to denylist clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Advanced Settings > **Disable If Uplink Type Is**	To exclude uplink, select an uplink type.

2. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security** > **External Captive Portal** data pane and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network pane. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the

captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. Under **WLANs** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
   The Create a New Network pane is displayed.
2. Under **Security** tab, in the **Security Level**, select **Captive Portal** and configure the following parameters under **Splash Page**:
3. Select the Splash Page type as **External**.
4. If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive Portal Proxy Server IP** and **Captive Portal Proxy Server Port** fields.
5. Select a captive portal profile. To add a new profile, click **+** and configure the following parameters:

Table 142: *External Captive Portal Profile Configuration Parameters*

Data Pane Item	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: ▪ **Radius Authentication**—Select this option to enable user authentication against a RADIUS server. ▪ **Authentication Text**—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or Hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL of the external captive portal server.
Port	Enter the port number that is used for communicating with the external captive portal server.
Use HTTPS	Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected.
Captive Portal Failure	This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select **Deny Internet** to prevent guest users from using the network, or **Allow Internet** to access the network.
Server Offload	Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server.
Prevent Frame Overlay	Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
Automatic URL Allowlisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically allowlisted.

Data Pane Item	Description
Auth Text	If the **External Authentication Splash** page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

6. Click **Save**.
7. On the external captive portal splash page configuration page, specify encryption settings if required.
8. Specify the following authentication parameters in **Advanced Settings**:
   - **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, turn on the **MAC Authentication** toggle switch.
   - **Primary Server**—Sets a primary authentication server.
     - To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users.
     - To add a new server, click **+**. For information on configuring external servers, see Configuring External Authentication Servers for APs.
   - **Secondary Server**—To add another server for authentication, configure another authentication server.
   - **Load Balancing**—Turn on the toggle switch to enable, if you are using two RADIUS authentication servers, to balance the load across these servers.
9. If required, under **Walled Garden**, create a list of domains that are denylisted and also an allowlist of websites that the users connected to this splash page profile can access.
10. To exclude uplink, select an uplink type.
11. If MAC authentication is enabled, you can configure the following parameters:
    - **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
    - **Uppercase Support**—Turn on the toggle switch to enable, to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
12. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, Instant APs periodically re-authenticate all associated and authenticated clients.
13. If required, enable denylisting. Set a threshold for denylisting clients based on the number of failed authentication attempts.
14. Click **Save Settings**.

Configuring a Cloud Guest Splash Page Profile

For information on how to create a cloud guest network profile, see Configuring a Guest Splash Page Profile

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest Splash page profile for the guest SSID, ensure that the Cloud Guest Splash Page profile is configured through the **Guest Access** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. Under **WLANs** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.

   The Create a New Network pane is displayed.
2. Click the **Security** tab.
   a. Select **Cloud Guest** from the **Splash Page Type** list.
   b. Select the splash page profile name from the **Guest Captive Portal Profile** list, and then click **Next**.
   c. To enable encryption, turn on the **Encryption** toggle switch and configure the encryption parameters.
   d. To exclude uplink, select **3G/4G**, **Wi-Fi**, or **Ethernet** option from **Disable If Uplink Type Is** accordion.
   e. Click **Next**.
3. Click **Save Settings**.

Configuring ACLs for Guest User Access

To configure access rules for a guest network, complete the following steps:

1. Under **WLANs** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.

   The Create a New Network pane is displayed.
2. Click the **Access** tab.
3. Under **Access**, select any of the following types of access control:
   - **Unrestricted**—Select this to set unrestricted access to the network.
   - **Network Based**—Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule, complete the following steps:
     a. Click **+** and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
     b. Click **Save**.
   - **Role Based**—Select **Role Based** to enable access based on user roles. For role-based access control, complete the following steps:
     - Create a user role:
       a. Click **New** in **Role** pane.
       b. Enter a name for the new role and click **OK**.
     - Create access rules for a specific user role:
       a. Click **+** and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
       b. Click **Save**.
     - Create a role assignment rule:
       a. Under **Role Assignment Rule**, click **New**. The **New Role Assignment Rule** pane is displayed.
       b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.
       c. Click **Save**.
4. Click **Save Settings**.

Disabling Captive Portal Authentication

To disable captive portal authentication, complete the following steps:

1. Under **WLANs** tab, in the **Wireless SSIDs** table, select a guest SSID and click the edit icon.
   The Create a New Network pane is displayed.
2. Click the **Security** tab.
3. Under **Security**, select **None** for **Splash Page Type**.
4. Click **Save Settings**.

Configuring Wired Port Profiles on Instant APs

If the wired clients must be supported on the Instant APs, configure wired port profiles and assign these profiles to the ports of an Instant AP.

The wired ports of an Instant AP allow third-party devices such as VoIP phones or printers (which support only wired port connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.

To configure wired port profiles on Instant AP, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Wired** accordion.
7. To create a new wired port profile, click **+ Add Port Profile**.
   The Create a New Network pane is displayed.

Complete the configuration for each of the tabs in the **Create a New Network** page as described in the below sections:

Configuring General Network Profile Settings

To configure general network profile settings, complete the following steps in the **General** tab:

1. Under **General**, enter the following information:
   a. **Name**—Enter a name.
   b. **ports**—Select port(s) form the drop-down list.
2. Under **Advanced Settings** section, configure the following parameters:
   - **Speed/Duplex**—Select the appropriate value from the Speed and Duplex drop-down list. Contact your network administrator if you need to assign speed and duplex parameters.
   - **Port Bonding**—Turn on the **Port Bonding** toggle switch to enable port bonding.
   - **Power over Ethernet**—Turn on the **Power over Ethernet** toggle switch to enable PoE.
   - **Admin Status**—The **Admin Status** indicates if the port is up or down.
   - **Content Filtering**—Turn on the **Content Filtering** toggle switch to ensure that all DNS requests to non-corporate domains on this wired port network are sent to OpenDNS.

- **Uplink**—Turn on the toggle switch to configure uplink on this wired port profile. If the **Uplink** toggle switch is turned on and this network profile is assigned to a specific port, the port is enabled as an uplink port.
- **Spanning Tree**—Turn on the toggle switch to enable STP on the wired port profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP does not operate on uplink ports and is supported only on Instant APs with three or more ports. By default, STP is disabled on wired port profiles.
- **Inactivity Timeout**—Enter the time duration after which an inactive user needs to be disabled from the network. The user must undergo the authentication process to re-join the network.
- **802.3az**—Turn on the toggle switch to enable, to support 802.3az Energy Efficient Ethernet (EEE) standard on the device. This option allows the device to consume less power during periods of low data activity. This setting can be enabled for provisioned APs or AP groups through the wired port network. If this feature is enabled for an AP group, APs in the group that do not support 802.3.az ignore this setting. This option is available for Instant APs that support a minimum of Aruba Instant 8.4.0.0 firmware version.
- **Deny Intra VLAN Traffic**—Turn on the toggle switch to disable intra VLAN traffic. It enables the client isolation and disable all peer-to-peer communication. Client isolation disables inter-client communication by allowing only client to gateway traffic from clients to flow in the network. All other traffic from the client that is not destined to the gateway or configured servers will not be forwarded by the Instant AP. This feature enhances the security of the network and protects it from vulnerabilities.

3. Click **Next**.

   The VLANs details page is displayed.

Configuring VLAN Network Profile Settings

To configure VLAN settings, complete the following steps in the **VLANs** tab:

1. **Mode**—Specify any of the following modes:
   - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN. If the **Access** mode is selected, perform one of the following options:
     - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 6.
     - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.
   - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs. If the **Trunk** mode is selected:
   - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges, for example 1, 2, 5, or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
   - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.
2. **Client IP Assignment**—specify any of the following values:
   - **Instant AP Assigned**—Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client. In the **Client VLAN Assignment** section, select **Default** when the client VLAN must be assigned to the native VLAN on the network. Select **Custom** to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. Click the **Show Named VLANs**

section to view all the named VLANs mapped to VLAN ID. Click **+ Add Named VLAN** and enter the VLAN Name and VLAN ID that is required to be mapped. Clicking **OK** populates the named VLAN in the VLAN Name to VLAN ID Mapping table.

- **External DHCP server Assigned**—Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

3. Click **Next**.

   The Security details page is displayed.

Configuring Security Settings

To configure security-specific settings, complete the following steps in the **Security** tab:

1. On the **Security** pane, select the following security options as per your requirement:
   - **802.1X Authentication**—Set the toggle button to enable **802.1X Authentication**. Configure the basic parameters such as the authentication server, and MAC Authentication Fail-Through. Select any of the following options for authentication server:
     - **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see Configuring External Authentication Servers for APs.
     - **Internal Server**—If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users.
     - **Load Balancing**—Set the toggle button to enable, if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Authentication Servers.
   - **MAC Authentication**—To enable MAC authentication, enable the toggle button. The MAC authentication is disabled by default.
   - **Captive Portal**—Set the toggle button to enable captive portal authentication. For more information on configuring security on captive portal, see Configuring Wired Networks for Guest Users on Instant APs.
   - **Open**—Set the toggle button to enable, to set security for open network.
2. Enable the **Port Type Trusted** option to connect uplink and downlink to a trusted port only.
3. In the **Primary Server** field, perform one of the following steps:
   - **Internal Server**—To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. To add a new server, click **+**. For information on configuring external servers, see Configuring External Authentication Servers for APs.
   - **Secondary Server**—To add another server for authentication, configure another authentication server.
     - **Load Balancing**—Set the toggle button to enable, if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Authentication Servers.
4. **MAC Authentication Fail-Thru**—Set the toggle button to enable, to attempt 802.1X authentication is attempted when the MAC authentication fails.

5. Under the **Advance Settings** section, configure the following options:
   - **Use IP for Calling Station ID**—Set the toggle button to enable, to configure client IP address as calling station ID.
   - **Called Station ID Type**—Select one of the following options:
     - **Access Point Group**—Uses the VC ID as the called station ID.
     - **Access Point Name**—Uses the host name of the Instant AP as the called station ID.
     - **VLAN ID**—Uses the VLAN ID of as the called station ID.
     - **IP Address**—Uses the IP address of the Instant AP as the called station ID.
     - **MAC address**—Uses the MAC address of the Instant AP as the called station ID.

The **Called Station ID Type** detail can be configured even if the **Use IP for Calling Station ID** is set to disabled.

   - **Reauth Interval**—Specify the interval at which all associated and authenticated clients must be re-authenticated.
6. Click **Next**.

   The Access pane is displayed.

Configuring Access Settings

To configure access-specific settings, complete the following steps:

1. In the **Access** tab, turn on the **Downloadable Role** toggle switch to allow downloading of pre-existing user roles. or more information, see Configuring Downloadable Roles.

- The **Downloadable Role** feature is optional. The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
- At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see Authentication Servers for Instant APs.

2. Click the action corresponding to the server.

   The **Edit Server** page is displayed.

The **Edit Server** page displays the radius server name. The **Name** field is non-editable.

3. Enter the CPPM username along with the CPPM authentication credentials for the radius server.
4. Click **Ok**.
5. Under **Access Rules**, configure the following access rule parameters:
   a. Select any of the following types of access control:
      - **Role-based**—Allows the users to obtain access based on the roles assigned to them.
      - **Unrestricted**—Allows the users to obtain unrestricted access on the port.
      - **Network-based**—Allows the users to be authenticated based on access rules specified for a network.
   b. If the **Role-based** access control is selected:
      - Under **Role**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. To add a new access rule, click **Add Rule** under **Access Rules For**

Selected Roles.

The default role with the same name as the network is automatically defined for each network. The default roles cannot be modified or deleted.

- Configure role assignment rules. To add a new role assignment rule, click **New** under **Role Assignment Rules**. Under **New Role Assignment Rule**:

c. Select an attribute.
d. Specify an operator condition.
e. Select a role.
f. Click **Save**.

6. Click **Finish** to create the wired port profile successfully.

Configuring Network Port Profile Assignment

To map the wired port profile to ethernet ports, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Wired** accordion.
   The Wired Port Profiles page is displayed.
7. In the **Port Profiles Assignments** section, assign wired port profiles to Ethernet ports:
   a. Select a profile from the **Ethernet 0/0**drop down list.
   b. Select the profile from the **Ethernet 0/1** drop down list.
   c. If the Instant AP supports Ethernet 2, Ethernet 3 and Ethernet 4 ports, assign profiles to these ports by selecting a profile from the **Ethernet 0/2**, **Ethernet 0/3**, and **Ethernet 0/4** drop-down list respectively.
8. Click **Save Settings**.

Viewing Wired Port Profile Summary

In the **Summary** tab, the **Network Summary** page displays all the settings configured in the **General**, **VLANs**, **Security**, and **Access** tabs. Click **Save Settings** to complete the network profile creation and save the settings.

Configuring Downloadable Roles

Aruba Central allows you to download pre-existing user roles when you create network profiles.

The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

Aruba Instant and ClearPass Policy Manager include support for centralized policy definition and distribution.

When ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. In order to provide highly granular per-user level access, user roles can be created when a user has been successfully authenticated. During the configuration of a policy enforcement profile in ClearPass Policy Manager, the administrator can define a role that should be assigned to the user after successful authentication. In RADIUS authentication, when ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager.

If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. This feature supports roles obtained by the following authentication methods:

- 802.1X (WLAN and wired users)
- MAC authentication
- Captive Portal

This section describes the following topics:

ClearPass Policy Manager Certificate Validation for Downloadable Role

When a ClearPass Policy Manager server is configured as the domain for RADIUS authentication for downloading user roles, in order to validate the ClearPass Policy Manager customized CA, Instant APs are required to publish the root CA for the HTTPS server to the well-known URL (**http://<clearpass-fqdn>/.wellknown/ aruba/clearpass/https-root.pem**). The Instant AP must ensure that an FQDN is defined in the above URL for the RADIUS server and then attempt to fetch the trust anchor by using the RADIUS FQDN. Upon configuring the domain of the ClearPass Policy Manager server for RADIUS authentication along with a username and password, the Instant AP tries to retrieve the CA from the above well-known URL and store it in flash memory. However, if there is more than one ClearPass Policy Manager server configured for authentication, the CA must be uploaded manually.

Enabling Downloadable Role Feature for Wireless Networks in Aruba Central

To enable the **Downloadable Role** feature, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **WLANs** tab, click **+ Add SSID**. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.

6. In the **Security** tab, select the **RADIUS** server in **Primary Server** field.

At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see Authentication Servers for Instant APs

7. Click **Next**.
8. The **Access** tab is displayed.
9. Turn on the **Downloadable Role** toggle switch to allow downloading of pre-existing user roles. The **CPPM Settings** table with **Name**, **CPPM Username**, and **Actions** columns related to the radius servers are displayed.

- The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
- At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see Authentication Servers for Instant APs

10. Click the action corresponding to the radius server listed in the **CPPM Settings** table. The **Edit Server** page is displayed.

The **Edit Server** page displays the name of the radius server name. The **Name** field is non-editable.

11. Enter the following details:
    a. **CPPM Username**—Enter the ClearPass Policy Manager admin username.
    b. **Password**—Enter the password.
    c. **Retype**—Retype the password.
12. Click **OK**.

Enabling Downloadable Role Feature for Wired Networks in Aruba Central

To enable the **Downloadable Role** feature, perform the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Wired** accordion.
7. Under **Wired**, click **+ Add Port Profile**. To modify an existing profile, select the network that you want to edit in the **Wired Port Profiles** pane, and then click the edit icon.

8. In the **Security** tab, select the **RADIUS** server in **Primary Server** field.

NOTE

At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see Authentication Servers for Instant APs

9. Click **Next**.
10. The **Access** tab is displayed.
11. Enable the **Downloadable Role** option to allow downloading of pre-existing user roles. The **CPPM Settings** table with **Name**, **CPPM Username**, and **Actions** columns related to the radius servers are displayed.

NOTE

- The **Downloadable Role** feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.
- At least one radius server must be configured to apply the **Downloadable Role** feature. For more information on configuring radius server, see Authentication Servers for Instant APs

12. Click the action corresponding to the radius server listed in the **CPPM Settings** table. The **Edit Server** page with the radius server name is displayed.

NOTE

The **Edit Server** page displays the radius server name. The **Name** field is non-editable.

13. Enter the following details:
    a. **CPPM Username**—Enter the ClearPass Policy Manager admin username.
    b. **Password**—Enter the password.
    c. **Retype**—Retype the password.
14. Click **OK**.

Editing a Wireless Network Profile

To edit a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select the network that you want to edit, and then click the edit icon under the **Actions** column.
6. Modify the profile and click **Save Settings**.

NOTE

You can directly edit the SSID name under the **Display Name** column of the **Wireless SSIDs** table. Double-click the relevant SSID that you want to rename, and type the new name. Press Enter to complete the process.

Editing a Wired Port Profile

To edit a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
2. Under **Manage**, click **Devices** > **Access Points**.
3. Click the **Config** icon.
   The tabs to configure APs are displayed.
4. Click **Show Advanced**, and click the **Interfaces** tab.
   The Interfaces details page is displayed.
5. Click the **Wired** accordion.
6. In the **Wired Port Profiles** pane, select the network that you want to edit, and then click the edit icon under the **Actions** column.
7. Modify the profile and click **Save Settings**.

Deleting a Network Profile

To delete a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select the network that you want to delete, and then click the delete icon under the **Actions** column.
6. Click **Yes** in the confirmation dialog box.

Configuring Mesh Instant AP

Mesh Network Overview

The mesh solution effectively expands and configures network coverage for outdoor and indoor enterprises in a wireless environment. The mesh network automatically reconfigures broken or blocked paths when traffic traverses across mesh Instant AP. This feature provides increased reliability by allowing the network to continue operating even when an Instant AP is non-functional or if the device fails to connect to the network.

A mesh network requires at least one valid wired or 3G uplink connection. The mesh network must be provisioned by plugging into the wired network for the first time.

Mesh Instant APs

The Instant APs that are configured for mesh can either operate as mesh portals or as mesh points based on the uplink type.

Instant AP as Mesh Portal

Any provisioned Instant AP that has a valid wired or 3G uplink connection functions as a mesh portal. A mesh portal acts as a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the Instant AP configuration. The mesh portal can also act as a virtual controller.

The mesh portal reboots after 5 minutes, when it loses its uplink connectivity to a wired network.

Instant AP as Mesh Point

The Instant AP without an ethernet link functions as a mesh point. The mesh point establishes an all-wireless path to the mesh portal and provides traditional WLAN services such as client connectivity, IDS capabilities, user role association, and QoS for LAN-to-mesh communication to the clients, and performs mesh backhaul or network connectivity. The mesh points authenticate to the mesh portal and establish a secured link using AES encryption.

- A mesh point also supports LAN bridging by connecting any wired device to the downlink port of the mesh point. In the case of single ethernet port platforms such as Instant AP-105, you can convert the Eth0 uplink port to a downlink port by enabling Eth0 Bridging.
- Redundancy is observed in a mesh network when two Instant APs have valid uplink connections, and most mesh points try to mesh directly with one of the two portals.

There can be a maximum of eight mesh points per mesh portal in a mesh network. When mesh Instant APs boot up, they detect the environment to locate and associate with their nearest neighbor. The mesh Instant APs determine the best path to the mesh portal ensuring a reliable network connectivity.

In a dual-radio Instant AP, the 2.4 GHz radio is always used for client traffic, and the 5 GHz radio is always used for both mesh-backhaul and client traffic.

Automatic Mesh Role Assignment

Aruba Central supports enhanced role detection during Instant AP boot-up and Instant AP running time. When a mesh point discovers that the Ethernet 0 port link is up, it sends loop detection packets to check the availability of Ethernet 0 link. If the Ethernet 0 link is available, the mesh point reboots as a mesh portal. Else, the mesh point does not reboot.

Mesh Role Detection during System Boot-Up

If the ethernet link is down during Instant AP boot-up, the Instant AP acts as a mesh point. If the ethernet link is up, the Instant AP continues to detect if the network is reachable in the following scenarios:

- In a static IP address scenario, the Instant AP acts as a mesh portal if it successfully pings the gateway. Otherwise, it acts as a mesh point.
- In case of DHCP, the Instant AP acts as a mesh portal when it obtains the IP address successfully. Otherwise, it acts as a mesh point.
- In case of IPv6, Instant APs do not support the static IP address but only support DHCP for detection of network reachability.

If the Instant AP has a 3G or 4G USB modem plugged, it always acts as a mesh portal. If the Instant AP is set to Ethernet 0 bridging, it always acts as a mesh point.

Mesh Role Detection during System Running Time

The mesh point uses the Loop Protection for Secure Jack Port feature to detect the loop when the ethernet is up. If the loop is detected, the Instant AP reboots. Otherwise, the Instant AP does not reboot and the mesh role continues to act as a mesh point.

Setting up Instant Mesh Network

To provision Instant APs as mesh Instant APs, complete the following steps:

1. Connect the Instant APs to a wired switch.
2. Ensure that the virtual controller key is synchronized and the country code is configured.
3. Ensure that a valid SSID is configured on the Instant AP.
4. If the Instant AP has a factory default SSID (Instant SSID), delete the SSID.
5. If an ESSID is enabled on the virtual controller, disable it and reboot the Instant AP cluster.
6. Disconnect the Instant APs that you want to deploy as mesh points from the switch, and place the Instant APs at a remote location. The Instant APs come up without any wired uplink connection and function as mesh points. The Instant APs with valid uplink connections function as mesh portals.

Configuring Wired Bridging on Eth0 for Mesh Point

Aruba Central supports wired bridging on the Eth0 port of an Instant AP. You can configure wired bridging, if the Instant AP is configured to function as a mesh point.

To configure support for wired bridging on the Eth0 port of an Instant AP from Aruba Central UI, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select an AP group in the filter:
     a. Set the filter to a group containing at least one AP.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.
   - To select an AP in the filter:
     a. Set the filter to **Global** or a group containing at least one AP.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.
     c. Click an AP listed under **Device Name**.
        The dashboard context for the AP is displayed.
     d. Under **Manage**, click **Devices** > **Access Point**.
2. Click the **Config** icon.
   The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
   The Access Points table is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.

5. Click the **Uplink** tab.
6. To configure a non-native uplink VLAN, specify the number of VLANs in the **Uplink Management VLAN** text-box.
7. From the **Eth0 Mode** drop-down list, select any of the following:
   - **Uplink**—Select this option to change the Eth0 bridging mode to the uplink port.
   - **Downlink**—Select this option to change the Eth0 bridging mode to the downlink port.
8. Click **Save Settings**.

NOTE

After configuring the support for wired bridging on the Eth0 port of an Instant AP, ensure that you reboot the Instant AP.

Mesh Cluster Function

Aruba Central introduces the mesh cluster function for easy deployments of Instant APs. You can configure the ID, password, and also provision Instant APs to a specific mesh cluster.

In a cluster-based scenario, you can configure unlimited mesh profiles in a network. When an Instant AP boots up, it attempts to find a mesh cluster configuration. The Instant AP fetches a pre-existing mesh cluster configuration, if any. Otherwise, it uses the default mesh configuration in which the SSID, password, and cluster name are generated by the virtual controller key.

NOTE

Instant APs that belong to the same mesh network can establish mesh links with each other. The Instant APs can establish a mesh link in a standalone scenario also. However, the network role election does not take place in a standalone environment. Users can set the same mesh cluster configuration to establish mesh links with other networks. For more information on mesh cluster configuration, refer to the *Mesh Instant AP Configuration* chapter of *Aruba Instant User Guide*.

Configuring Time-Based Services for Wireless Network Profiles

Aruba Central allows you to configure the availability of a WLAN SSID at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that you can enable or disable access to the SSID and thus control user access to the network during a specific time period.

Instant APs support the configuration of both absolute and periodic time range profiles. You can configure an absolute time range profile to execute during a specific time frame, or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration.

This section describes the following topics:

Before You Begin

Before you configure time-based services, ensure that the NTP server connection is active.

Creating a Time Range Profile

To create a time range profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **Time-Based Services** accordion.
7. Click **+** in the **Time Based Profiles** table.
   The **New Profile** window for creating a time range profile is displayed.
8. Configure the parameters that are listed in the following table:

Table 143: *Time Range Profile Configuration Parameters*

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile: ▪ **Periodic**—Allows you configure a specific periodicity and recurrence pattern for a time range profile. ▪ **Absolute**—Allows you to configure an absolute day and time range.
Repeat	Specify the frequency for the periodic time range profile: ▪ **Daily**—Enables daily recurrence. ▪ **Weekly**—Allows you define a specific time range with specific start and end days in a week.
Day Range	▪ **Absolute**—For an absolute time range profile, this field allows you to specify the start day and end day, both in **mm/dd/yyyy** format. You can also use the calendar to specify the start and end days. ▪ **Periodic**—For a periodic time range profile, the following **Day Range** options are available: ◦ For daily recurrence—If the **Repeat** option is set to **Daily**, this field allows you to select the following time ranges: • **Monday—Sunday (All Days)** • **Monday—Friday (Weekdays)** • **Saturday—Sunday (Weekend)** For example, if you set the **Repeat** option to **Daily** and then select **Monday—Friday (Weekday)** for **Day Range**, and **Start Time** as 1 and **End time** as 2, the applied time range will be Monday to Friday from 1 am to 2 am; that is, on Monday at 3 am, the profile will not be applied or disabled. ◦ For weekly occurrence—If the **Repeat** option is set to **Weekly**, this field allows you to select the start and end days of a week and time range.

Table 143: *Time Range Profile Configuration Parameters*

Parameter	Description
	For example, if you set **Start Day** as Monday and **End Day** as Friday, and **Start Time** as 1 and **End Time** as 2, the applied time range profile is Monday 1 am to Friday 2 am every week; that is, on Monday at 3 am, the profile will be applied or enabled.
Start Time	Select the start time for the time range profile from the **Hours** and **Minutes** drop-down lists, respectively.
End Time	Select the end time for the time range profile from the **Hours** and **Minutes** drop-down lists, respectively.
Visualization Graph for Time	The Visualization graph (approximated to the hour) provides a visual display of the selected time range (Day Range, Start Time, and End Time) for periodic profiles.

Associating a Time Range Profile to an SSID

To apply a time range profile to an SSID, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile for which you want to apply the time range profile, and then click the edit icon. You can also add a time range profile when configuring an SSID.
6. In **General**, click **Time Range Profiles** under **Advanced Settings**.
7. In the **Time Range Profiles** section, enter the following information:
   - Select a time range profile from the **Time Range Profile** list.
   - Select a value from the **Status** drop-down list.
   - When a time range profile is enabled on SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00 to 13:00, the SSID becomes available only between 12 PM to 1 PM on a given day.
   - If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if configured time-range is 14:00 to 17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.
8. Click **Save**.

To create a time range profile, click **+ New Time Range Profile**. The **New Profile** window for creating a time range profile is displayed.

Associating a Time Range Profile to ACL

Aruba Central allows you to configure time-based services for specific ACL. To apply a time range profile to an access rule, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. In the **Roles** accordion, click the edit icon listed for access rules under **Access Rules For Selected Roles** to which you want to apply the time range profile.
   The Access Rules page is displayed.
7. In the **Options** section, select the **Time Range** check-box and select the time range profile from the drop-down list.
   - When a time range profile is associated with an ACL, the configured time range is applied on all the WLAN SSID with the specific ACL.
   - If a time range is disabled or if the time range profile is deleted for an ACL, all WLAN SSID with the specific ACL will be able to access the network without any time constraint.
8. Click **Save**.

For more information on time range configuration, see the *Aruba Instant User Guide*.

Configuring ARM and RF Parameters on Instant APs

This section provides the following information:

- ARM Overview
- Configuring ARM Features
- Configuring Radio Parameters

ARM Overview

ARM is a radio frequency management technology that optimizes WLAN performance even in the networks with highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each Instant AP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11a, b, g, n, and ac client types to inter operate at the highest performance levels.

When ARM is enabled, an Instant AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports on WLAN coverage, interference, and intrusion detection to the virtual controller. ARM computes coverage and interference metrics for each valid channel, chooses the best performing channel, and transmit power settings for each Instant AP RF environment. Each Instant AP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

Instant APs support the following ARM features:

- Channel or Power Assignment—Assigns channel and power settings for all the Instant APs in the network according to changes in the RF environment.
- Voice Aware Scanning—Improves voice quality by preventing an Instant AP from scanning for other channels in the RF spectrum during a voice call and by allowing an Instant AP to resume scanning when there are no active voice calls.
- Load Aware Scanning—Dynamically adjusts the scanning behavior to maintain uninterrupted data transfer on resource intensive systems when the network traffic exceeds a predefined threshold.
- Band Steering—Assigns the dual-band capable clients to the 5 GHz band on dual-band Instant APs thereby reducing co-channel interference and increasing the available bandwidth for dual-band clients.
- Client Match—Continually monitors the RF neighborhood of the client to support the ongoing band steering and load balancing of channels, and enhanced Instant AP reassignment for roaming mobile clients.

When Client Match is enabled on 802.11n capable Instant APs, the Client Match feature overrides any settings configured for the legacy band steering, station hand-off assist or load balancing features. The 802.11ac capable Instant APs do not support the legacy band steering, station hand off or load balancing settings, so these Instant APs must be managed using Client Match.

- Airtime Fairness—Provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system to deliver uniform performance to all clients.

For more information on ARM features supported by the APs, see the *Aruba Instant User Guide*.

Spectrum Scan Overview

Wireless networks operate in environments with electrical and RF devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference.

The spectrum monitor (SM) software modules on Instant Access Points (IAPs) can examine the RF environment in which the Wi-Fi network is operating, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues associated with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel. SMs are IAP radios that gather spectrum data but do not service clients. Each SM scans and analyzes the spectrum band used by the SMs radio (2.4 GHz or 5 GHz).

The recorded spectrum is not reported to the virtual controller. A spectrum alert is sent to the virtual controller when a non-Wi-Fi interference device is detected.

For more information on the Spectrum tab, see Access Point > Overview > Spectrum.

In Aruba Central, the Spectrum Scan feature is available only on IAP devices running Aruba Instant firmware version 8.5.0.1 and later.

Configuring ARM Features

To configure the ARM features, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.

3. Click the **Config** icon.

   The tabs to configure the APs are displayed.
4. Click the **Radios** tab.

   The Radios details page is displayed.
5. Under **RF** > **Adaptive Radio Management (ARM)**, the **Client Control** section displays the following components:
   - **Band Steering Mode**
   - **Airtime Fairness Mode**
   - **ClientMatch**
   - **ClientMatch Calculating Interval**
   - **ClientMatch Neighbor Matching**
   - **ClientMatch Threshold**
   - **ClientMatch Key**
   - **Spectrum Load Balancing Mode**

a. For **Band Steering Mode**, configure the following parameters:

Table 144: *Band Steering Mode Configuration Parameters*

Data pane item	Description
Prefer 5 GHz	Enables band steering in the 5 GHz mode. On selecting this, the Instant AP steers the client to the 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Enforces 5 GHz band steering mode on the Instant APs.
Balance Bands	Allows the Instant AP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.5 GHz band operates in 20 MHz.
Disable	Allows the clients to select the band to use.

b. For **Airtime Fairness Mode**, specify any of the following values:

Table 145: *Airtime Fairness Mode Configuration Parameters*

Data Pane Item	Description
Default Access	Allows access based on client requests. When **Airtime Fairness Mode** is set to **Default Access** option, per user and per SSID bandwidth limits are not enforced.
Fair Access	Allocates air time evenly across all the clients.
Preferred Access	Sets a preference where 802.11n clients are assigned more air time than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1.

c. For **ClientMatch**, configure the following parameters:

Table 146: *Client Match Configuration Parameters*

Data Pane Item	Description
Client Match	Turn on the toggle switch to enable the **Client Match** feature on APs. When enabled, client count is balanced among all the channels in the same band. When **Client Match** is enabled, ensure that the **Scanning** option is enabled. For more information, see AP Control Configuration Parameters. **NOTE:** When **Client Match** is disabled, channels can be changed even when the clients are active on a BSSID. The **Client Match** option is disabled by

Data Pane Item	Description
	default.
ClientMatch Calculating Interval	Configures a value for the calculating interval of **Client Match**. The interval is specified in seconds and the default value is 3 seconds. You can specify a value within the range of 10-600.
ClientMatch Neighbor Matching	Configures the calculating interval of **Client Match**. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of **Client Match**. You can specify a percentage value within the range of 20-100. The default value is 60%.
ClientMatch Threshold	Configures a **Client Match** threshold value. This number takes acceptance client count difference among all the channels of **Client Match**. When the client load on an AP reaches or exceeds the threshold in comparison, **Client Match** is enabled on that AP. You can specify a value within range of 1-20. The default value is 5.
ClientMatch Key	Enables the **Client Match** feature to work across different standalone Instant APs in the same management VLAN. All such standalone Instant APs must be set with the same **Client Match** key. **Client Match** uses the wired layer 2 protocol to synchronize information exchanged between Instant APs. Users have an option to configure the **Client Match** keys. Instant APs verify if the frames that they broadcast contain a common **Client Match** key. Instant APs that receive these frames verify if the sender belongs to the same network or if the sender and receiver both have the same **Client Match** key. You can specify a value within the range of 1– 2147483646.
Spectrum Load Balancing Mode	Enables the **Spectrum Load Balancing** mode to determine the balancing strategy for **Client Match**. The following options are available: ▪ **Channel** ▪ **Radio** ▪ **Channel + Radio**

6. Click **Access Point Control**, and configure the following parameters:

Table 147: *AP Control Configuration Parameters*

Data pane item	Description
Customize Valid Channels	Allows you to select a custom list of valid 20 MHz and 40 MHz channels for 2.4 GHz and 5 GHz bands. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting **Customize Valid Channels**, a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. The valid channels automatically show in the **Static Channel Assignment** pane.
Min Transmit Power	Allows you to configure a minimum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm.
Max Transmit Power	Allows you to configure the maximum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the local regulatory requirements or AP model, the value is reduced to the highest supported power settings.
Client Aware	Allows ARM to control channel assignments for the Instant APs with active clients. When the **Client Match** mode is disabled, an Instant AP may change to a more optimal channel, which disrupts current client traffic. The **Client Aware** option is enabled by default.
Scanning	Allows the Instant AP to dynamically scan all 802.11 channels within its 802.11 regulatory domain at regular intervals. This scanning report includes WLAN coverage, interference, and intrusion detection data. **NOTE:** For **Client Match** configuration, ensure that **Scanning** is enabled.
Wide Channel Bands	Allows the administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. For high performance, you can select 5 GHz. If the AP density is low, enable in the 2.4 GHz band.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5 GHz radios, which support a very high throughput. This setting is enabled by default. **NOTE:** Only the APs that support 802.11ac can be configured with 80 MHz channels.

7. Click **Channel Control**, and configure the following parameters:

Table 148: *Channel Control Configuration Parameters*

Data pane item	Description
Backoff Time	Allows you to configure the time within a range of 10 to 3600 seconds, when an Instant AP backs off after requesting a new channel or power. It can increase the time window of channel interference check, and the time window of power check. The default value for minimum back off time is 240 seconds.
Free Channel Index	Allows you to check the difference in threshold in the channel interference index between the new channel and the existing channel. An Instant AP only moves to a new channel if the new channel has a lower interference index value than the current channel. This parameter specifies the required difference between the two interference index values before the Instant AP moves to the new channel. The lower this value, the more likely the Instant AP moves to the new channel. It has a default value of 25.
Ideal Coverage Index	Allows you to specify the ideal coverage index in the range of 2 to 20, which an Instant AP tries to achieve on its channel. The denser the Instant AP deployment, the lower this value should be. It has a default value of 10.
Channel Quality Aware Arm Disable	Allows ARM to ignore the internally calculated channel quality metric and initiates channel changes based on thresholds defined in the profile. ARM chooses the channel based on the calculated interference index value. The option **Channel Quality Aware Arm Disable** is disabled by default.
Channel Quality Threshold	Allows you to specify the channel quality percentage within a range of 0 to 100, below which ARM initiates a channel change. It has a default value of 70%.
Channel Quality Wait Time	Specifies the time that the channel quality is below the channel quality threshold value to initiate a channel change. It has a range of 1 to 3600 seconds, with a default value of 120 seconds. **NOTE:** If current channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.

8. Click **Error Rate**, and configure the following parameters:

Table 149: *Error Rate Configuration Parameters*

Data Pane Item	Description
Error Rate Threshold	Configures the minimum percentage of errors in the channel that triggers a channel change. It has a range of 0 to 100 % with a default value of 70%.
Error Rate Wait Time	Configures the time that the error rate has to be at least equal to the error rate threshold to trigger a channel change. The error rate must be equal to or more than the error rate threshold to trigger a channel change. It has a range of 1 to 3600 seconds, with a default value of 90 seconds.

9. Click **Save Settings**.

Configuring Radio Parameters

To configure RF parameters for the 2.4 GHz and 5 GHz radio bands on an Instant AP, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **Radios** tab.
   The Radios details page is displayed.
5. Expand the **Radio** accordion in the **RF** dashboard.

6. Under **2.4 GHz band**, **5 GHz band**, or both, click the **+** sign to configure the following parameters:

Table 150: *Radio Configuration Parameters*

Data Pane Item	Description
Zone	Allows you to configure a zone per radio band for Instant APs in a cluster. You can also configure an RF zone per Instant AP. **NOTE:** Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors.
Legacy Only	Turn on the **Legacy Only** toggle switch. When enabled, the Instant AP runs the radio in the non-802.11n mode. This option is disabled by default.
802.11d / 802.11h	Turn on the **802.11d / 802.11h** toggle switch. When enabled, the radios advertise their 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is disabled by default.
Beacon Interval	Configures the beacon period for the Instant AP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. You can specify a value within the range of 60–500. The default value is 100 milliseconds.
Interference Immunity Level	Configures the immunity level to improve performance in high-interference environments. The default immunity level is 2. ▪ **Level 0**—No ANI adaptation. ▪ **Level 1**—Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ▪ **Level 2**—Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ▪ **Level 3**—Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ▪ **Level 4**—Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ▪ **Level 5**—The AP completely disables PHY error reporting, improving performance by eliminating the time the Instant AP spends on PHY processing. **NOTE:** Increasing the immunity level makes the AP lose a small amount of range.
Channel Switch Announcement Count	Configures the number of channel switching announcements to be sent before switching to a new channel. This allows the associated clients to recover gracefully from a channel change.

Table 150: *Radio Configuration Parameters*

Data Pane Item	Description
Background Spectrum Monitoring	Turn on the **Background Spectrum Monitoring** toggle switch. When enabled, the APs in the access mode continue with their normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving the clients.
Customize ARM Power Range	Configures a minimum (Min Power) and maximum (Max Power) power range value for the 2.4 GHz and 5 GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration.
Enable 11ac	Turn on the **Enable 11ac** toggle switch. When enabled, VHT is enabled on the 802.11ac devices for the 5 GHz radio band. If VHT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs. **NOTE:** If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear this check box to disable VHT on these devices.
Smart antenna	Turn on the **Smart antenna** toggle switch to combine an antenna array with a digital signal-processing capability to transmit and receive in an adaptive, spatially sensitive manner.
ARM/WIDS Override	When **ARM/WIDS Override** is disabled, the Instant AP will always process frames for WIDS. WIDS is an application that detects the attacks on a wireless network or wireless system. purposes even when it is heavily loaded with client traffic. When **ARM/WIDS Override** is enabled, the Instant AP will stop processing frames for WIDS.

7. Click **Save Settings**.

Configuring IDS Parameters on APs

Aruba Central supports the IDS feature that monitors the network for the presence of unauthorized APs and clients. It also logs information about the unauthorized APs and clients, and generates reports based on the logged information. The IDS feature is available under the Foundation license.

Rogue APs

The IDS feature in the Aruba Central network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations. A rogue AP is an unauthorized AP plugged into the wired side of the network. An interfering AP is an AP seen in the RF environment, but it is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

The built-in IDS scans for APs that are not controlled by the VC. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Configuring Wireless Intrusion Detection and Protection Policies

To configure a Wireless Intrusion Detection and Protection policy:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details page is displayed.
6. Click the **Wireless IDS/IPS** accordingly.
   The following three sections are displayed:
   - **Detection**
   - **Protection**
   - **Firewall Settings**

   You can configure the following options in the above mentioned sections:
   - **Infrastructure Detection Policies**—Specifies the policy for detecting wireless attacks on APs.
   - **Client Detection Policies**—Specifies the policy for detecting wireless attacks on clients.
   - **Infrastructure Protection Policies**—Specifies the policy for protecting APs from wireless attacks.
   - **Client Protection Policies**—Specifies the policy for protecting clients from wireless attacks.
   - **Firewall Policies**—Specifies the policies to set a firewall for a secured network access.
   - **Containment Methods**—Prevents unauthorized stations from connecting to your Aruba Central network.

     Each of these options contains several default levels that enable different sets of policies. An administrator can customize enable or disable these options accordingly.

Detection

The detection levels can be configured using the **Detection** section. The following levels of detection can be configured in the WIP Detection page:

- **High**
- **Medium**
- **Low**
- **Off**
- **Custom**

The following table describes the detection policies enabled in the Infrastructure Detection field.

Table 151: *Infrastructure Detection Policies*

Detection level	Detection policy
Off	All detection policies are disabled.
Low	▪ **Detect Windows Bridge** ▪ **Signature Deassociation Broadcast** ▪ **Signature Deauthentication Broadcast** ▪ **Detect AP Spoofing**

Table 151: *Infrastructure Detection Policies*

Detection level	Detection policy
Medium	▪ **Detect Windows Bridge** ▪ **Signature Deassociation Broadcast** ▪ **Signature Deauthentication Broadcast** ▪ **Detect AP Spoofing** ▪ **Detect adhoc using VALID SSID** ▪ **Detect malformed large duration**
High	▪ **Detect Windows Bridge** ▪ **Signature Deassociation Broadcast** ▪ **Signature Deauthentication Broadcast** ▪ **Detect AP Spoofing** ▪ **Detect adhoc using VALID SSID** ▪ **Detect malformed large duration** ▪ **Detect Overflow EAPOL key** ▪ **Detect Invalid Address Combination** ▪ **Detect AP Impersonation** ▪ **Detect AP Flood** ▪ **Detect Beacon Wrong Channel** ▪ **Detect ht Greenfield** ▪ **Detect Overflow IE** ▪ **Detect RTS Rate Anomaly** ▪ **Detect Malformed HT IE** ▪ **Detect CTS Rate Anomaly** ▪ **Detect Malformed Frame Auth**. ▪ **Detect devices with invalid MAC OUI** ▪ **Detect Malformed Association Request** ▪ **Detect Bad WEP** ▪ **Detect Wireless Bridge** ▪ **Detect HT 40 MHz intolerance** ▪ **Detect Valid SSID Misuse** ▪ **Detect Adhoc Network** ▪ **Detect Client Flood**
Custom	Allows you to select custom detection policies. To select, click the check box of respective detection policy.

The following table describes the detection policies enabled in the Client Detection field.

Table 152: *Client Detection Policies*

Detection level	Detection policy
Off	All detection policies are disabled.
Low	**Detect Valid Station Misassociation**

Detection level	Detection policy
Medium	▪ **Detect Valid Station Misassociation** ▪ **Detect Hotspotter Attack** ▪ **Detect Power Save DOS Attack** ▪ **Detect Omerta Attack** ▪ **Detect Disconnect Station** ▪ **Detect unencrypted Valid** ▪ **Detect Block ACK Attack** ▪ **Detect FATA-Jack**
High	▪ **Detect Valid Station Mis-association** ▪ **Detect Hotspotter Attack** ▪ **Detect Power Save DOS Attack** ▪ **Detect Omerta Attack** ▪ **Detect Disconnect Station** ▪ **Detect unencrypted Valid** ▪ **Detect Block ACK Attack** ▪ **Detect FATA-Jack** ▪ **Detect Rate Anomaly** ▪ **Detect Chop Chop Attack** ▪ **Detect EAP Rate Anomaly** ▪ **Detect TKIP Replay Attack** ▪ **Signature — Air Jack** ▪ **Signature — ASLEAP**
Custom	Allows you to select custom detection policies. To select, click the check box of respective detection policy.

Protection

The following levels of detection can be configured in the WIP Protection page:

- **Off**
- **Low**
- **High**
- **Custom**

The following table describes the protection policies that are enabled in the Infrastructure Protection field.

Table 153: *Infrastructure Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	▪ **Protect SSID** ▪ **Rogue Containment**
High	▪ **Protect SSID**

Protection level	Protection policy
	▪ **Rogue Containment** ▪ **Protect AP Impersonation** ▪ **Protect from Adhoc Networks**
Custom	Allows you to select custom detection policies. To select, click the check box of respective protection policy.

The following table describes the detection policies that are enabled in the Client Protection field.

Table 154: *Client Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	**Protect Valid Station**
High	▪ **Protect Valid Station** ▪ **Protect Windows Bridge**
Custom	Allows you to select custom detection policies. To select, click the check box of respective protection policy.

Containment Methods

You can enable wired and wireless containment measures to prevent unauthorized stations from connecting to your Aruba Central network.

Aruba Central supports the following types of containment mechanisms:

- **Wired containment**—When enabled, APs generate ARP packets on the wired network to contain wireless attacks.
- **Wireless containment**—When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified AP.
  - **None** —Disables all the containment mechanisms.
  - **Deauthenticate only**—With deauthentication containment, the AP or client is contained by disrupting the client association on the wireless interface.
  - **Tarpit containment**—With tarpit containment, the AP is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the AP being contained.
  - **Tarpit all stations**

The FCC and some third parties have alleged that under certain circumstances, the use of containment functionality violates 47 U.S.C. §333. Before using any containment functionality, ensure that your intended use is allowed under the applicable rules, regulations, and policies. Aruba is not liable for any claims, sanctions, or other direct, indirect, special, consequential or incidental damages related to your use of containment functionality.

Protection Against Wired Attacks

In the **Protection Against Wired Attacks** section, enable the following options:

- **Drop Bad ARP**—Drops the fake ARP packets.
- **Fix Malformed DHCP**—Fixes the malformed DHCP packets.
- **ARP Poison Check**—Triggers an alert on ARP poisoning caused by the rogue APs.

Firewall Settings

To configure firewall settings by specifying the policies for a secured network access, see Configuring Firewall Parameters for Wireless Network Protection.

- For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.
- Management access to the Instant AP is allowed irrespective of the inbound firewall rule.
- The inbound firewall is not applied to traffic coming through the GRE tunnel.

Configuring Authentication and Security Profiles on Instant APs

This section describes the authentication and security parameters to configure on an Instant AP:

- Supported Authentication Methods
- Authentication Servers for Instant APs
- Denylisting Instant AP Clients
- Configuring Network Service ACLs
- Enabling ALG Protocols on Instant APs
- Configuring External Authentication Servers for APs
- Configuring Role Derivation Rules for AP Clients
- Configuring Firewall Parameters for Wireless Network Protection
- Configuring Intra VLAN Traffic Allowlist
- Configuring an MPSK Local Profile
- Configuring User Roles for AP Clients
- Configuring Firewall Parameters for Inbound Traffic
- Configuring Roles and Policies on Instant APs for User Access Control
- Support for Multiple PSK in WLAN SSID
- Configuring WPA3 Encryption
- Configuring Users Accounts for the Instant AP Management Interface
- Configuring Guest and Employee User Profiles on Instant APs

Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password. Clients can also be authenticated based on their MAC addresses.

The authentication methods supported by the Instant APs managed through Aruba Central are described in the following sections.

802.1X Authentication

802.1X is a method for authenticating the identity of a user before providing network access to the user. The Aruba Central network supports internal RADIUS server and external RADIUS server for 802.1X authentication. For authentication purpose, the wireless client can associate to a NAS or RADIUS client such as a wireless Instant AP. The wireless client can pass data traffic only after successful 802.1X authentication.

The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for a Network Profile

To configure 802.1X authentication for a wireless network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile for which you want to enable 802.1X authentication, and then click the edit icon.

You can directly edit the SSID name under the **Display Name** column in the **Wireless SSIDs** table. Double-click the relevant SSID that you want to rename, and type the new name. Press Enter to complete the process.

6. Under **Security**, for the **Enterprise** security level, select the preferred option from **Key Management**.
7. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, set **Termination** to **Enabled**.
   For 802.1X authorization, by default, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the Instant AP itself acts as an authentication server, terminates the outer layers of the EAP protocol, and only relays the innermost layer to the external RADIUS server.
8. Specify the type of authentication server to use.
9. Click **Save Settings**.

MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings.

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication.

Configuring MAC Authentication for a Network Profile

To configure MAC authentication for a wireless profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **WLANs** tab, select a network profile for which you want to enable MAC authentication and then click the edit icon.
6. In **Security**, turn on the **MAC Authentication** toggle switch to enable **Personal** or **Open** security level.
7. Specify the type of authentication server to use.
8. Click **Save Settings**.

MAC Authentication with 802.1X Authentication

The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.

You can also configure the following authentication parameters for MAC+802.1X authentication:

- MAC authentication only—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- L2 authentication fall-through—Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

Configuring MAC Authentication with 802.1X Authentication

To configure MAC authentication with 802.1X authentication for wireless network profile, configure the following parameters:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.

3. Click the **Config** icon.

   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.

   The WLANs details page is displayed.
5. In the **WLANs** tab, select a network profile for which you want to enable MAC and 802.1X authentication and click the edit icon.
6. Turn on the **Perform MAC Authentication Before 802.1X** toggle switch to use 802.1X authentication only when the MAC authentication is successful.
7. Turn on the **MAC Authentication Fail Through** toggle switch to use 802.1X authentication even when the MAC authentication fails.
8. Click **Save Settings**.

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information, see Configuring Wireless Networks for Guest Users on Instant APs.

MAC Authentication with Captive Portal Authentication

The following conditions apply to a network profile with MAC authentication and Captive Portal authentication enabled:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **None**, MAC authentication is disabled.

The MAC authentication with captive portal authentication supports the **mac-auth-only** role.

Configuring MAC Authentication with Captive Portal Authentication

To configure the MAC authentication with captive portal authentication for a network profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.

   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.

   The WLANs details page is displayed.
5. In the **WLANs** tab, select an existing wireless profile for which you want to enable MAC authentication with captive portal authentication, and then click the edit icon.
6. Under **Access**, specify the following parameters for a network with **Role Based** rules:
   - Turn on the **Enforce Machine Authentication** toggle switch, when MAC authentication is enabled for captive portal. If the MAC authentication fails, the captive portal authentication role is assigned to the client.

- Turn on the **Enforce MAC Auth Only Role** toggle switch, when MAC authentication is enabled for captive portal. After successful MAC authentication, the **MAC Auth Only** role is assigned to the client.

7. Click **Next**.

802.1X Authentication with Captive Portal Authentication

This authentication method allows you to configure different captive portal settings for clients on the same SSID. For example, you can configure an 802.1X SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal Captive portal, or none.

For more information on configuring captive portal roles for an SSID with 802.1X authentication, see Configuring Wireless Networks for Guest Users on Instant APs.

WISPr Authentication

WISPr authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an ISP with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISPs WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot own ISP as per their service agreements. The Instant AP assigns the default WISPr user role to the client when your ISP sends an authentication message to the Instant AP.

Instant APs support the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the Instant AP.

Configuring WISPr Authentication

To configure WISPr authentication, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **WISPr** accordion.

7. Under **WISPr**, configure the following parameters:
   a. **ISO Country Code**—The ISO Country Code for the WISPr Location ID.
   b. **E.164 Area Code**—The E.164 Area Code for the WISPr Location ID.
   c. **Operator Name**—The operator name of the hotspot.
   d. **E.164 Country Code**—The E.164 Country Code for the WISPr Location ID.
   e. **SSID/Zone**—The SSID/Zone for the WISPr Location ID.
   f. **Location Name**—Name of the hotspot location. If no name is defined, the name of the Instant AP, to which the user is associated, is used.
8. Click **Save Settings**.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and http://www.itu.int).

A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the RADIUS server profile for the WISPr server.

Walled Garden

On the Internet, a walled garden typically controls access to web content and services. The Walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the allowlist of the walled garden profile, the user is redirected to the login page. Instant AP supports Walled Garden only for the HTTP requests. For example, if you add yahoo.com in Walled Garden allowlist and the client sends an HTTPS request (https://yahoo.com), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a denylisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

Configuring Walled Garden Access

To configure walled garden access, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Walled Garden** accordion.

7. To allow access to a specific set of websites, click **+** under **Allowlist**, enter the domain name in the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:
   - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
   - www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
   - favicon.ico allows access to /favicon.ico from all domains.
8. To deny users access to a domain, click **+** under **Denylist**, and enter the domain name in the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the denylist is accessed by an unauthenticated user, Instant AP sends an HTTP 403 response to the client with an error message.
9. Click **Save Settings**.

Authentication Servers for Instant APs

Based on the security requirements, you can configure internal or external RADIUS servers. This section describes the types of authentication servers and authentication termination, that can be configured for a network profile.

External RADIUS Server

In the external RADIUS server, the IP address of the VC is configured as the NAS IP address. Aruba Central RADIUS is implemented on the VC, and this eliminates the need to configure multiple NAS clients for every Instant AP on the RADIUS server for client authentication. Aruba Central RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and users are allowed or denied access to the network depending on the response from the RADIUS server.

When you enable an external RADIUS server for the network, the client on the Instant AP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Aruba Central supports the following external authentication servers:

- RADIUS
- LDAP

To use an LDAP server for user authentication, configure the LDAP server on the VC, and configure user IDs and passwords.

To use a RADIUS server for user authentication, configure the RADIUS server on the VC.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the Instant AP the VSA that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

Internal RADIUS Server

Each Instant AP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the Instant AP sends a RADIUS packet to the local IP address. The internal RADIUS server listens and replies to the RADIUS packet.

The following authentication methods are supported in the Aruba Central network:

- **EAP-TLS**—The EAP-TLS method supports the termination of EAP-TLS security using the internal RADIUS server. The EAP-TLS requires both server and CA certificates installed on the Instant AP. The client certificate is verified on the virtual controller (the client certificate must be signed by a known CA), before the username is verified on the authentication server.
- **EAP-TTLS (MSCHAPv2)**—The EAP-TTLS method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- **EAP-PEAP (MSCHAPv2)**—EAP-PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- **LEAP**—LEAP uses dynamic WEP keys for authentication between the client and authentication server.

To use the internal database of an AP for user authentication, add the names and passwords of the users to be authenticated.

Aruba does not recommend the use of LEAP authentication because it does not provide any resistance to network attacks.

RADIUS Communication over TLS (RadSec)

RADIUS over TLS, also known as RadSec, is a RADIUS protocol that uses TLS protocol for end-to-end secure communication between the RADIUS server and Instant AP. RadSec wraps the entire RADIUS packet payload into a TLS stream. Enabling RadSec increases the level of security for authentication that is carried out across the cloud network. When configured, this feature ensures that the RadSec protocol is used for safely transmitting the authentication and accounting data between the Instant AP and the RadSec server.

The following conditions applies to RadSec configuration:

- The RADIUS packets go through the tunnel when TLS tunnel is established.
- By default, the TCP port 2083 is assigned for RadSec. Separate ports are not used for authentication, accounting, and dynamic authorization changes.
- Aruba Central supports dynamic CoA (RFC 3576) over RadSec and the RADIUS server uses an existing TLS connection opened by the Instant AP to send the request.
- By default, the Instant AP uses its device certificate to establish a TLS connection with RadSec server. You can also upload your custom certificates on to Instant AP. For more information on uploading certificates, see Certificates.

Authentication Termination on Instant AP

Aruba Central allows EAP termination for PEAP-Generic Token Card (PEAP-GTC) and Protected Extensible Authentication Protocol-Microsoft Challenge Authentication Protocol version 2 (PEAP-MSCHAPv2). PEAP-GTC termination allows authorization against an LDAP server and external RADIUS server while PEAP-MSCHAPv2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- **EAP-GTC**—This EAP method permits the transfer of unencrypted usernames and passwords from client to server. The EAP-GTC is mainly used for one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the Instant AP to an external authentication server for user data backup.

- **EAP-MSCHAPv2**—This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

Dynamic Load Balancing between Authentication Servers

You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the Instant APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in Instant AP is performed based on the outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across asymmetric capacity RADIUS servers without the need to obtain inputs about the server capabilities from the administrators.

Configuring External Authentication Servers for APs

You can configure an external RADIUS server, TACACS, and LDAP server for user authentication. You can configure guest network using External Captive Portal profile for external authentication.

To configure a server, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. In the **Authentication Server** panel, click **+** to create a new server.
7. Select any of the following server types and configure the parameters for your deployment scenario.

Table 155: *Authentication Server Configuration*

Type of Server	Parameters
RADIUS	
Name	Name of the external RADIUS server.
IP Address	IP address or the FQDN of the external RADIUS server.
Radsec	Set **Radsec** to **Enabled** to enable secure communication between the RADIUS server and Instant AP by creating a TLS tunnel between the Instant AP and the server. If **Radsec** is enabled, the following configuration options are displayed: **Radsec Port**—Communication port number for RadSec TLS connection. By default, the port number is set to 2083. ■ NAS Identifier ■ NAS IP Address

Type of Server	Parameters
	■ Service Type Framed User ■ Query Status of RADIUS Servers (RFC 5997) ■ Dynamic Authorization
Auth Port	Authorization port number of the external RADIUS server. The default port number is 1812.
Accounting Port	The accounting port number used for sending accounting records to the RADIUS server. The default port number is 1813.
Shared Key and Retype Shared Key	Shared key for communicating with the external RADIUS server.
Timeout	The timeout duration for one RADIUS request. The Instant AP retries sending the request several times (as configured in the **Retry count**) before the user is disconnected. For example, if the **Timeout** is 5 seconds, **Retry counter** is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
Retry Count	The maximum number of authentication requests that can be sent to the server group by the Instant AP. You can specify a value within the range of 1–5. The default value is 3 requests.
Dynamic Authorization	To allow the APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, select this check box. Disconnect messages terminate the user session immediately, whereas the CoA messages modify session authorization attributes such as data filters. When you enable the **Dynamic Authorization** option, the **AirGroup CoA Port** field is displayed with the port number for sending Bonjour support CoA on a different port than on the standard CoA port. The default value is 5999.
NAS IP Address	Enter the IP address. ■ For Instant AP based cluster deployments, ensure that you enter the VC IP address as the NAS IP address.
NAS Identifier	Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
Dead Time (in mins)	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the Instant AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server is available if the server is marked as unavailable. If Dynamic RADIUS Proxy (DRP) is enabled on the APs, configure the following parameters: ■ **DRP IP**—IP address to be used as source IP for RADIUS packets. ■ **DRP MASK**—Subnet mask of the DRP IP address. ■ **DRP VLAN**—VLAN in which the RADIUS packets are sent. ■ **DRP GATEWAY**—Gateway IP address of the DRP VLAN.

Type of Server	Parameters
Service Type Framed User	Select any of the following check boxes to send the service type as **Framed User** in the access requests to the RADIUS server: ■ **802.1X**—Changes the service type to frame for 802.1X authentication. ■ **MAC**—Changes the service type to frame for MAC authentication. ■ **Captive Portal**—Changes the service type to frame for Captive Portal authentication.
Query Status of RADIUS Servers (RFC 5997)	Select any of the following check boxes to detect the server status of the RADIUS server: ■ **Authentication**—Select this check-box to ensure the Instant AP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. ■ **Accounting**—Select this check-box to ensure the Instant AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.
LDAP	
Name	Name of the LDAP server.
IP Address	IP address of the LDAP server.
Auth Port	Authorization port number of the LDAP server. The default port number is 389.
Admin-DN	A distinguished name for the admin user with read and search privileges across all the entries in the LDAP database (the admin user need not have write privileges, but the admin user must be able to search the database, and read attributes of other users in the database).
Admin Password and Retype Admin Password	Password for the admin user.
Base-DN	Distinguished name for the node that contains the entire user database.
Filter	The filter to apply when searching for a user in the LDAP database. The default filter string is **(objectclass=*)**.
Key Attribute	The attribute to use as a key while searching for the LDAP server. For Active Directory, the value is **sAMAccountName**.
Timeout	Timeout interval within a range of 1–30 seconds for one RADIUS request. The default value is 5.
Retry Count	The maximum number of authentication requests that can be sent to the server group. You can specify a value within the range of 1–5. The default value is 3.

Type of Server	Parameters
TACACS	
Name	Name of the server.
Shared Key and Retype Key	The secret key to authenticate communication between the TACACS client and server.
Auth Port	The TCP IP port used by the server. The default port number is 49.
Timeout	A number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds.
IP Address	IP address of the server.
Retry Count	The maximum number of authentication attempts to be allowed. The default value is 3.
Dead Time (in mins)	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server is available if the server is marked as unavailable.
Session Authorization	Enable this option to allow the authorization of sessions.
External Captive Portal—The external captive portal servers are used for authenticating guest users in a WLAN.	
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: ■ **Radius Authentication**—Select this option to enable user authentication against a RADIUS server. ■ **Authentication Text**—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or Hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL of the external captive portal server.
Port	Enter the port number that is used for communicating with the external captive portal server.
Use HTTPS	Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected.

Type of Server	Parameters
Captive Portal Failure	This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select **Deny Internet** to prevent guest users from using the network, or **Allow Internet** to access the network.
Server Offload	Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server.
Prevent Frame Overlay	Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
Automatic URL Allowlisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically allowlisted.
Auth Text	If the **External Authentication splash** page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.
Dynamic Authorization Only	
Name	Name of the server.
IP Address	IP address of the server.
AirGroup CoA Port	A port number for sending Bonjour support CoA on a different port than on the standard CoA port. The default value is 5999.
Shared Key and Retype Key	A shared key for communicating with the external RADIUS server. Change of Authorization(CoA) is a subset of Dynamic Authorization include disconnecting messages.

8. Click **Save**.

To assign the authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

You can also add an external RADIUS server when configuring a WLAN SSID profile.

Configuring Users Accounts for the Instant AP Management Interface

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an Instant AP. The authentication servers determine if the user has access to management interface. The privilege level for different types of management users is defined on the RADIUS or TACACS server. The Instant APs map the management users to the corresponding privilege level and provide access to the users based on the attributes returned by the RADIUS or TACACS server.

In Aruba Central, the Instant AP management user passwords are stored and displayed as hash instead of plain text. The **hash-mgmt-user** command is enabled by default on the Instant APs provisioned in the template and UI groups. If a pre-configured Instant AP joins Aruba Central and is moved to a new group, Aruba Central uses the **hash-mgmt-user** configuration settings and discards **mgmt-user** configuration settings, if any, on the Instant AP. In other words, Aruba Central hashes management user passwords irrespective of the management user configuration settings running on an Instant AP.

To configure authentication parameters for local admin, read-only, and guest management administrator account settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.

6. Expand the **Administrator** accordion and configure the following parameters:

Table 156: *Configuration Parameters for the Instant AP Users*

Type of the User	Authentication Options	Steps to Follow
Client Control	**Internal**	In the **Authentication** drop-down list, select **Internal** if you want to specify a single set of user credentials. If using an internal authentication server: 1. In **Username** and **Password**, enter a username and password. 2. In **Retype Password**, retype the password to confirm.
	Authentication Server	In the **Authentication** drop-down list, select the RADIUS or TACACS authentication servers. You can also create a new server by selecting **New** from the **Authentication server** drop-down list.
	Authentication Server with fallback to Internal	In the **Authentication** drop-down list, select **Authentication server w/ fallback to internal** option if you want to use both internal and external servers. When enabled, the authentication switches to **Internal** if there is no response from the RADIUS server (RADIUS server timeout). To use this option, select the authentication servers and configure the user credentials for internal server based authentication. 1. In **Username** and **Password**, enter a username and password. 2. In **Retype Password**, retype the password to confirm.
	Load Balancing	If two servers are configured, the users can use them in the primary or backup mode, or load balancing mode. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list. For more information on load balancing, see Authentication Servers for Instant APs.
	TACACS Accounting	If a TACACS server is selected, enable TACACS accounting to report management commands, if required.
View Only		To configure a user account with the read-only privileges: 1. In **Username** and **Password**, enter a username and password. 2. In **Retype Password**, retype the password to confirm.
Guest Registration Only		To configure a guest user account with the read-only privileges: 1. In **Username** and **Password**, enter a username and password. 2. In **Retype Password**, retype the password to confirm.

7. Click **Save Settings**.

Support for Multiple PSK in WLAN SSID

Aruba Central allows you to configure multiple PSK (MPSK) in WLAN network profiles that include APs running a minimum of Aruba Instant 8.4.0.0 firmware version and later. MPSK enhances the WPA2 PSK mode by allowing device-specific or group-specific passphrases, which are generated by ClearPass Policy Manager and sent to the Instant AP.

WPA2 PSK-based deployments generally consist of a single passphrase configured as part of the WLAN SSID profile. This single passphrase is applicable for all clients that associate with the SSID. Starting from Aruba

Instant 8.4.0.0, multiple PSKs in conjunction with ClearPass Policy Manager are supported for WPA and WPA2 PSK-based deployments. Every client connected to the WLAN SSID can have its own unique PSK.

A MPSK passphrase requires MAC authentication against a ClearPass Policy Manager server. The MPSK passphrase works only with wpa2-psk-aes encryption and not with any other PSK-based encryption. The Aruba-MPSK-Passphrase radius VSA is added and the ClearPass Policy Manager server populates this VSA with the encrypted passphrase for the device.

The workflow is as follows:

1. A user registers the device on a ClearPass Policy Manager guest-registration or device-registration webpage and receives a device-specific or group-specific passphrase.
2. The device associates with the SSID using wpa2-psk-aes encryption and uses MPSK passphrase.
3. The Instant AP performs MAC authentication of the client against the ClearPass Policy Manager server. On successful MAC authentication, the ClearPass Policy Manager returns Access-Accept with the VSA containing the encrypted passphrase.
4. The Instant AP generates a PSK from the passphrase and performs 4-way key exchange.
5. If the device uses the correct per-device or per-group passphrase, authentication succeeds. If the ClearPass Policy Manager server returns Access-Reject or the client uses incorrect passphrase, authentication fails.
6. The Instant AP stores the MPSK passphrase in its local cache for client roaming. The cache is shared between all the Instant APs within a single cluster. The cache can also be shared with standalone Instant APs in a different cluster provided the APs belong to the same multicast VLAN. Each Instant AP first searches the local cache for the MPSK information. If the local cache has the corresponding MPSK passphrase, the Instant AP skips the MAC authentication procedure, and provides access to the client.

When multiple PSK is enabled on the wireless SSID profile, make sure that MAC authentication is not configured for RADIUS authentication. Multiple PSK and MAC authentication are mutually exclusive and follows a special procedure which does not require enabling MAC authentication in the WLAN SSID manually. Also, ensure that the RADIUS server configured for the wireless SSID profile is not an internal server.

Points to Remember

The following configurations are mutually exclusive with MPSK for the WLAN SSID profile and does not require to be configured manually:

- MPSK and MAC authentication
- MPSK and Denylisting
- MPSK and internal RADIUS server

Configuring Multiple PSK for Wireless Networks

To configure multiple PSK for wireless networks, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.

4. Click **WLANs** tab.

   The WLANs detail page is displayed.
5. Click **+ Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. Click the **Security** tab.
7. Select **Personal** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
8. From the **Key Management** drop-down list, select the **MPSK-AES** option.
9. From the **Primary Server** drop-down list, select a server. The radius server selected from the list is the CPPM server.
10. Click **Save Settings**.

Enabling MPSK Local for Wireless Networks

To configure MPSK Local for wireless networks, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.

   The tabs to configure the APs are displayed.
4. Click **WLANs** tab.

   The WLANs detail page is displayed.
5. Click **+ Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. Click the **Security** tab.
7. Select **Personal** from the **Security Level**.

   The authentication options applicable to the personal network are displayed.
8. From the **Key Management** drop-down list, select the **Mpsk Local** option.
9. From the **Mpsk Local** drop-down list, select an MPSK Local profile.

MPSK Local feature is supported for 8.7.0.0 or later versions. You cannot select an MPSK Local profile from the **Mpsk Local** drop-down list if the AP version is less than 8.7.0.0.

10. Click **Save Settings**.

Configuring an MPSK Local Profile

MPSK Local allows the user to configure 24 PSKs per SSID locally on the device. These local PSKs would serve as an extension of the base MPSK functionality.

To configure an MPSK Local profile, complete the following steps

1. In the **Network Operations** app, set the filter to a group containing at least one AP.

   The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Mpsk Local** accordion.
7. In the **MPSK Local** window, click **+** and enter a name for the MPSK Local profile.
8. To create an MPSK Local passphrase, enter the following information in the **Mpsk Local Passphrase** window:
   a. **Name**—Enter a name.
   b. **Passphrase**—Enter a passphrase.
   c. **Retype Passphrase**—Retype the passphrase to confirm.
9. Click **OK**.
10. In the **Mpsk Local Passphrase** window, select the MPSK Local passphrase name created in the previous step, and then click **OK**.
11. Click **Save Settings**.

Configuring WPA3 Encryption

Aruba Central supports WPA3 encryption for security profiles in SSID creation for networks that include APs running Aruba Instant 8.4.0.0 firmware version and above. The WPA3 security provides robust protection with unique encryption per user session thereby ensuring a highly secured connection even on a public Wi-Fi hotspot.

The following are the WPA3 encryptions based on the **Enterprise**, **Personal**, or **Open** network types:

- **WPA-3 Enterprise** when the security level is **Enterprise**.
- **WPA-3 Personal** when the security level is **Personal**.
- **Enhanced Open** when the security level is **Open**.

WPA3 Enterprise

WPA3-Enterprise enforces top secret security standards for an enterprise Wi-Fi in comparison to secret security standards. Top secret security standards includes:

- Deriving at least 384-bit PMK/MSK using Suite B compatible EAP-TLS.
- Securing pairwise data between STA and authenticator using AES-GCM-256.
- Securing group addressed data between STA and authenticator using AES-GCM-256.
- Securing group addressed management frames using BIP-GMAC-256.

Aruba Instant supports WPA3-Enterprise only in non-termination 802.1X and tunnel-forward modes. WPA3-Enterprise compatible 802.1x authentication occurs between STA and CPPM.

WPA3-Enterprise advertises or negotiates the following capabilities in beacons, probes response, or 802.11 association:

- AKM Suite Selector as 00-0F-AC:12
- Pairwise Cipher Suite Selector as 00-0F-AC:9
- Group data cipher suite selector as 00-0F-AC:9
- Group management cipher suite (MFP) selector as 00-0F-AC:12

If WPA3-Enterprise is enabled, STA is successfully associated only if it uses one of the four suite selectors for AKM selection, pairwise data protection, group data protection, and group management protection. If a STA mismatches any one of the four suite selectors, the STA association fails.

Configuring WPA3 for Wireless Network

To configure WPA3 for enterprise security, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **WLANs** tab.
   The WLANs detail page is displayed.
5. Click **+ Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table, and then click the edit icon.
6. Click the **Security** tab.
7. Select **Enterprise** from the **Security Level**.
   The authentication options applicable to the Enterprise network are displayed.
8. Select one of the following from the **Key Management** drop-down list:
   - **WPA-3 Enterprise(GCM 256)**—Select this option to use WPA-3 security employing GCM encryption operation mode limited to encrypting 256 bits of plain text.
   - **WPA-3 Enterprise(CCM 128)**—Select this option to use WPA-3 security employing CCM encryption operation mode limited to encrypting 128 bits of plain text.
9. Click **Save Settings**.

Configuring WPA3 for Personal Security

To configure WPA3 for personal security, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **WLANs** tab.
   The WLANs detail page is displayed.

5. Click **+ Add SSID** to create a new SSID. To modify an existing SSID, select a wireless SSID from the **Wireless SSIDs** table and then click the edit icon.
6. Click the **Security** tab.
7. Select **Personal** from the **Security Level**.

   The authentication options applicable to the Personal network are displayed.
8. Select **WPA-3 Personal** from the **Key Management** drop-down list.
9. Click **Save Settings**.

Configuring Guest and Employee User Profiles on Instant APs

The local database of an Instant AP consists of a list of guest and employee users. The addition of a user involves specifying a login credentials for a user. The login credentials for these users are provided outside the Aruba Central system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.

The user database is also used when an Instant AP is configured as an internal RADIUS server. The local user database of APs can support up to 512 user entries except IAP-92 and IAP-93. IAP-92 and IAP-93 supports only 256 user entries. If there are already 512 users, IAP-92 and IAP-93 will not be able to join the cluster.

To configure users, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.

   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.

   The Security page is displayed.
6. Click **User For Internal Server**.
7. In the **Users** pane, click the **+** icon.
8. In the **Add User** window, enter the following information, and then click **OK**.
   a. In the **Username** text-box, enter a username.
   b. In the **Password** text-box, enter the password.
   c. In the **Retype** text-box, retype the password to confirm.
   d. In the **Type** drop-down list, select a type of user from the drop-down list.
9. To edit a user settings:

a. In the **Users** pane, select the username to edit.
b. Click the edit icon to modify the user settings.
c. Click **OK**.

10. To delete a user:
    a. In the **Users** pane, select the username to delete.
    b. Click the delete icon.
    c. Click **OK**.
11. To delete all users, select **Delete All** in the **Users** pane, and then click **Yes**.
12. Click **Save Settings**.

Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the username.

Configuring Intra VLAN Traffic Allowlist

The Intra VLAN Traffic Allowlist is a global allowlist for all WLAN SSIDs and wired networks configured with the network. For servers to serve the network, you must add them to the Intra VLAN Traffic Allowlist using their IP or MAC address. When you configure wired servers with their IP address or MAC address, the Instant Access Point allows client traffic to the destination MAC addresses.

Configuring a Wired Server with the IP Address

To configure a wired server with the IP address, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Intra VLAN Traffic Allowlist** accordion.
7. In the **Wired Server IP** window, click **+** and enter the IP address of the server.
8. Click **OK**.
9. Click **Save Settings**.

To edit a wired server, select the IP address of the wired server in the **Wired Server IP** window, and then click the edit icon.

To delete a wired server, select the IP address of the wired server in the **Wired Server IP** window, and then click the delete icon.

Configuring a Wired Server with the MAC Address

To configure a wired server with the MAC address, complete the following steps:

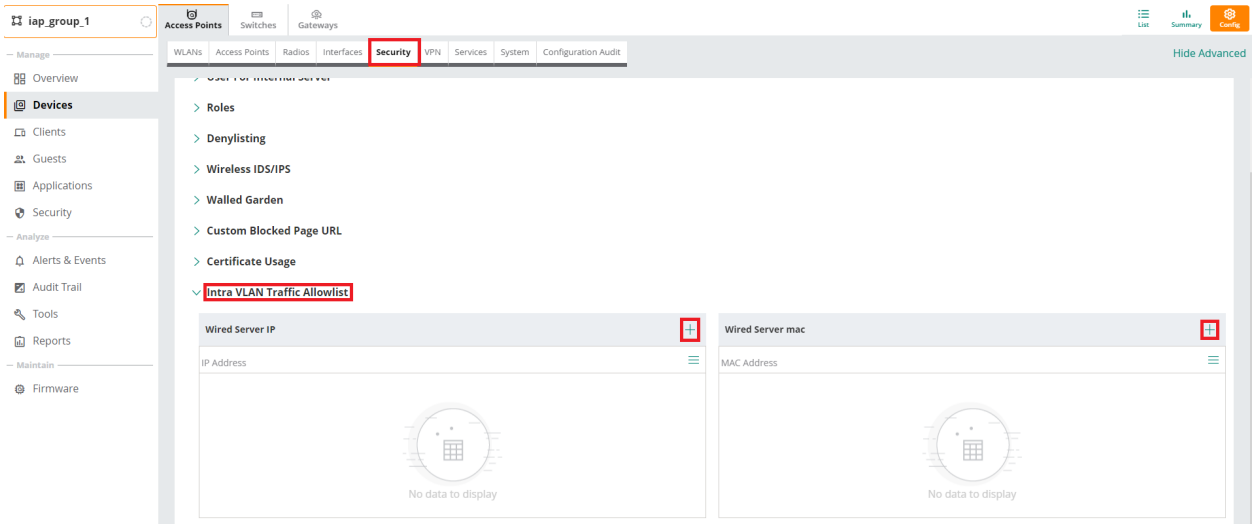
1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Intra VLAN Traffic Allowlist** accordion.
7. In the **Wired Server MAC** window, click **+** and enter the MAC address of the server.
8. Click **OK**.
9. Click **Save Settings**.

To edit a wired server, select the IP address of the wired server in the **Wired Server MAC** window, and then click the edit icon.

To delete a wired server, select the IP address of the wired server in the **Wired Server MAC** window, and then click the delete icon.

The following figure shows the configuration options of a wired server with the IP address or MAC address:

Figure 138 *Intra VLAN Traffic Allowlist Configuration*



Configuring Roles and Policies on Instant APs for User Access Control

Instant APs support identity-based access control to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using the Instant AP firewall policies, you can enforce network access policies to define access to the network, areas of the network that the user may access, and the performance thresholds of various applications.

Instant APs supports a role-based stateful firewall. In other words, Instant firewall can recognize flows in a network and keep track of the state of sessions. The firewall logs on the Instant APs are generated as syslog messages. The firewall feature also supports ALG functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

ACL Rules

You can use ACL rules to either permit or deny data packets passing through the Instant AP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The Instant AP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate. Instant AP supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on source or destination IP address, or source or destination port number.

You can configure up to 64 access control rules for a firewall policy.

Configuring Network Address Translation Rules

NAT is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and private (local network), which allows translation of private network IP addresses to a public address space.

Instant AP supports the NAT mechanism to allow a routing device to use the translation tables to map the private addresses into a single IP address and packets are sent from this address, so that they appear to originate from the routing device. Similarly, if the packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

For more information, see:

- Configuring Network Service ACLs
- Configuring ACLs for Deep Packet Inspection
- Configuring User Roles for AP Clients
- Configuring Role Derivation Rules for AP Clients
- Configuring Firewall Parameters for Inbound Traffic

Configuring Network Service ACLs

To configure access rules for network services, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.

5. Click the **Security** tab.

   The Security page is displayed.
6. Click the **Roles** accordion.
7. Under **Access Rules For Selected Roles**, click **+** to add a new rule.

   The Access Rule window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To configure access to applications or application categories, select a service category from the following list:
   - **Network**
   - **App Category**
   - **Application**
   - **Web Category**
   - **Web Reputation**
10. Based on the selected service category, configure the following parameters:

Table 157: *Access Rule Configuration Parameters*

Data Pane Item	Description
Rule Type	Select a rule type from the list, for example **Access Control**.
Service	Select a service from the list of available services. You can allow or deny access to any or all of the following services based on your requirement: ■ **Any**—Access is allowed or denied to all services. ■ **CUSTOM**—Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the Other option, enter the appropriate ID. **NOTE:** If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.
Action	Select any of following attributes: ■ Select **Allow** to allow access users based on the access rule. ■ Select **Deny** to deny access to users based on the access rule. ■ Select **Destination-NAT** to allow the changes to destination IP address. ■ Select **Source-NAT** to allow changes to the source IP address.
Destination	Select a destination option. You can allow or deny access to any the following destinations based on your requirements. ■ **To all destinations**—Access is allowed or denied to all destinations. ■ **To a particular server**—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ■ **Except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ **To a network**—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network.

Table 157: *Access Rule Configuration Parameters*

Data Pane Item	Description
	■ **Except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ **To a Domain Name**—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box. ■ **To AP IP**—Traffic to the specified Instant AP is allowed. After selecting this option, specify the domain name in the **IP** text box. ■ **To AP Network**—Traffic to the specified Instant AP network is allowed. After selecting this option, specify the domain name in the **IP** text box. ■ **To conductor IP**—Traffic to the specified conductor Instant AP or virtual controller is allowed. After selecting this option, specify the domain name in the **IP** text box.
Log	Select **Log** to create a log entry when this rule is triggered. The Aruba Central firewall supports firewall based logging. Firewall logs on the Instant APs are generated as security logs.
Denylist	Select **Denylist** to denylist the client when this rule is triggered. The denylisting lasts for the duration specified as **Auth failure denylist time** on the **Denylisting** tab of the **Security** window.
Classify Media	Select **Classify Media** to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: ■ Video: Priority 5 (Critical) ■ Voice: Priority 6 (Internetwork Control)
Disable Scanning	Select **Disable Scanning** to disable ARM scanning when this rule is triggered. The selection of the **Disable Scanning** applies only if ARM scanning is enabled.
DSCP TAG	Select **DSCP TAG** to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63.
802.1p priority	Select **802.1p priority** to specify an 802.1 priority. Specify a value between 0 and 7.
Time Range	Select this check-box to allow a specific user to access the network for a specific time range. You can select the time range profile from the drop-down list that appears when the **Time Range** check box is selected.

11. Click **Save Settings**.

Configuring ACLs for Deep Packet Inspection

To configure ACL rules for a user role for Deep Packet Inspection (DPI), complete the following procedure:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.

3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Under **Roles**, select the role for which you want to configure access rules.
7. Under **Access Rules For Selected Roles**, click **+** to add a new rule.
   The Access Rule window is displayed.
8. Under **Rule Type**, select **Access Control.**
9. To configure access to applications or application categories, select a service category from the following list:
   - Network
   - App Category
   - Application
   - Web Category
   - Web Reputation
10. Based on the selected service category, configure the following parameters:

Table 158: *Access Rule Configuration Parameters*

Service category	Description
App Category	Select the application categories to which you want to allow or deny access.
Application	Select the applications to which you want to allow or deny access.
Application Throttling	Application throttling allows you to set a bandwidth limit for an application and application categories. For example, you can limit the bandwidth rate for video streaming applications such as YouTube or Netflix, or assign a low bandwidth to high risk sites. To specify a bandwidth limit: a. Select the **Application Throttling** check box. b. Specify the **Downstream** and **Upstream** rates in Kbps per user.
Action	Select one of the following actions: ■ **Destination-NAT**—Translation of the destination IP address of a packet entering the network. ■ **Source-NAT**—Used by internal users to access the internet. ■ **Allow**—Select **Allow** to allow access users based on the access rule. ■ **Deny**—Select **Deny** to deny access to users based on the access rule.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. ■ **To all destinations**— Access is allowed or denied to all destinations. ■ **To a particular server**—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server.

Table 158: *Access Rule Configuration Parameters*

Service category	Description
	■ **Except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ **To a network**—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ■ **Except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ **To a Domain Name**—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box. ■ **To AP IP**—Traffic to the specified Instant AP is allowed. After selecting this option, specify the domain name in the **IP** text box. ■ **To AP Network**—Traffic to the specified Instant AP network is allowed. After selecting this option, specify the domain name in the **IP** text box. ■ **To conductor IP**—Traffic to the specified conductor Instant AP or virtual controller is allowed. After selecting this option, specify the domain name in the **IP** text box.
Log	Select this check box if you want a log entry to be created when this rule is triggered. Aruba Central supports firewall based logging. Firewall logs on the Instant APs are generated as security logs.
Denylist	Select the **Denylist** check box to denylist the client when this rule is triggered. The denylisting lasts for the duration specified as **Auth failure denylist time** on the **Denylisting** tab of the **Security** window.
Classify Media	Select the **Classify Media** check-box to classify and tag media on https traffic as voice and video packets.
Disable Scanning	Select **Disable Scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable Scanning** applies only if ARM scanning is enabled.
DSCP Tag	Select this check box to add a DSCP tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing QoS on the network. To assign a higher priority, specify a higher value.
802.1p priority	Select this check box to enable 802.1p priority. 802.1p priority is an L2 protocol for traffic prioritization to manage QoS on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.
Time Range	Select this check box to enable user to access network for a specific time period. You can select the time range profile from the drop-down list that appears when the **Time Range** check box is selected..

11. Click **Save**.

Configuring ACLs on APs for Website Content Classification

You can configure web policy enforcement on an AP to block certain categories of websites based on your organization specifications by defining ACL rules.

To configure ACLs for website content classification, follow the below procedure:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
6. Under **Roles**, select the role to modify.
7. Under **Access Rules For Selected Roles**, click **+** to add a new rule.
   The Access Rule window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To set an access policy based on web categories:
   a. Under **Service**, select **Web Category**.
   b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.
   c. Under **Action**, select **Allow** or **Deny**.
   d. Click **Save**.
10. To filter access based on the security ratings of the website:
    a. Select **Web Reputation** under **Service**.
    b. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available:
       - **Trustworthy WRI > 81**—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.
       - **Low Risk WRI 61-80**—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
       - **Moderate WRI 41-60**—These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
       - **Suspicious WRI 21-40**—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
       - **High Risk WRI < 20**—These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads.
    c. Under **Action**, select **Allow** or **Deny** as required.
11. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high risk sites.
12. If required, select the following check boxes:
    - **Log** —Select this check box if you want a log entry to be created when this rule is triggered. Aruba Central supports firewall based logging. Firewall logs on the Instant APs are generated as security logs.
    - **Denylist** —Select this check-box to denylist the client when this rule is triggered. The denylisting lasts for the duration specified as **Auth Failure Denylist Time** on the **Denylisting** pane of the **Security** window. For more information, see Denylisting Instant AP Clients.

- **Disable Scanning**—Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see Configuring Radio Parameters.
- **DSCP Tag**—Select this check box to add a DSCP tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing QoS on the network. To assign a higher priority, specify a higher value.
- **802.1p priority**—Select this check box to enable 802.1p priority. 802.1p priority is an L2 protocol for traffic prioritization to manage QoS on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.

13. Click **Save** to save the rules.
14. Click **Save Settings** in the **Roles** pane to save the changes to the role for which you defined ACL rules.

In mixed versions of the groups, the application rule update is supported only at the VC level and not at the group level. If you have a group with multiple Instant APs running 6.2.1.0-4.0 and if you upgrade one or more VC to 6.2.1.0-4.1, you can configure application rules at the VC level, but not at the group level. To use application rules at the group level, create a new group and move Instant APs running 6.2.1.0-4.1 to the newly created group. If application rules are configured in this group, ensure that the Instant APs with versions lower than 6.2.1.0-4.1 are not moved to that group.

Configuring User Roles for AP Clients

Every client in the Aruba Central network is associated with a user role, which determines the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts.

Creating a User Role

To create a user role, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Roles** accordion.
7. In the **Roles** pane, click **+**.
8. In the **Add Role** window, enter a name for the new role in **Roles**, and then click **OK**.

You can also create a user role when configuring wireless profile. For more information, see Configuring Wireless Network Profiles on Instant APs.

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the Instant AP) or downstream (Instant AP to clients) traffic for a user role. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. For example, if clients are connected to an SSID, you can restrict the upstream bandwidth rate allowed for each user to 512 Kbps.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth per user to provide every user a specific bandwidth within a range of 1 to 65535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

To assign bandwidth contracts to a user role, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Roles** accordion.
7. Creating a User Role or select an existing role.
8. In the **Access Rues For Selected Roles** pane, click **+**.
9. In the **Access Rule** window, select **Bandwidth Contract** under **Rule Type**.
10. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select **Per User**.
11. Click **Save**. Associate the user role to a WLAN SSID or wired profile.

You can also create a user role and assign bandwidth contracts while configuring an SSID.

Configuring Role Derivation Rules for AP Clients

Aruba Central allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or VLAN to the clients connecting to an SSID or a wired profile.

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.

When creating more than one role assignment rule, the first matching rule in the rule list is applied.

To create a role assignment rule, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.
6. Click the **Access** tab.
7. Under **Access rules**, select **Role Based** to enable access based on user roles.
8. Under **Role Assignment Rules**, click **+ Add Role Assignment**. In **New Role Assignment Rule**, define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.
9. Select the attribute from the **Attribute** list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options.
10. Select the operator from the **Operator** list. The following types of operators are supported:
    - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
    - **Is the role**—The rule is applied if the attribute value is the role.
    - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
    - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
    - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
    - **ends-with**—The rule is applied only if the attribute value ends with string specified in *Operand*.
    - **matches-regular-expression**—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for WLAN clients.
11. Enter the string to match in the **String** box.
12. Select the appropriate role from the **Role** list.
13. Click **Save**.

Configuring VLAN Assignment Rule

To configure VLAN assignment rules for an SSID profile:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.

6. Click the **Access** tab.
7. Select the access rule from **Access rules**.
8. In the **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The **Access Rule** page is displayed.

The **VLAN Assignment** option is also listed in the **Access Rule** page when you create or edit a rule for wired port profiles in the **Ports** > **Create a New Network** > **Access** tab.

9. From the **Rule Type** drop-down list, select **VLAN Assignment** option.
10. Enter the VLAN ID in the **VLAN ID** field under **Service** section. Alternatively, you can select the VLAN ID or the VLAN name from the drop-down list provided next to the VLAN ID field.

The VLAN name for a specific VLAN is available only after mapping the VLAN ID with the VLAN name in the **Systems** > **Named VLAN Mapping** section. .

11. Click **Save**.

Configuring VLAN Derivation Rules

The users are assigned to a VLAN based on the attributes returned by the RADIUS server after users authenticate.

To configure VLAN derivation rules for an SSID profile:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click the **WLANs** tab.
   The WLANs details page is displayed.
5. In the **Wireless SSIDs** table, select a network profile and then click the edit icon.
6. Under **VLANs**, select **Dynamic** under **Client VLAN Assignment**.
7. Click **+ Add Rule** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.
8. Select an attribute from the **Attribute** list.
9. Select an operator from the **Operator** list. The following types of operators are supported:
   - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
   - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
   - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
   - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
   - **ends-with**—The rule is applied only if the attribute value ends with string specified in *Operand*.

- **matches-regular-expression**—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.

10. Enter the string to match in the **String** field.
11. Select the appropriate VLAN ID from **VLAN**. Ensure that all other required parameters are configured.
12. Click **OK**.

Configuring Firewall Parameters for Wireless Network Protection

To configure firewall settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Under **Firewall Settings**, turn on the toggle switch to enable **SIP**, **VOCERA**, **ALCATEL NOE**, **Auto Topology Rules**, **Restrict Corporate Access**, and **CISCO Skinny** protocols.
8. Under **Protection**, in the **Protection Against Wired Attacks** section, enable the following options:
   - **Drop Bad ARP**—Drops the fake ARP packets.
   - **Fix Malformed DHCP**—Fixes the malformed DHCP packets.
   - **ARP Poison Check**—Triggers an alert on ARP poisoning caused by the rogue APs.

Configuring Management Subnets

You can configure subnets to ensure that the Instant AP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.

To configure management subnets, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.

6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. Under **Management Subnets** pane, to add a new management subnet, complete the following steps:
   a. Enter the subnet address in **Subnet**.
   b. Enter the subnet mask in **Mask**.
   c. Click **Add**.
9. Click **Save Settings**.

Configuring Custom Redirection URLs for Instant AP Clients

You can create a list of URLs to redirect users to when they access blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network.

Creating a List of Error Page URLs

To create a list of error page URLs, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Under **Custom Blocked Page URL**, click **+** and enter the URL to block.
7. Repeat the procedure to add more URLs. You can add up to 8 URLs to the list of blocked web pages.
8. Click **OK**.

Configuring ACL Rules to Redirect Users to a Specific URL

To configure ACL rules to redirect users to a specific URL, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Under **Roles**, select the role for which you want to configure access rules.
7. Click **+** in the **Access Rules** section.
8. In the **New Rule Window**, select the rule type as **Blocked Page URL**.

9. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **+**.
10. Click **Save**.

Configuring Firewall Parameters for Inbound Traffic

Instant APs support an enhanced inbound firewall for the traffic that flows into the network through the uplink ports of an Instant AP.

To configure the firewall rules, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. In the **Access Rule** section, click the **+** icon.
   The **Inbound Firewall** page is displayed.
9. In the **Inbound Firewall** page, enter the following information:

Table 159: *Inbound Firewall Rule Configuration Parameters*

Parameter	Description
Service	Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement: ■ **Any**—Access is allowed or denied to all services. ■ **Custom**—Customize the access based on available options such as TCP, UDP, and other options. If you select the TCP or UDP options, enter appropriate port numbers. If the **Other** option is selected, ensure that an appropriate ID is entered.
Action	Select any of following actions: ■ Select **Allow** to allow user access based on the access rule. ■ Select **Deny** to deny user access based on the access rule. ■ Select **Destination-NAT** to allow making changes to the destination IP address and the port. ■ Select **Source-NAT** to allow making changes to the source IP address. The destination NAT and source NAT actions apply only to the network services rules.
Source	Select any of the following options: ■ **From all sources**—Traffic from all sources is either allowed, denied, or the IP address is translated at the source or the

Parameter	Description
	destination as defined in the rule. ■ **From a particular host**—Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the host. ■ **From a network**—Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. ■ **To all destinations**—Traffic for all destinations is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ **To a particular server**—Traffic to a specific server is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the destination server. ■ **Except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ **To a network**—Traffic to the specified network is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. ■ **Except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ **To a Domain name**—Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the domain name in the **Domain Name** text box. ■ **To AP IP**—Traffic to the specified Instant AP is allowed. After selecting this option, specify the domain name in the **IP** text box. ■ **To AP Network**—Traffic to the specified Instant AP network is allowed. After selecting this option, specify the domain name in the **IP** text box. ■ **To conductor IP**—Traffic to the specified conductor Instant AP or virtual controller is allowed. After selecting this option, specify the domain name in the **IP** text box.
Log	Select the **Log** check box if you want a log entry to be created when this rule is triggered. Instant supports firewall-based logging function. Firewall logs on the Instant APs are generated as security logs.

Parameter	Description
Denylist	Select the **Denylist** check box to denylist the client when this rule is triggered. The denylisting lasts for the duration specified in the **Auth failure denylist time** on the **denylisting** tab of the **Security** window.
Classify Media	Select the **Classify Media** check box to classify and tag media on HTTPS traffic as voice and video packets.
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of **Disable scanning** applies only if ARM scanning is enabled.
DSCP TAG	Select the **DSCP TAG** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

10. Click **Ok**.
11. Click **Save Settings**.

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default. The inbound firewall is not applied to traffic coming through the GRE tunnel.

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of conductor Instant AP, including clients connected to a member Instant AP.

To configure restricted corporate access, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. To restrict corporate access, turn on the **Restrict Corporate Access** toggle switch.
9. Click **Save Settings**.

Enabling ALG Protocols on Instant APs

To configure protocols for ALG, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Under **Firewall Settings**, set the toggle button against the corresponding protocol to enable **SIP**, **VOCERA**, **ALCATEL NOE**, **Auto Topology Rules**, **Restrict Corporate Access**, and **CISCO Skinny** protocols.
8. Click **Save Settings**.

When the protocols for the ALG are disabled, the changes do not take effect until the existing user sessions have expired. Reboot the Instant AP and the client, or wait a few minutes for changes to take effect.

Denylisting Instant AP Clients

The client denylisting denies connection to the denylisted clients. When a client is denylisted, it is not allowed to associate with an Instant AP in the network. If a client is connected to the network when it is denylisted, a deauthentication message is sent to force client disconnection.

Denylisting Clients Manually

Manual denylisting adds the MAC address of a client to the denylist. These clients are added into a permanent denylist. These clients are not allowed to connect to the network unless they are removed from the denylist.

To add a client to the denylist manually, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Denylisting** accordion.
7. Under **Manual Denylisting**, click **+** and enter the MAC address of the client to be denylisted.

8. Click **OK**.
9. Click **Save Settings**.

To delete a client from the manual denylist, select the MAC Address of the client under the **Manual Denylisting**, and then click the delete icon.

For the denylisting to take effect, you must enable the denylisting option when you create or edit the WLAN SSID profile. Go to **WLANs** > **Security** > **Advanced Settings** and enable the **Denylisting** option. For more information, see Configuring Wireless Network Profiles on Instant APs.

Denylisting Clients Dynamically

The clients can be denylisted dynamically when they exceed the authentication failure threshold or when a denylisting rule is triggered as part of the authentication process.

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically denylisted by an Instant AP.

In session firewall based denylisting, an ACL rule automates denylisting. When the ACL rule is triggered, it sends out denylist information and the client is denylisted.

To configure the denylisting duration, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Click the **Denylisting** accordion.
7. Under **Dynamic Denylisting**, enter the following information:
   - For **Auth Failure Denylist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be denylisted.
   - For **Policy Enforcement Failure Rule**, enter the duration after which the clients can be denylisted due to an ACL rule trigger.
8. Click **Save Settings**.

- You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. For more information on configuring maximum authentication failure attempts, see Configuring Wireless Network Profiles on Instant APs.
- To enable session-firewall-based denylisting, select the **Denylist** check-box in the **Access Rule** page during the WLAN SSID profile creation. For more information, see Configuring Network Service ACLs.

Mapping Instant AP Certificates

When an Instant AP joins a group that does not have a certificate, the Instant AP's existing certificate is retained. When an Instant AP joins a group that already has a certificate, the certificate of the Instant AP is overwritten by the group certificate.

To map an Instant AP certificate name to a specific certificate type or category, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Security** tab.
   The Security page is displayed.
6. Expand the **Certificate Usage** accordion.
7. To map a certificate, for each usage type under **Usage Type**, select the suitable certificate from the **Certificate** drop-down list:
   - **Certificate Authority**—To verify the identity of a client.
   - **Authentication Server**—To verify the identity of the server to a client.
   - **Captive Portal**—To verify the identity of internal captive portal server.
   - **RadSec**—To verify the identity of the TLS server.
   - **RadSec Certificate Authority**—To verify the authentication between the Instant AP and the TLS server.
   - **Clearpass**—To verify the identity of the ClearPass server.
8. Click **Save Settings**.

To enable certificates for the **Cloud Guest Service**, contact the Aruba Central support team.

Configuring Instant APs for VPN Services

This section describes the following VPN configuration procedures:

- Instant AP VPN Overview
- Configuring Instant APs for VPN Tunnel Creation
- Configuring Routing Profiles for Instant AP VPN

Configuring Instant APs for VPN Tunnel Creation

Instant AP supports the configuration of tunneling protocols such as GRE, IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on an Instant AP to enable communication with a controller in a remote location:

- Configuring IPsec VPN Tunnel
- Configuring Automatic GRE VPN Tunnel

- Configuring a GRE VPN Tunnel
- Configuring an L2TPv3 VPN Tunnel

Instant AP VPN Overview

As Instant APs use a virtual controller architecture, the Instant AP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating VPN tunnels from the Instant AP networks at branch locations or data centers, where the Aruba controller acts as a VPN Concentrator.

When the VPN is configured, the Instant AP acting as the virtual controller creates a VPN tunnel to Aruba Mobility Controller in your corporate office. The controller acts as a VPN endpoint and does not supply the Instant AP with any configuration.

The VPN features are recommended for:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple APs.
- Individuals working from home, connecting to the VPN.

Supported VPN Protocols

Instant APs support the following VPN protocols for remote access:

Table 160: *VPN Protocols*

VPN Protocol	Description
Aruba IPsec	IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session. You can configure an IPsec tunnel to ensure that to ensure that the data flow between the networks is encrypted. However, you can configure a split-tunnel to encrypt only the corporate traffic. When IPsec is configured, ensure that you add the Instant AP MAC addresses to the allowlist database stored on the controller or an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations. **NOTE:** The Instant APs support IPsec only with Aruba Controllers.
Layer-2 (L2) GRE	GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an endpoint. Instant APs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an Aruba Controller to encapsulate the packets sent and received by the Instant AP. You can use the GRE configuration for L2 deployments when there is no encryption requirement between the Instant AP and controller for client traffic. Instant APs support two types of GRE configuration: ■ **Manual GRE**—The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on the Instant AP, ensure that the GRE tunnel settings are enabled on the controller. ■ **Aruba GRE**—With Aruba GRE, no configuration on the controller is required except for adding the Instant AP MAC addresses to the allowlist database stored on the controller or an external server. Aruba GRE reduces manual configuration when **Per-AP Tunnel** configuration is required and supports failover between two GRE endpoints. **NOTE:** Instant APs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only with Aruba Controllers.

Table 160: *VPN Protocols*

VPN Protocol	Description
L2TP	The L2TP version 3 feature allows Instant AP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to LNS. In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with Instant AP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.

Configuring IPsec VPN Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the controller secures corporate data. You can configure an IPsec tunnel from virtual controller using Aruba Central.

To configure an IPsec tunnel from virtual controller, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
   The VPN page is displayed.
6. Click the **Controller** accordion.
7. In the **Protocol** drop-down list, select **Aruba IPsec**.
8. In the **Primary host** field, enter the IP address or FQDN for the main VPN/IPsec endpoint.
9. In the **Backup host** field, enter the IP address or FQDN for the backup VPN/IPsec endpoint. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
10. Specify the following parameters:
    a. Select the **Preemption** check-box to allow the VPN tunnel to switch back to the primary host when it becomes available again. This step is optional. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
    b. Select the **Fast Failover** check-box to allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately. When fast failover is enabled and if the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
    c. Specify a value in seconds for **Secs Between Test Packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.
    d. Enter a value for **Max Allowed Test Packet Loss** to define a number for lost packets, after which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.

e. Select the **Reconnect User On Failover** check-box to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary.
f. Specify a value in seconds for **Reconnect Time On Failover** to configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch. By default, the reconnection duration is set to 60 seconds. The **Reconnect Time on Failover** field is displayed only when **Reconnect User On Failover** is enabled.
g. From the **Branch Name** drop-down list, select the branch name.

When the IPsec tunnel configuration is completed, the packets that are sent from and received by an Instant AP are encrypted.

11. Click **Save Settings**.

You will be unable to upload the self-signed certificate from Aruba Central. You must upload the self-signed certificate to Aruba Activate followed by the AP reboot procedure. When the AP contacts Aruba Activate, the Aruba Activate informs the AP about the self-signed AP certificate that is required to be downloaded. The AP then installs a new certificate before connecting to Aruba Central. For more information, see *Aruba Activate User Guide*.

Configuring Automatic GRE VPN Tunnel

In Aruba Central, you can configure an Instant AP to automatically set up a GRE tunnel from the Instant AP to the controller.

To configure an Instant AP to automatically set up a GRE tunnel, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
   The VPN page is displayed.
6. Click the **Controller** accordion.
7. In the **Protocol** drop-down list, select **Aruba GRE**.
8. In the **Primary host** field, enter the IP address or FQDN for the main VPN/IPsec endpoint.
9. In the **Backup host** field, enter the IP address or FQDN for the backup VPN/IPsec endpoint. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
10. Specify the following parameters:
    a. Select the **Preemption** check-box to allow the VPN tunnel to switch back to the primary host when it becomes available again. This step is optional. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.

b. Select the **Fast Failover** check-box to allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately. If the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
c. Select the **Reconnect User On Failover** to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary,
d. Specify a value in seconds for **Reconnect Time On Failover** to configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch. By default, the reconnection duration is set to 60 seconds.
e. Specify a value in seconds for **Seconds Between Test Packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.
f. Enter a value for **Max Allowed Test Packet Loss** to define a number for lost packets, after which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.
g. Select the **Per-AP-Tunnel** check-box to create a GRE tunnel from each Instant AP to the VPN/GRE Endpoint rather than the tunnels created just from the conductor Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the conductor Instant AP.
h. From the **Branch Name** drop-down list, select the branch name.

11. Click **Save Settings**.

Configuring a GRE VPN Tunnel

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the Instant AP and controller. This procedure describes the steps involved in the manual configuration of a GRE tunnel from virtual controller by using Aruba Central.

During the manual GRE setup, you can either use the virtual controller IP or the Instant AP IP to create the GRE tunnel at the controller side depending upon the following Instant AP settings:

- If a virtual controller IP is configured and if Per-AP tunnel is disabled, the virtual controller IP is used to create the GRE tunnel.
- If a virtual controller IP is not configured or if Per-AP tunnel is enabled, the Instant AP IP is used to create the GRE tunnel.

To configure the GRE tunnel manually, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
   The VPN page is displayed.
6. Click the **Controller** accordion.
7. In the **Protocol** drop-down list, select **Manual GRE**.

8. Specify the following parameters:
   a. **Host**—Enter the IPv4 or IPv6 address or FQDN for the main VPN/GRE tunnel.
   b. **Backup Host**—(Optional) Enter the IPv4 or IPv6 address or FQDN for the backup VPN/GRE tunnel. You can edit this field only after you enter the IP address or FQDN in the **Host** field.
   c. **Reconnect User On Failover**—When you enter the host IP address and backup host IP address, this field appears. Select this check-box to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, select the **Reconnect User On Failover**.
   d. **Reconnect Time On Failover**—If you select the **Reconnect User On Failover** check-box, this field appears. To configure an interval for which wired and wireless users must be disconnected during a VPN tunnel switch, specify a value within a range of 30-90 seconds. By default, the reconnection duration is set to 60 seconds.
   e. **GRE Type**—Enter a value for the parameter.
   f. **GRE Mtu**—Specify a size for the **GRE MTU** within the range of 1024–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1300.
   g. **Per-AP-Tunnel**—The administrator can enable this option to create a GRE tunnel from each Instant AP to the VPN/GRE endpoint rather than the tunnels created just from the conductor Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the conductor Instant AP.

By default, the **Per-AP tunnel** option is disabled.

   h. **Branch Name**—Select the branch name from the **Branch Name** drop-down list.
9. When the GRE tunnel configuration is completed on both the Instant AP and the Controller, the packets sent from and received by an Instant AP are encapsulated, but not encrypted.

Configuring an L2TPv3 VPN Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows Instant AP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to LNS. In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with Instant AP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.

To configure an L2TPv3 tunnel by using Aruba Central, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
   The VPN page is displayed.
6. Click the **Controller** accordion.

7. In the **Protocol** drop-down list, select **L2TPv3**.
8. To configure a tunnel profile, complete the following steps:
    a. Turn on the **Enable Tunnel Profile** toggle switch.
    b. Enter the profile name in the **Profile Name** text-box.
    c. Enter the primary server IP address in the **Primary Peer Address** text-box.
    d. Enter the remote end backup tunnel IP address in the **Backup Peer Address** text-box. This is an optional field and is required only when backup server is configured.
    e. Enter the peer UDP port numbers in the **Peer UDP Port** text-box. The default value is 1701.
    f. Enter the local UDP port numbers in the **Local UDP Port** text-box. The default value is 1701.
    g. Enter the interval in the **Hello Interval** text-box at which the hello packets are sent through the tunnel. The default value is 60 seconds.
    h. Select the message digest as MD5 or SHA from the **Message Digest Type** drop-down list for message authentication.
    i. Enter a shared key in the **Shared Key** text-box for the message digest. This key should match with the tunnel end point shared key.
    j. Ensure that **Checksum** check-box is enabled.
    k. Specify a tunnel MTU value in the MTU check-box. The default value is 1460.
9. To configure a session profile, complete the following steps:
    a. Turn on the **Enable Session Profile** toggle switch.
    b. Enter the session profile name.
    c. Enter the tunnel profile name where the session will be associated.
    d. Configure the tunnel IP address with the corresponding network mask and VLAN ID. This is required to reach an AP from a corporate network. For example, SNMP polling.
    e. Select the cookie length and enter a cookie value corresponding to the length. By default, the cookie length is not set.
    f. From the **Branch Name** drop-down list, select the branch name.
10. Click **Save Settings**.

Configuring Routing Profiles for Instant AP VPN

Aruba Central can terminate a single VPN connection on Aruba Mobility Controller. The routing profile defines the corporate subnets which need to be tunneled through IPsec.

You can configure routing profiles to specify a policy based on routing into the VPN tunnel.

To configure routing profiles, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **VPN** tab.
   The VPN page is displayed.
6. Click the **Routing** accordion.

7. Click **+** in the **Routing** pane.

   The **New Route** page with the route parameters is displayed.
8. Update the following parameters:
   a. **Destination**—Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel.
   b. **Netmask**—Specify the subnet mask to the destination defined for **Destination**.
   c. **Gateway**—Specify the gateway to which traffic must be routed. In this field, enter one of the following based on the requirement:
      - The controller IP address on which the VPN connection will be terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route.
      - The "tunnel" string if you are using the Instant AP in **Local** mode during local DHCP configuration.
   d. **Metric**—Specify the best optimal path for routing traffic. A value of 1 indicates the best path, 15 indicates the worst path, and 16 indicates that the destination is unreachable on the route.
9. Click **OK**.
10. Click **Save Settings**.

Configuring DHCP Pools and Client IP Assignment Modes on Instant APs

This section provides the following information:

- Configuring DHCP Scopes on Instant APs
- Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients

Configuring DHCP Scopes on Instant APs

The VC supports the following types of DHCP address assignments:

- Configuring Distributed DHCP Scopes
- Configuring a Centralized DHCP Scope
- Configuring Local DHCP Scopes

Configuring Distributed DHCP Scopes

Aruba Central allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Aruba Central supports the following distributed DHCP scopes:

- **Distributed, L2**—In this mode, the VC acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC controls a scope that is a subset of the complete IP Address range for the subnet distributed across all the branches. This DHCP Assignment mode is used with the L2 forwarding mode.

- **Distributed, L3**—In this mode, the VC acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC is configured with a unique subnet and a corresponding scope.

To configure distributed DHCP scopes such as Distributed, L2 or Distributed, L3, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **DHCP** accordion.
7. To configure distributed DHCP scope, click **+** under **Distributed DHCP Scopes**.
   The **New Distributed DHCP Scopes** pane is displayed.
8. Based on the type of distributed DHCP scope, configure the following parameters:

Table 161: *Distributed DHCP Scope Configuration Parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ■ **Distributed, L2**—On selecting **Distributed, L2**, the VC acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ■ **Distributed, L3**—On selecting **Distributed, L3**, the VC acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Netmask	If **Distributed, L2** is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default Router	If **Distributed, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server.
Domain Name	If required, specify the domain name.
Lease Time	Specify a lease time for the client in minutes.

Table 161: *Distributed DHCP Scope Configuration Parameters*

Data pane item	Description
IP Address Range	Specify a range of IP addresses to use. To add another range, click the **+** icon. You can specify up to four different ranges of IP addresses. ■ For Distributed, L2 mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. ■ For Distributed, L3 mode, you can configure any dis-contiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. **NOTE:** You can allocate multiple branch IDs (BID) per subnet. The Instant AP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.
DHCP Reservation	Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations. **NOTE:** You can configure DHCP reservation only on virtual controllers. From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details: ■ **MAC**—Specify the MAC address of the device for which the IP address has to be reserved. ■ **IP**—Specify the IP address that has to be reserved for the MAC address. The IP address should be in the IP address range. **NOTE:** Aruba Central allows you to configure a maximum of 32 DHCP reservations. To delete a DHCP reservation, click the delete icon.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

9. Click **Next**. The **Branch Size** tab is displayed. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The Instant AP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
10. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.
11. Click **Finish**.

Configuring a Centralized DHCP Scope

The centralized DHCP scope supports L2 and L3 clients.

When a centralized DHCP scope is configured:

- The virtual controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For L2 clients, the virtual controller bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For L3 clients, the virtual controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPsec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

To configure a centralized DHCP scope, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **DHCP** accordion.
7. To configure centralized DHCP scopes, click **+** under **Centralized DHCP Scopes**.
   The New Centralized DHCP Scope data pane is displayed.

8. Based on type of centralized DHCP scope, configure the following parameters:

Table 162: *DHCP mode configuration parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select one of the following options: ■ Centralized, Layer-2 ■ Centralized, Layer-3
VLAN	Specify a VLAN ID or multiple VLAN IDs by entering a list of comma separated digits or ranges, for example 1,2,5, or 1- 4, or all. You can enter the VLAN ID in the range of 1-4093. To use this subnet, ensure that the VLAN ID(s) specified here is assigned to an SSID profile.
Split Tunnel	Enable the split tunnel function if you want allow a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. When the split tunnel function is enabled, the user can connect to file servers, database servers, mail servers, and other servers on the corporate network through the VPN connection. When the user connects to resources on the Internet (websites, FTP sites, and so on), the connection request goes directly to the gateway provided by the home network. The split DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to the Instant AP's own DNS server. When split tunnel is disabled, all the traffic including the corporate and the Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped. **NOTE:** When split tunnel is enabled, you can specify only a single VLAN ID in the **VLAN** field. When split tunnel is disabled, you can enter multiple VLAN IDs separated by commas in the **VLAN** field.
DHCP Relay	Select the **DHCP Relay** check-box to allow the Instant APs to intercept the broadcast packets and relay DHCP requests.
Helper Address	Enter the IP address of the DHCP server.
VLAN IP	Field is applicable only if you select **Centralized, Layer-3**. Specify the VLAN IP address of the DHCP relay server.
VLAN Mask	Field is applicable only if you select **Centralized, Layer-3**. Specify the VLAN subnet mask of the DHCP relay server.
Option 82	Select one of the following options: ■ **None**—If you have configured the DHCP Option 82 XML file, the **ALU** option scope is disabled in the drop-down list. To enable **ALU**, set the drop-down list to **None** and delete the DHCP Option 82 XML file. To enable the **XML** option, select **None** from the drop-down list and select the XML file from the **DHCP Option 82 XML** drop-down list. ■ **ALU**—ALU option is disabled if an XML file is selected from the **DHCP Option 82 XML** drop-down list in the **System** > **General** pane. Select **ALU** to enable DHCP Option 82 to

Table 162: *DHCP mode configuration parameters*

Data pane item	Description
	allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: ◦ Remote Circuit ID; X AP-MAC; SSID; SSID-Type ◦ Remote Agent; X IDUE-MAC ■ **XML**—XML option is enabled only if an XML file is selected from the **DHCP Option 82 XML** drop-down list in the **System** > **General** pane. Alternatively, to enable the **XML** option, select **None** from the drop-down list and select the XML file from the **DHCP Option 82 XML** drop-down list. For information related to XML files, see Configuring System Parameters for an AP

9. Click **Save Settings**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the Instant AP.

Table 163: *DHCP Relay and Option 82*

DHCP Relay	Option 82	Behavior
Enabled	**Enabled**	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	**Disabled**	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	**Enabled**	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	**Disabled**	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

Configuring Local DHCP Scopes

You can configure the following types of local DHCP scopes on an Instant AP:

- **Local**—In this mode, the VC acts as both the DHCP Server and default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured in other Instant AP clusters. The VC assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L2**—In this mode, the VC acts as a DHCP server and the gateway is located outside the Instant AP.
- **Local, L3**—In this mode, the VC acts as a DHCP server and default gateway, and assigns an IP address from the local subnet. The Instant AP routes the packets sent by clients on its uplink. This DHCP assignment mode is used with the L3 forwarding mode.

To configure a new local DHCP scope, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **DHCP** accordion.
7. To configure local DHCP scopes, click **+** under **Local DHCP Scopes**.
   The New DHCP Scopes data pane is displayed.
8. Based on type of local DHCP scope, configure the following parameters:

Table 164: *Local DHCP Configuration Parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ■ **Local**—On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the Instant AP. In the NAT mode, the traffic is forwarded through the uplink. ■ **Local, L2**—On selecting Local, L2, the VC acts as a DHCP server and a default gateway in the local network is used. ■ **Local, L3**—On selecting **Local, L3**, the VC acts as a DHCP server and gateway.
VLAN	Enter the VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Network	Specify the network to use.
Netmask	Specify the subnet mask. The subnet mask and the network determine the size of subnet.
Excluded Address	Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for **Excluded address**, the IP addresses either before or after the defined range are excluded.
DHCP Reservation	Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations. **NOTE:** You can configure DHCP reservation only on virtual controllers. From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details: ■ **MAC**—Specify the MAC address of the device for which the IP address has to be reserved. ■ **IP**—Specify the IP address that has to be reserved for the MAC address. The IP address should be in the IP address range.

Table 164: *Local DHCP Configuration Parameters*

Data pane item	Description
	NOTE: Aruba Central allows you to configure a maximum of 32 DHCP reservations. To delete a DHCP reservation, click the delete icon.
Default Router	Enter the IP address of the default router.
DNS Server	Enter the IP address of a DNS server.
Domain Name	Enter the domain name.
Lease Time	Enter a lease time for the client in minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. To add multiple DHCP options, click the **+** icon.

9. Click **Save Settings**.

Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the VC. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

- When the DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the virtual controller assigns the IP addresses to the WLAN or wired clients. By default, the Instant AP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.
- The Instant AP typically selects the 172.31.98.0/23 subnet. If the IP address of the Instant AP is within the 172.31.98.0/23 subnet, the Instant AP selects the 10.254.98.0/23 subnet. However, this mechanism does not avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Aruba Central, manually configure the DHCP pool by following the steps described in this section.

To configure DHCP server for client IP assignment, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.

4. Click **Show Advanced**.
5. Click the **System** tab.

   The System page is displayed.
6. Click the **DHCP** accordion.
7. Click **DHCP For WLANs** and enter the following information:
   a. Enter the domain name of the client in **Domain Name**.
   b. Enter the IP addresses of the DNS servers in **DNS Server**. To add another DNS server, click the **+** icon.
   c. Enter the duration of the DHCP lease in **Lease Time**. Select **Minutes**, **Hours**, or **Days** for the lease time from the list next to **Lease Time**. The default lease time is 0.
   d. Enter the network name in the **Network** box.
   e. Enter the mask name in the **Mask** box.
8. Click **Save Settings**.

To provide simultaneous access to more than 512 clients, use the **Network** and **Mask** fields to specify a larger range. While the network (prefix) is the common part of the address range, the mask (suffix) specifies how long the variable part of the address range is.

Configuring Services

This section describes how to configure location services, Lawful Intercept, OpenDNS, SIP phones, and Firewall services.

- Configuring an Instant AP for RTLS Support
- Configuring an Instant AP for ALE Support
- Managing BLE Beacons
- Configuring OpenDNS Credentials on Instant APs
- Configuring CALEA Server Support on Instant APs
- Configuring Instant APs for Palo Alto Networks Firewall Integration
- Configuring XML API Interface
- Configuring SIP Phones with Source-NAT
- Application Visibility and Deep Packet Inspection

Configuring an Instant AP for RTLS Support

Aruba Central supports the real time tracking of devices. With the help of the RTLS, the devices can be monitored in real time or through history.

To configure RTLS, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
5. Click **Real Time Locating System** > **Aruba**.
6. Select **Aruba RTLS** to send the RFID tag information to the Aruba RTLS server.
7. Click **3rd Party** and select **Aeroscout** to send reports on the stations to a third-party server.

8. In the **IP/FQDN** and **Port** field, specify the IP address and port number of the RTLS server, to which location reports must be sent.
9. In the **Passphrase** field, enter the passphrase required for connecting to the RTLS server.
10. Retype the passphrase in the **Retype Passprahrse** field.
11. Specify the update interval within the range of 6–60 seconds in the **Update every** field. The default interval is 30 seconds.
12. If **3rd Party** is selected, specify the IP address and port number of the 3rd party server.
13. Select **Include Unassociated Stations** to send reports on the stations that are not associated to any Instant AP.
14. Click **Save Settings**.

Configuring an Instant AP for ALE Support

ALE is designed to gather client information from the network, process it and share it through a standard API. The client information gathered by ALE can be used for analyzing a client's Internet behavior for business such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client user name
- IP address
- MAC address
- Device type
- Application firewall data, showing the destinations and applications used by associated devices.
- Current location
- Historical location

ALE requires the AP placement data to be able to calculate location for the devices in a network.

ALE with Aruba Central

Aruba Central supports Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the Instant AP sends client information and all status information to the ALE server.

To integrate Instant AP with ALE, the ALE server address must be configured on an Instant AP. If the ALE sever is configured with a host name, the Virtual Controller performs a mutual certificated-based authentication with ALE server, before sending any information.

Enabling ALE support on an Instant AP

To configure an Instant AP for ALE support:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services** tab. The Services page is displayed.
5. Click the **Real Time Locating System** accordion.
6. Click **Aruba**, and then select **Analytics & Location**.

7. Specify the ALE server name or IP address.
8. Specify the reporting interval within the range of 6–60 seconds. The Instant AP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
9. Click **Save Settings**.

Managing BLE Beacons

Instant APs support Aruba BLE devices, such as BT-100 and BT-105, which are used for location tracking and proximity detection. The BLE devices can be connected to an Instant AP and are managed by a cloud-based Beacon Management Console. The BLE Beacon Management feature allows you to configure parameters for managing the BLE beacons and establishing secure communication with the Beacon Management Console.

Support for BLE Asset Tracking

Instant AP assets can be tracked using BLE tags, Instant AP beacons scan the network. When a tag is detected, the Instant AP sends a beacon with information about the tag including the MAC address and RSSI of the tag to the Virtual Controller.

To manage beacons and configure BLE operation mode, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services** tab. The Services page is displayed.
5. Click the **Real Time Locating System** accordion.
6. Click **Aruba**.
7. Select **Manage BLE Beacons** to manage the BLE devices using BMC.
   a. Enter the authorization token in **Authorization token**. The authorization token is a text string of 1–255 characters used by the BLE devices in the HTTPS header when communicating with the BMC. This token is unique for each deployment.
   b. Enter the server URL in **Endpoint URL**. The BLE data is sent to the server URL for monitoring.
8. Select any of the following options from **BLE Operation Mode** drop-down list:

Table 165: *BLE Operation Modes*

Mode	Description
beaconing	The built-in BLE chip in the Instant AP functions as an iBeacon combined with the beacon management functionality.
disabled	The built-in BLE chip of the Instant AP is turned off. The BLE operation mode is set to **Disabled** by default.
dynamic-console	The built-in BLE chip of the Instant AP functions in the beaconing mode and dynamically enables access to Instant AP console over BLE when the link to LMS is lost.
persistent-console	The built-in BLE chip of the Instant AP provides access to the Instant AP console over BLE and also operates in the **Beaconing** mode.

9. To configure BLE web socket management server, enter the URL of BLE web socket management server in **BLE Asset Tag Mgmt Server(wss)**.

10. Select **BLE Asset Tag Mgmt Server(https)** to configure BLE HTTPS management server.
    a. Enter the URL of BLE HTTPS management server in **Server URL**.
    b. Enter the authorization token in **Authorization token**.
    c. Enter the location ID in **Location ID**.
11. Click **Save Settings**.

Configuring OpenDNS Credentials on Instant APs

Instant APs use the OpenDNS credentials to provide enterprise-level content filtering.

To configure OpenDNS credentials:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
5. Click the **OpenDNS** accordion.
6. Enter the **Username** and **Password**.
7. Click **Save Settings**.

Configuring CALEA Server Support on Instant APs

LI allows the Law Enforcement Agencies to perform an authorized electronic surveillance. Depending on the country of operation, the ISPs are required to support LI in their respective networks.

In the United States, Service Providers are required to ensure LI compliance based on CALEA specifications.

Aruba Central supports CALEA integration with an Instant AP in a hierarchical and flat topology, mesh Instant AP network, the wired and wireless networks.

NOTE

Enable this feature only if lawful interception is authorized by a law enforcement agency.

For more information on the communication and traffic flow from an Instant AP to CALEA server, see *Aruba Instant User Guide*.

To enable an Instant AP to communicate with the CALEA server, complete the following steps:

- Creating a CALEA Profile
- Creating ACLs for CALEA Server Support

Creating a CALEA Profile

To create a CALEA profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services** tab. The Services page is displayed.
5. Click the **CALEA** accordion.

6. Specify the following parameters:
   - **IP address**—Specify the IP address of the CALEA server.
   - **Encapsulation type**—Specify the encapsulation type. The current release of Aruba Central supports GRE only.
   - **GRE type**—Specify the GRE type.
   - **MTU**—Specify a size for the MTU within the range of 68—1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500.
7. Click **Save Settings**.

Creating ACLs for CALEA Server Support

To create an access rule for CALEA, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. If you select a group, perform the following steps:
   a. Under **Manage**, click **Devices** > **Access Points**.
   b. Click the **Config** icon. The tabs to configure the group is displayed.
3. If you select a device, under **Manage**, click **Devices**.
4. Click **Show Advanced**, and click **Security** tab. The Security page is displayed.
5. Click the **Roles** accordion.
6. Under **Access Rules for Selected Roles**, click **+** icon. The **New Rule** window is displayed.
7. Set the **Rule Type** to **CALEA**.
8. Click **Save**.
9. Create a role assignment rule if required.
10. Click **Save Settings**.

Configuring Instant APs for Palo Alto Networks Firewall Integration

Instant APs maintains the network (such as mapping IP address) and user information for its clients in the network. To integrate the Instant AP network with a third-party network, you can enable an Instant AP to provide this information to the third-party servers.

To integrate an Instant AP with a third-party network, you must add a global profile. This profile can be configured on an Instant AP with information such as IP address, port, user name, password, firewall enabled or disabled status.

Configuring an Instant AP for Network Integration

To configure an Instant AP for network integration:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed.
4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
5. Click the **Network Integration** accordion.
6. Select **Enable** to enable PAN firewall.
7. Specify the **Username** and **Password**. Ensure that you provide user credentials of the PAN firewall administrator.
8. Re-enter the password in **Retype**.

9. Enter the PAN firewall **IP Address**.
10. Enter the port number within the range of 1—65535. The default port is 443.
11. Enter the client domain in **Client Domain**.
12. Click **Save Settings**.

Application Visibility and Deep Packet Inspection

AppRF is a custom built Layer 7 firewall capability supported for Instant APs managed by Aruba Central. It consists of an on-board deep packet inspection and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application.

Instant APs with DPI capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories and website URLs based on security ratings. You can also define traffic shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.

- The Deep Packet Inspection feature is supported on Instant AP running Aruba InstantOS 6.4.3.x-4.1.x.x or later releases. The AppRF feature is not supported on IAP-104 and IAP-105 and IAP-134 and IAP-135.
- You can configure Instant APs to send URL information for the blocked HTTP and HTTPS sessions to ALE. The URL information can be extracted for the associated clients for DPI, analytics, and data mining through the Northbound APIs. To enable URL information logging and extraction, enable the URL Visibility parameter in the Instant AP UI or CLI. For more information, see *Aruba Instant User Guide*.

For more information on DPI and application analytics, see the following topics:

- Application Visibility
- Enabling Application Visibility Service on APs
- Configuring ACLs for Deep Packet Inspection
- Configuring ACLs on APs for Website Content Classification
- Configuring Custom Redirection URLs for Instant AP Clients

Enabling Application Visibility Service on APs

To view application usage metrics for WLAN clients, enable the Application Visibility service on APs.

To enable the Application Visibility feature, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select an AP group in the filter:
     a. Set the filter to a group containing at least one AP.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.
   - To select an AP in the filter:
     a. Set the filter to **Global** or a group containing at least one AP.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.

c. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.

d. Under **Manage**, click **Devices** > **Access Point**.

2. Click the **Config** icon.

   The tabs to configure the APs are displayed.
3. Click **Show Advanced**.
4. Click the **Services** tab.

   The Services page is displayed.
5. Expand the **AppRF** accordion.
6. Select any of the following options for **Deep Packet Inspection**:
   - **All**—Performs deep packet inspection on client traffic to application, application categories, website categories, and websites with a specific reputation score.
   - **App**—Performs deep packet inspection on client traffic to applications and application categories.
   - **WebCC**—Performs deep packet inspection on client traffic to specific website categories and websites with specific reputation ratings.
   - **None**—Disables deep packet inspection.
7. Click **Save Settings**.

Configuring SIP Phones with Source-NAT

Aruba Central allows to use SIP phones with source-NAT function using centralized Gateway service. SIP ALG is supported in bridge mode along with the use of NAT on APs.

The SIP phones with source-NAT supported only on AP devices running Aruba Instant 8.6.0.3.

To configure SIP phones with source-NAT function, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of access points is displayed in the **List** view.
3. Click the **Config** icon.

   The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Services** tab.

   The **Services** details page is displayed.
5. Click the **SIP** accordion.
6. Click the **+** icon in the **SIP** pane.

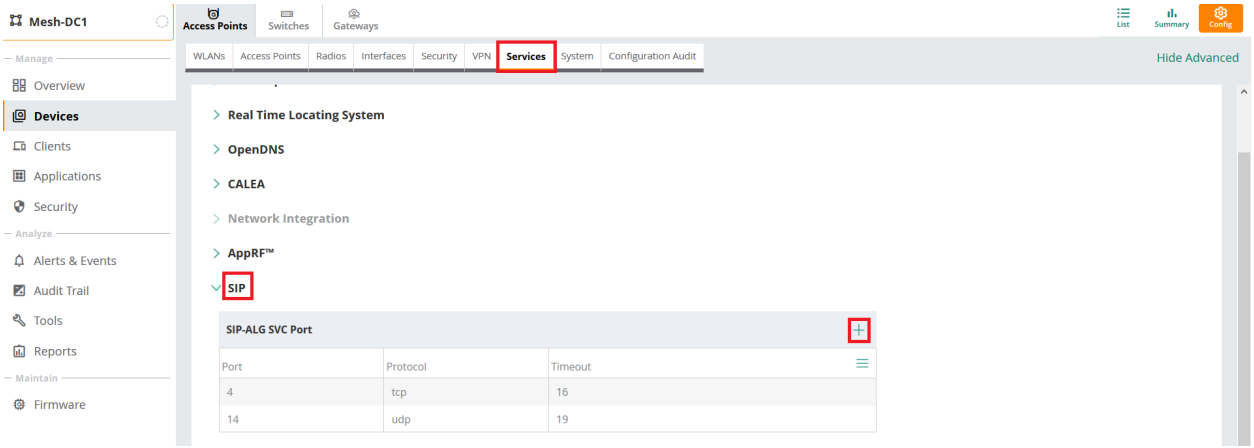
   The **SIP-ALG SVC Port** window is displayed.
7. In the **Port** field, enter the port number within the range of 1—65535.
8. Select **TCP** or **UDP** from the **Protocol** drop-down list.
9. In the **Timeout** field, enter the timeout value in seconds. The value should be between 15 to 30 seconds.

10. Click **OK**.

    The **SIP-ALG SVC Port** table in the **SIP** section lists the configured SIP settings.
11. Click **Save Settings**.

The following figure displays the SIP configuration page:

Figure 139 *SIP Configuration*



Configuring XML API Interface

The XML API interface allows Instant APs to communicate with an external server. The communication between Instant AP and an external server through XML API Interface includes the following steps:

- An API command is issued in the XML format from the server to the virtual controller.
- The virtual controller processes the XML request and identifies where the client is and sends the command to the correct member Instant AP.
- Once the operation is completed, the virtual controller sends the XML response to the XML server.
- The administrators can use the response and take appropriate action to suit their requirements. The response from the virtual controller is returned using the predefined formats.

To configure XML API for servers, complete the following steps:

1. In the **Network Operations** app, set the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon. The tabs to configure access points is displayed
4. Click **Show Advanced**, and click **Services**. The Services page is displayed.
5. Go to **Network Integration** > **XML API Server Configuration**.
6. Click **+** to add a new XML API server.
7. Enter a name for the XML API server in the **Name** text box.
8. Enter the IP address of the XML API server in the **IP Address** text box.
9. Enter the subnet mask of the XML API server in the **Mask** text box.
10. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server.
11. Re-enter the passcode in the **Retype Passphrase** box.
12. To add multiple entries, repeat the procedure.
13. Click **Add**.

14. Click **Save Settings**.
15. To edit or delete the server entries, use the **Edit** and **Delete** buttons, respectively.

For information on adding an XML API request, see *Aruba Instant User Guide*.

Configuring Uplink Interfaces on Instant APs

This section provides the following information:

- Configuring Uplink Interfaces
- Configuring Uplink Preferences and Switching
- Enabling 802.1X Authentication on Uplink Ports of an AP

Configuring Uplink Interfaces

Aruba Central supports 3G and 4G USB modems, ethernet, and the Wi-Fi uplink to provide access to the corporate network.

By default, the AP-318, AP-374, AP-375, and AP-377 access points have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and 8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable.

The following types of uplinks are supported on Aruba Central:

- 3G/4G Uplink
- Ethernet Uplink
- Wi-Fi Uplink

3G/4G Uplink

Aruba Central supports the use of 3G/4G USB modems to provide the Internet back haul to Aruba Central. The 3G/4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the Instant APs to automatically choose the available network in a specific region.

Types of Modems

Aruba Central supports the following three types of 3G modems:

- **True Auto Detect**—Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary.
- **Auto-detect + ISP/country**—Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto Detect**—Modems of this type are used only if they share the same Device-ID, Country, and ISP details. You need to configure different parameters for each of them. These modems work with Aruba Central when the appropriate parameters are configured.

Table 166: *4G Supported Modem*

Modem Type	Supported 4G Modem
True Auto Detect	▪ Pantech UML290 ▪ Ether-lte

When Pantech UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

To configure 3G or 4G uplinks using Aruba Central, complete the following steps:

Before you begin, obtain the modem configuration parameters from the local IT administrator or the modem manufacturer.

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **3G/4G**, complete the following steps:
   - To configure a 3G or 4G uplink automatically, select the country and the ISP from the **Country** and **ISP** drop-down list. The parameters are automatically populated.
   - To configure a 3G or 4G uplink manually, complete the following steps:
     - Select the country from the **Country** drop-down list.
     - Select the service protocol from the **ISP** drop-down list.
     - Enter the type of 3G modem in the **USB Type** text-box.
     - Enter the type of 4G modem in the **4G USB Type** text-box.
     - Enter the device ID of modem in the **USB DEV** text-box
     - Enter the TTY port of the modem in the **USB TTY** text-box.
     - Enter the parameter to initialize the modem in the **USB INIT** text-box.
     - Enter the parameter to dial the cell tower in the **USB Dial** text-box.
     - Enter the parameter used to switch a modem from the storage mode to modem mode in the **USB Mode Switch** text-box.

- Select the USB authentication type from the **USB Auth Type** drop-down list.
- Enter the username used to dial the ISP in the **USB User** text-box.
- Enter the password used to dial the ISP in the **USB Password** text-box.

8. Click **Save Settings** and reboot the Instant AP for changes to affect.

Ethernet Uplink

The Ethernet 0 port on an Instant AP is enabled as an uplink port by default. The Ethernet uplink supports the following:

- **PPPoE**
- **DHCP**
- **Static IP**

You can use **PPPoE** for your uplink connectivity in a single AP deployment.

Uplink redundancy with the **PPPoE** link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The Instant AP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using PAP or the CHAP. Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the Instant AP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during Instant AP boot and if the configuration is correct, Ethernet is used for the uplink connection.

When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the VC. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE Uplink Profile

To configure PPPoE settings, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Uplink** accordion.

7. Under **PPPoE**, specify the following parameters:
   a. In the **Service Name** text-box, enter the PPPoE service name provided by your service provider.
   b. In the **CHAP Secret** text-box, enter the secret key used for CHAP authentication. You can use a maximum of 34 characters for the CHAP secret key.
   c. In the **Retype CHAP Secret** text-box, re-enter the secret key used for CHAP authentication.
   d. From the **Local Interface** drop-down list, set a local interface for the PPPoE uplink connections. The selected DHCP scope is used as a local interface on the PPPoE interface and the Local, L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allocated the entire Local, L3 DHCP subnet to the clients.
   e. In the **User** text-box, enter the user name for the PPPoE connection
   f. In the **Password** text-box, enter a password for the PPPoE connection.
   g. In the **Retype Password** text-box, re-enter the password for the PPPoE connection.

The options in **Local Interface** are displayed only if a Local, L3 DHCP scope is configured on the Instant AP.

8. Click **Save Settings** and reboot the Instant AP for changes to affect.

Wi-Fi Uplink

The Wi-Fi uplink is supported for all Instant AP models, except 802.11ac APs. Only the conductor Instant AP uses the Wi-Fi uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single radio Instant APs, the radio serves wireless clients and Wi-Fi uplink.
- For dual radio Instant APs, both radios can be used to serve clients but only one of them can be used for Wi-Fi uplink.

When Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the Instant AP.
- If Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.

To provision an Instant AP with Wi-Fi Uplink, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Uplink** accordion.

7. Under **Wi-Fi**, specify the following parameters:
   - In the **Name(SSID)** text-box, enter the name of the wireless network that is used for Wi-Fi uplink.
   - From the **Band** drop-down list, select the band in which the VC currently operates. The following options are available:
     - **2.4 GHz (default)**
     - **5 GHz**
   - From the **Key Management** drop-down list, select the type of key for uplink encryption and authentication.
   - When **WPA Personal** or **WPA-2 Personal** key management type is selected, the passphrase options are available for configuration.
     - From the **Passphrase Format** drop-down list, select either **8 - 63 alphanumeric characters** or **64 hexadecimal characters**.
     - In the **Passphrase** text-box, enter the passphrase.
   - When **WPA Enterprise** or **WPA-2 Enterprise** key management type is selected, the 802.1x authentication options are available for configuration.
     - From the **WIFI1X** drop-down list, select the 802.1x authentication protocol to be used:
       - Specify the certificate type to be used by selecting **Cert TPM** or **Cert User**.
       - If **PEAP** authentication type is selected, enter the user credentials in the **Username** and **Password** text-box.
     - Toggle the **Validate Server** button to enable or disable server certificate verification by the AP.
8. Click **Save Settings** and reboot the Instant AP for changes to affect.

If the uplink wireless router uses mixed encryption, **WPA-2 Personal** or **WPA-2 Enterprise** is recommended for Wi-Fi uplink.

Configuring Uplink Preferences and Switching

This section describes the following topics:

- Enforcing Uplinks
- Setting an Uplink Priority
- Enabling Uplink Pre-emption

Enforcing Uplinks

The following conditions apply to the uplink enforcement:

- When an uplink is enforced, the Instant AP uses the specified uplink regardless of uplink pre-emption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the Instant AP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and pre-emption is not enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured.
- When no uplink is enforced and pre-emption is enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured. If current uplink is active, the Instant AP

periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

To enforce a specific uplink on an Instant AP, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Expand the **Uplink** accordion.
7. Under **Management** > **Enforce Uplink**, select the type of uplink from the drop-down list. If Ethernet uplink is selected, the **Port** field is displayed.
8. Specify the Ethernet interface port number.
9. Click **Save Settings**.
   The selected uplink is enforced on the Instant AP.

Setting an Uplink Priority

To set an uplink priority, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **Management** > **Uplink Priority List**, select the uplink to increase or decrease the priority. By default, the **Eth0** uplink is set as a high priority uplink.
8. Click **Save Settings**.
   The selected uplink is prioritized over other uplinks.

Enabling Uplink Pre-emption

The following configuration conditions apply to uplink pre-emption:

- Pre-emption can be enabled only when no uplink is enforced.
- When pre-emption is disabled and the current uplink fails, the Instant AP tries to find an available uplink based on the uplink priority configuration.

- When pre-emption is enabled and if the current uplink is active, the Instant AP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.

To enable uplink pre-emption, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **Management**, ensure that the **Enforce Uplink** is set to **None**.
8. Select the **Pre-emption** check-box.
9. Specify value for **Pre-emption Interval**.
10. Click **Save Settings**.

Switching Uplinks based on the Internet Availability

You can configure Aruba Central to switch uplinks based on the Internet availability.

When the uplink switchover based on Internet availability is enabled, the Instant AP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the Internet is not reachable from the current uplink, the Instant AP switches to a different connection.

To configure uplink switching, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **Interfaces** tab.
   The Interfaces page is displayed.
6. Click the **Uplink** accordion.
7. Under **Management**, specify a value for **Failover Internet IP**.
8. Select the **Internet Failover** check-box.
9. Specify values for **Failover Internet Packet Send Frequency**, **Failover Internet Packet Lost Count**, and **Internet Check Count**.

10. Click **Save Settings**.

- By default, the conductor AP sends the ICMP packets to 8.8.8.8 IP address only if the out-of-service operation based on Internet availability (internet-down state) is configured on the SSID. You can use **Failover Internet IP** as an alternative to the default option to configure an IP address to which the AP must send AP packets, and verify if the Internet is reachable when the uplink is down.
- When **Internet Failover** is enabled, the Instant AP ignores the VPN status, although uplink switching based on VPN status is enabled.

Configuring Preferred Uplink on AP-318 and 370 Series APs

The AP-318 and 370 Series APs have an ethernet port for Eth0 and a fibreport for Eth1. Either of these ports can be configured as the uplink port as required. By default, Eth1 port is configured as the uplink for these AP platforms. All functionality of the Eth0 port is supported by Eth1 port with exception to the following:

- Eth0 bridging feature is not supported when the Eth1 port is configured as preferred uplink.
- If LACP is enabled, the Eth1 port cannot be configured as the preferred uplink.

By default, the AP-318, AP-374, AP-375, and AP-377 Instant APs have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and 8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable.

Configuring Enterprise Domains

In a typical Instant AP deployment without tunneling, all DNS requests from a client are forwarded to the client's DNS server by default. However, if an Instant AP is configured for tunneling, the IAP-VPN enables split DNS by default, and the DNS behavior for both the clients on the Instant AP network is determined by the enterprise domain settings.

The enterprise domain setting on the Instant AP specifies the domains for which DNS resolution must be forwarded to the default DNS server of the client. For example, if the enterprise domain is configured for **arubanetworks.com**, the DNS resolution for host names in the **arubanetworks.com** domain is forwarded to the default DNS server of the client. The DNS resolution for host names in all other domains is forwarded to the local DNS server of the Instant AP.

- In a full-tunnel mode, all DNS traffic is forwarded over IPSec tunnel to DNS server of the client regardless of the enterprise domain configuration. If an asterisk is configured in the enterprise domain list instead of a domain name, then all DNS requests are forwarded to the default DNS server of the client.
- Split DNS functionality is supported for IAP-VPN scenarios only.

To configure an enterprise domain, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.

3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **Enterprise Domains** accordion.
7. Click **+** in the **Enterprise Domains** pane, and enter a name in the **New Domain Name** window.
8. Click **OK**.
9. Click **Save Settings**.

To delete an enterprise domain, select the domain in the **Enterprise Domains** pane, and then click the delete icon.

Configuring SNMP Parameters

This section describes the following topics:

- SNMP Configuration Parameters
- Configuring Community String for SNMP
- Configuring SNMP Trap Receivers

SNMP Configuration Parameters

Aruba Central supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An Instant AP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an Instant AP:

Table 167: *SNMP Parameters*

Data Pane Item	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the virtual controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the Instant AP, you can configure the following parameters:	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: ■ **MD5**—HMAC-MD5-96 Digest Authentication Protocol ■ **SHA**—HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption).

Data Pane Item	Description
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

Configuring Community String for SNMP

This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings in Aruba Central.

Creating Community strings for SNMPv1 and SNMPv2 using Aruba Central

To create community strings for SNMPv1 and SNMPv2, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **SNMP** accordion.
7. Under **SNMP**, click **+** to add a new community string.
8. In the **New SNMP** window, enter a name for the community string.
9. Click **OK**.
10. To delete a community string, select the string in the **SNMP** pane, and then click the delete icon.

Creating community strings for SNMPv3 using Aruba Central

To create community strings for SNMPv3, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **SNMP** accordion.
7. Under **User for SNMPV3**, click **+** to add a new community string for **SNMPv3**.

8. In the **New SNMPv3 User** window, enter the following information:
   a. In the **Auth protocol** drop-down list, select the type of authentication protocol.
   b. In the **Password** text-box, enter the authentication password and retype the password in the **Retype Password** text-box.
   c. In the **Privacy protocol** drop-down list, select the type of privacy protocol.
   d. In the **Password** text-box, enter the privacy protocol password and retype the password in the **Retype Password** text box.
   e. Click **OK**.
9. To edit the details for a particular user, select the user, and then click the edit icon.
10. To delete a particular user, select the user, and then click the delete icon.

Configuring SNMP Trap Receivers

Aruba Central supports the configuration of external trap receivers. Only the Instant AP acting as the VC generates traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

To configure SNMP traps, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **SNMP** accordion.
7. Under **SNMP Traps Receivers**, click **+** to add a new community string for **SNMP Traps Receivers**.
8. In the **New SNMP Trap Receiver** window, enter the following information:
   a. In the **IP Address** text-box, enter the IP address of the new SNMP Trap Receiver.
   b. In the **Version** drop-down list, select the SNMP version, such as **v1, v2c, v3**. The version specifies the format of traps generated by the access point.
   c. In the **Community/Username** text-box, specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
   d. In the **Port** text-box, enter the port to which the traps are sent. The default value is 162.
   e. In the **Inform** drop-down list, select **Yes** or **No**. When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**.
   f. Click **OK**.

Configuring Syslog and TFTP Servers for Logging Events

This section describes the following topics:

- Configuring Syslog Server on Instant APs
- Configuring TFTP Dump Server on Instant APs

Configuring Syslog Server on Instant APs

To specify a syslog server for sending syslog messages to the external servers, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **Logging** accordion.
7. In the **Servers** section, enter the IP address of the syslog server in the **Syslog Server** text-box.
   You can enter up to three IP addresses in the **Syslog Server** text box. Separate each value with a comma.

Aruba Central allows you to configure up to three syslog servers for logging events.

8. Click **Syslog Facility Levels**, and enter the required logging level from the drop-down in each of the fields. Syslog facility level is an information field associated with a syslog message. It is an application or operating system component that generates a log message.
   The Instant AP supports the following syslog facilities:
   - **Syslog Level**—Detailed log about syslog levels.
   - **AP-Debug**—Detailed log about the AP device.
   - **Network**—Log about change of network, for example, when a new Instant AP is added to a network.
   - **Security**—Log about network security, for example, when a client connects using wrong password.
   - **System**—Log about configuration and system status.
   - **User**—Important logs about client.
   - **User-Debug**—Detailed log about client.
   - **Wireless**—Log about radio.

   Table 168 describes the logging levels in order of severity, from the most severe to the least.

Table 168: *Logging Levels*

Logging level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical condition such as a hard drive error.
Error	Error conditions.
Warning	Warning messages.

Logging level	Description
Notice	Significant events of a non-critical nature. The default value for all syslog facilities.
Information	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

9. Click **Save Settings**.

Configuring TFTP Dump Server on Instant APs

To configure a TFTP server for storing core dump files, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **Logging** accordion.
7. In the **Servers** section, enter the IP address of the TFTP server in the **TFTP Dump Server** text-box.
8. Click **Save Settings**.

Configuring Mobility for Clients

Instant APs form a single Aruba Central network when they are in the same Layer-2 (L2) domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the Aruba Central network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

Layer-3 (L3) mobility allows a client to roam without losing its IP address and sessions. If WLAN access parameters are the same across these networks, clients connected to Instant APs in a given Aruba Central network can roam to Instant APs in a foreign Aruba Central network and continue their existing sessions using their IP addresses. You can configure a list of Virtual Controller IP addresses across which L3 mobility is supported.

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby AP and overload it. When load balancing is enabled, the VC assigns the home AP for roamed clients by using a round robin policy. With this policy, the load for the APs acting as Home Agents for roamed clients is uniformly distributed across the Instant AP cluster.

Configuring L3 Mobility Domain

To configure a mobility domain, you have to specify the list of all Aruba Central networks that form the mobility domain. To allow clients to roam seamlessly among all the APs, specify the VC IP for each foreign

subnet. You may include the local Aruba Central or VC IP address, so that the same configuration can be used across all Aruba Central networks in the mobility domain.

Aruba recommends that you configure all client subnets in the mobility domain. When client subnets are configured:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, the L3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, the L3 roaming is set up.

To configure a Layer-3 Mobility domain, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the APs are displayed.
4. Click **Show Advanced**.
5. Click the **System** tab.
   The System page is displayed.
6. Click the **Layer-3 Mobility** accordion.
7. Turn on the **Home Agent Load Balancing** toggle switch. By default, home agent load balancing is disabled.
8. Under **IP Address**, click **+**, and enter an IP address name in the **New IP Address** window, and then click **OK**.
   Repeat Step 7 to add the IP addresses of all VCs that form the L3 mobility domain.
9. Under **Subnets**, click **+**, and specify the following:
   a. Enter the client subnet in the **IP Address** box.
   b. Enter the mask in the **Subnet Mask** box.
   c. Enter the VLAN ID in the home network in the **VLAN ID** box.
   d. Enter the home VC IP address for this subnet in the **Virtual Controller IP** box.
10. Click **OK**.

Renaming an AP

You can change the name of an AP provisioned in Aruba Central. The AP can be online or offline. When you rename an AP or a VC, the AP or VC does not reboot, and the client traffic is not affected. The new name must be a character string of up to 32 ASCII or non-ASCII characters, including spaces.

To rename an AP, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select an AP group in the filter:
     a. Set the filter to a group containing at least one AP.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of APs is displayed in the **List** view.

- To select an AP in the filter:
  a. Set the filter to **Global** or a group containing at least one AP.
  b. Under **Manage**, click **Devices** > **Access Points**.
     A list of APs is displayed in the **List** view.
  c. Click an AP listed under **Device Name**.
     The dashboard context for the AP is displayed.
  d. Under **Manage**, click **Devices** > **Access Point**.

2. Click the **Config** icon.
   The tabs to configure the APs are displayed.
3. Click the **Access Points** tab.
   The Access Points table is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Under **Basic Info**, modify the AP or VC name in the **Name** field.
6. Click **Save Settings**.

The AP name is updated on the AP immediately. It may take up to 1 minute for the new AP name to get reflected in Aruba Central.Renaming an AP depends on various privileges and access permissions that are assigned to each user to make configuration changes. For more information, see Users and Roles.

Monitoring APs

The access point (AP) dashboard enables you to manage, configure, monitor and troubleshoot APs provisioned and managed through Aruba Central.

The AP Health Bar provides a snapshot of the overall health of the APs configured in Aruba Central. For more information, see Health Bar for the AP Dashboard.

The AP Foundation license is applicable for Access Point Monitoring.

Monitoring APs in Summary View

The access point (AP) Summary page provides all the metrics about the health, status, and clients information associated with the AP provisioned and managed in Aruba Central.

Viewing the AP Summary Page

To navigate to the AP Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of APs is displayed in the **List** view.
3. Click the **Summary** icon.
   The AP Summary page is displayed.

The AP Summary page displays the following information:

- **Usage**—Displays the incoming and outgoing data traffic detected on the APs.
- **Clients**—Displays the number of clients connected to an AP over a specific time period.
- **Bandwidth Usage Per Network**—Displays the incoming and outgoing traffic for all APs per SSID over a specific duration.
- **Client Count Per Network**—Displays the number of clients connected to an AP per SSID over a specific time period.

  You can change the time range for the AP Summary page by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Monitoring APs in List View

The access point (AP) List page provides information associated with the APs and radios provisioned and managed in Aruba Central.

The AP List page is available for Foundation and Advanced licenses for APs.

The AP List page displays the following sections:

Viewing the AP List Page

To navigate to the AP List page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.

The AP List page displays the following information:

- **Access Points**—Displays the total number of APs. When you click the **Access Points** tab, it provides information about all APs in the **Access Points** table.
- **Online**—Displays the total number of online APs. When you click the **Online** tab, it provides information about the online APs in the **Access Points** table.
- **Offline**—Displays the total number of offline APs. When you click the **Offline** tab, it provides information about the offline APs in the **Access Points** table.
- **Radios**—Displays the total number of radios. When you click the **Radios** tab, it provides information about all radios in the **Radios** table.
  - **2.4 GHz**—Displays the total number of 2.4 GHz radios. When you click the **2.4 GHz** tab, it provides information about 2.4 GHz radios in the **Radios** table.
  - **5 GHz**—Displays the total number of active 5 GHz and 5 GHz (Secondary) radios. When you click the **5 GHz** tab, it provides information about 5 GHz and 5 GHz (Secondary) radios in the **Radios** table.

NOTE

The tri-radio feature is available only for AP-555. In the **5 GHz** tab, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.

Access Points Table

The **Access Points** table displays the following information:

- **Device Name**—Name of the AP.
- **Status**—Displays the operational status of the AP. The status is as follows:
  - **Online**—Indicates that the AP is online.
  - **Offline**—Indicates that the AP is offline.
  - **Online**—Indicates that the AP is operating under thermal management. For more information, see Thermal Shutdown Support in IAP.
- **IP Address**—IP address of the AP.
- **Model**—The model number of the AP.
- **Serial**—The serial number of the device.
- **Firmware Version**—The firmware version running on the AP.
- **Clients**—Clients connected to the AP.
- **Alerts**—Opens alerts related to APs.
- **MAC Address**—MAC address of the AP.
- **Virtual Controller**—The name of the virtual controller.
- **Config Status**—The configuration changes associated with the AP. The **Config Status** column is not supported in the exported CSV file.
- **Group**—Group to which the AP belongs.
- **Labels**—Labels associated with the AP. If multiple labels are associated with the AP, hover over the label link to view all the labels.
- **Site**—The site to which the device belongs.
- **Uptime**—Time since when the device is operational. The **Uptime** column is not applicable for offline devices and remains blank for all the devices in the **Offline** page.
- **Last Seen**—The last active time and date of the device. The **Last Seen** column is not applicable for online devices and remains blank for all the devices in the **Online** page.
- **Public IP**—IP address logged by servers when the device is connected through internet connection.
- **LLDP Neighbor**—Displays the name of the LLDP neighbor. Click the LLDP Neighbor name to view the switch details page, if the switch is managed by Aruba Central.
- **LLDP Port**—Displays the port number of LLDP neighbor.
- **AI Insights**—The number of AI insights generated for the AP in the last three hours. The **AI Insights** column is not supported in the exported CSV file.
- **Note**—Displays the information captured in the **Note** parameter, in the AP Details section. The search filter allows you to search for exact and partial text search with prefix. The text search with suffix is not supported.
- **Zone**—Zone to which the AP belongs.

- A search filter is provided only for the **Device Name**, **IP Address**, **Model**, **Serial**, **MAC Address**, **Virtual Controller**, **Group**, **Labels**, **Site**, **LLDP Neighbor**, **Note**, and **Zone**columns. The and icons allow you to sort the **Device Name**, **IP Address**, **Serial**, **MAC Address**, **Virtual Controller**, and **Zone** columns in an ascending and descending order.

NOTE

- By default, the AP List table displays the **Device Name**, **Status**, **IP Address**, **Model**, **Serial**, and **Firmware Version**. You can customize the view of AP List table with additional columns such as the **Clients**, **Alerts**, **MAC Address**, **Virtual Controller**, **Config Status**, **Group**, **Labels**, **Site**, **Uptime**, **Last Seen**, **Public IP**, **LLDP Neighbor**, **LLDP Port**, **Insights**, **Note**, and **Zone**. These additional columns can be selected by clicking the icon provided at the right corner of the table that displays the AP list. Click the **Reset to default** button provided in the drop-down list to reset the AP List with default columns only. To autofit the columns, click the icon and select **Autofit columns**.

To download the **.csv** file of the AP list table, click the icon. If the table contains unicode value, you must use a UTF-8 enabled software to view the contents. To view the file in Microsoft Excel 2007 spreadsheet software, perform the following steps to view table with unicode values:

1. Open the Microsoft Excel 2007 software.
2. Click on the Data menu bar option.
3. Click on the **From Text** icon.
4. Browse to the location of the file that you want to import.
5. Select the file name and click **Import**.
6. The **Text Import** wizard is displayed.
7. Select the file type. For **.csv** format, select the **Delimited** option.
8. Select the **65001: Unicode (UTF-8)**option from the drop-down list that is displayed next to the **File** origin.
9. Click **Next**. The **Text ImportWizard-Step 1 of 3** page is displayed.
10. Place a check mark next to the delimiter such as the comma or full stop that was used in the file you wish to import into Microsoft Excel 2007.
11. The **Data Preview** window displays the data based on the selected delimiter.
12. Click **Next**. The **Text ImportWizard-Step 3 of 3** page is displayed. Select the appropriate data format for each column that you want to import.

NOTE

Importing one or more columns is optional.

13. Click **Finish** to import the data into Microsoft Excel 2007.

Deleting an Offline AP

To delete an offline AP, see Deleting an Offline AP.

Rebooting an AP

To reboot an AP, see Rebooting an AP.

Radios Table

When you click the **Radios**, **2.4 GHz**, and **5 GHz** tab in the **Radios** list page, the respective tables with the following columns are displayed:

- **Access Point**—Name of the AP.

NOTE

The online radios are displayed with a green dot and offline radios are displayed with a red dot.

- **Radio MAC Address**—The MAC address of the radios connected to the AP.
- **Band**—The type of radio band. For example, **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)**.

NOTE

The tri-radio feature is available only for AP-555. In the **Band** column, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.

- **Bandwidth**—The bandwidth of data transferred through the radios.
- **Channel**—Channels assigned for the radios.
- **Utilization (%)**—The percentage of time (normalized to 255) that the channels of the radios are sensed to be busy. The AP uses either the physical or the virtual carrier sense mechanism to sense a busy channel. This percentage not only depends on the data bits transferred but also with the transmission overhead that makes use of the channel.
- **Power (dBm)**—The transmit power of the radios measured in decibels.
- **Noise Floor (dBm)**—The noise at the radio receivers of the radios. Certain type of interferences, though not all, may affect or increase:
  - Noise at the radio receivers of the radios
  - Thermal noise
  - Noise floor

  Noise Floor value may vary depending on the noise introduced by components used in the computer or client device.

NOTE

A search filter is provided only for the **Access Point** column.

Rebooting an AP

To reboot an access point (AP), complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
3. A list of APs is displayed in the **List** view.
4. In the **Access Points** table, hover over the online AP that you want to reboot.
5. Click the reboot icon.

NOTE

To reboot multiple online APs, select the online APs that you want to reboot and click the reboot icon.

6. Click **Reboot** in the confirmation dialog box.

Deleting an Offline AP

Aruba Central allows you to delete an offline access point (AP) from the AP List page. When you delete an offline AP from the **Access Points** table, the AP is removed from the assigned groups, labels, and sites. However, the AP is still available in the **Device Inventory** and the assigned subscription is not revoked.

To delete an offline access point (AP), complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. In the **Access Points** table, hover over the offline AP that you want to delete.
4. Click the delete icon.

NOTE

To delete multiple offline APs, select the offline APs that you want to delete and click the delete icon.

5. Click **Delete** in the confirmation dialog box.

AP Live Events

Aruba Central allows you to troubleshoot issues related to access points. The AP Live events feature is similar to client live troubleshooting, but in this case, we can enable live events at the AP level. Currently users can subscribe to Radio, VPN, and Spectrum events.

NOTE

The Instant AP must be running Aruba Instant 8.5.0.0 or later versions to support this feature.

Troubleshooting an AP

Aruba Central allows you to troubleshoot issues related to an AP in real time for detailed analysis.

To troubleshoot an AP at the device level, perform the following steps:

1. In the **Network Operations** app, select an AP from the **Device** list.

   The dashboard context for the selected AP is displayed.
2. Under **Analyze**, click **Live Events**.The **Live Events** page is displayed.

The live troubleshooting session starts automatically. The status of the troubleshooting is displayed every minute. The troubleshooting session runs for a duration of 15 minutes. You can stop live troubleshooting at any point by clicking **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.

- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

Thermal Shutdown Support in IAP

Aruba AP-555 and AP-535 Instant Access Point(IAP) devices are equipped with an internal thermal sensor. The sensor initiates a shutdown when the operating temperature crosses the temperature threshold recommended for an IAP. When an IAP operates under thermal management, all the radios are in **Disabled** mode in the AP Health Bar.

- In swarm mode, the thermal shutdown support is as follows:
  - In swarm mode, when the member IAP operates beyond the recommended temperature threshold, the Virtual AP profile is disabled. Once the member IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message, and then reconnects with the virtual controller. This process of reboot and reconnection is executed for five times. If the connection between the member IAP and the virtual controller does not restore after five times, the member IAP remains in the shutdown state until it is manually turned on.
  - In swarm mode, when the conductor IAP operates beyond the recommended temperature threshold, it reboots with the **Reboot due to Thermal Management** message. Once the conductor IAP attains the optimum temperature again, it turns into a member IAP, reboots with the **Recovery from Thermal Management Mode** message, and then reconnects with the virtual controller. This process of reboot and reconnection is executed for five times. If the connection between the member IAP and the virtual controller does not restore after five times, the member AP remains in the shutdown state until it is manually turned on.
  - In swarm mode, when the conductor IAP operates beyond the recommended temperature threshold and the number of IAPs is one in the swarm scale, the Virtual AP profile is disabled. Once the conductor IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message. This process of reboot is executed for five times. If the conductor IAP does not reboot after five times, the conductor IAP remains in the shutdown state until it is manually turned on.
- In standalone mode, when the IAP operates beyond the recommended temperature threshold, the Virtual AP profile is disabled. Once the IAP attains the optimum temperature again, it reboots with the **Recovery from Thermal Management Mode** message. This process of reboot is executed for five times. If the IAP does not reboot after five times, it remains in the shutdown state until it is manually turned on.

Thermal Shutdown Events

To view the thermal shutdown events, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**.

        A list of access points is displayed in the **List** view.

c. Click an access point listed under **Device Name**.

The dashboard context for the access point is displayed.

2. Under **Analyze**, click **Alerts & Events**.

   The **Alerts & Events** page is displayed in the **List** view.

3. Click the **Events** tab.

   A list of events is displayed in the **Events** table.

When the thermal shutdown feature is either enabled or disabled in an IAP, the **Events** table displays the following details:

- The **Event Type** column includes the **AP Thermal Shutdown** type which can be used to filter thermal shutdown events.
- The **Description** column includes the status of the thermal shutdown feature in the IAP. For example, **Thermal management enabled** or **Thermal management disabled**.

In Aruba Central, the thermal shutdown feature is supported on IAPs running Aruba Instant 8.6.0.0 or later versions.

About Tri-Radio Mode

Aruba Central supports tri-radio mode in Aruba AP-555, a flagship 802.11ax access point (AP). In tri-radio mode or split 5 GHz mode, the 8x8 5 GHz radio is split into two independent 4x4 5 GHz radios. In the tri-radio mode, the **5GHz Band** operates on channels from 36 to 64 and **Second 5GHz Radio** operates on channels from 100 to 165.

The split 5 GHz radio can operate in the following modes:

- Access
- Monitor
- Spectrum

Enabling Tri-Radio Mode

To enable the tri-radio mode, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the filter selected contains at least one active access point.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.

   - To select an access point in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.

     c. Click an access point listed under **Device Name**.

        The dashboard context for the access point is displayed.

d. Under **Manage**, click **Devices** > **Access Point**.

2. Click the **Config** icon.
   The tabs to configure access points are displayed.
3. Click the **Access Points** tab.
   The **Access Points** page is displayed.
4. To edit an AP, select an AP in the **Access Points** table, and then click the edit icon.
5. Click **Radio**.
6. Select the **Split Radio** check-box.
7. Click **Save Settings**.

Viewing Tri-Radio Events

To view the tri-radio events, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**.
        A list of APs is displayed in the **List** view.
     c. Click an AP listed under **Device Name**.
        The dashboard context for the AP is displayed.
2. Under **Analyze**, click **Alerts & Events**.
   The **Alerts & Events** page is displayed in the **List** view.
3. Click the **Events** tab.
   A list of events is displayed in the **Events** table.

When the tri-radio mode is either enabled or disabled in an AP, the **Events** table displays the following details:

- The **Event Type** column includes the **AP Tri-Radio** type, which can be used to filter tri-radio events.
- The **Description** column includes the status of the tri-radio mode in AP.

In Aruba Central, the tri-radio mode feature is available only on AP-555, running Aruba Instant 8.6.0.0 or later versions. By default, the AP-555 operates in dual radio mode.

Access Point > Overview > Summary

In the access point (AP) dashboard, the **Summary** tab displays the device details, network information, radio details including the topology of clients connected to each radio, and the health status of the AP in the network.

The AP Details page is available for Foundation and Advanced licenses for APs.

The **Summary** tab displays the following sections:

- Device
- Network
- Radios
- Data Path
- Health Status
- WLANS
- Actions
- Go Live

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The **Summary** tab is displayed.

   To exit the AP dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Device

The **Device** section displays the following details:

- **AP Model**—The AP hardware model.
- **Country Code**—Country code in which the AP operates.
- **MAC**—MAC address of the AP.
- **Serial Number**—Serial number of the AP.
- **Uptime**—Time from when the AP is operational.

The **Uptime** does not reflect the time from when the AP is connected to Aruba Central.

- **Last Reboot Reason**—The reason for the latest rebooting of AP.
- **Firmware Version**—The firmware version running on the AP. If the device is running an older firmware version, this field prompts the user to upgrade to the latest firmware version along with the link to the **Maintenance** > **Firmware** page.
- **Configuration Status**—Displays the configuration status and the timestamp of the last device configuration changes.
- **Band Selection**—Displays the operating band of the AP. The supported bands are **Dual Band**, **Dual 5 GHz**, or **Tri-Radio**.
- **Power Draw**—The power utilized by the device in watts (W) or kilowatts (kW). For more information on the list of APs that support power draw, see Supported Instant APs.

- **Power Negotiation**—The power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Recommended Power**—The recommended power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Group**—The group to which the AP belongs. Click the group name to go to the **Overview** > **Summary** page for that group.

NOTE

When an AP belongs to an unprovisioned group, the hyperlink to the unprovisioned group is disabled.

- **Labels**—The labels associated with the AP. You can also add a new label to the AP by clicking the edit icon. To view all the labels associated with a device, hover your mouse over the **Labels** column.
- **LEDs on ACCESS POINT**—Click **Blink LED** to enable the blinking of LEDs on the AP to identify the location. The default blinking time is set to 5 minutes and it stops automatically after 5 minutes. To stop the blinking of the AP, click **Stop Blinking**.
- **Site**—The site to which the AP belongs. Click the site name to go to the **Overview** > **Site Health** page for that site.
- **Note**—When you click the edit icon, a text-box is displayed. It allows you to add information that can be used as reference. For example, AP location, and upgrade information.

Network

The **Network** section displays information of the network and interfaces to which the AP is connected. Along with the network profile name, the following fields are displayed in the **Network** section:

- **ETH0**—Displays the status of the ETH0 network.
- **Speed (Mbps)/Duplex**—The speed of the network measured in Mbps. This field also indicates whether the network has a full-duplex or half-duplex communication.
- **VLAN**—The number of VLAN connections associated with the network.
  - **LLDP Details**—Click the **LLDP Details** link to view the ETH0 LLDP details. The pop-up window displays the **Neighbor Name**, **Neighbor MAC**, **Neighbor Port**, and **Neighbor VLAN** details.

NOTE

In Aruba Central, all the LLDP details are supported on APs running Aruba Instant 8.6.0.3 or later versions.

- **ETH1**—Displays the status of the ETH1 network.
- **Speed (Mbps)/Duplex**—The speed of the network measured in Mbps. This field also indicates whether the network has a full-duplex or half-duplex communication.
- **VLAN**—The number of VLAN connections associated with the network.
  - **LLDP Details**—Click the **LLDP Details** link to view the ETH1 LLDP details. The pop-up window displays the **Neighbor Name**, **Neighbor MAC**, **Neighbor Port**, and **Neighbor VLAN** details.
- **Current Uplink**—The current uplink connection on the AP.
- **Uplink connected to**—The switch name to which the AP is connected. Click this link to view the switch details page, if the switch is managed by Aruba Central. For more information, see Switch > Overview > Summary.
  - **Port**—The port number of the switch to which the AP is connected.
- **IP Address**—IP address of the AP.
- **Public IP Address**—IP address logged by servers when the AP device is connected through internet connection.

- **DNS Name Servers**—The server that has a directory of domain names and their associated IP addresses.
- **Default Gateway**—A 32 bit value that is used to uniquely identify the device on a public network.
- **NTP Server**—Displays information about the NTP Server.

Radios

The **Radios** section displays the following information related to **Radio 2.4 GHz**, **Radio 5 GHz**, and **Radio 5 GHz Secondary**:

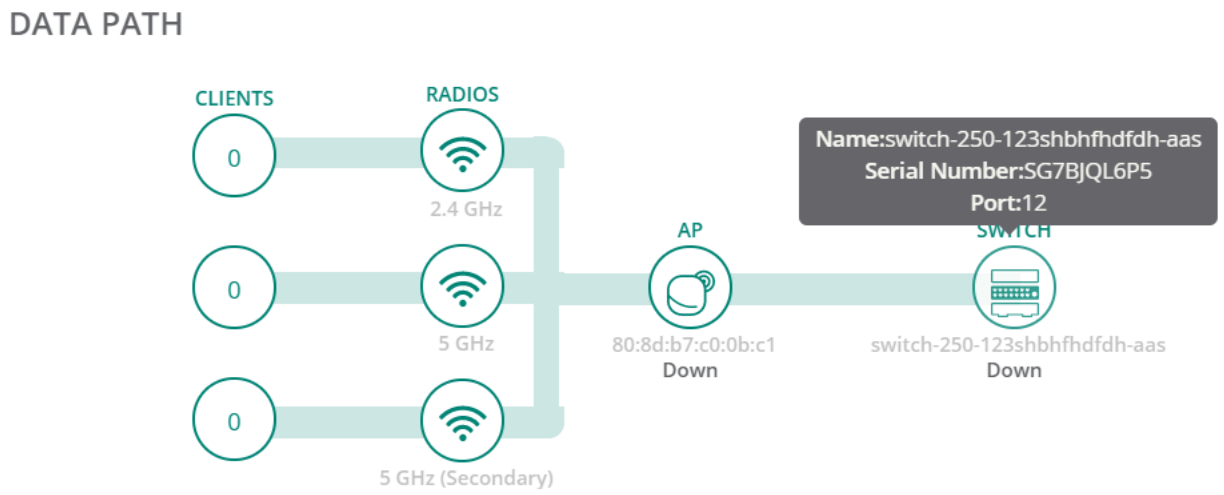
- **Mode**—The type of mode for the radios. For example, Client Access, Monitor, and Spectrum.
- **Status**—Displays the operational status of the radios connected to the AP. The status is as follows:
  - **Up**—Indicates that the radio is online.
  - **Down**—Indicates that the radio is offline.
  - **Down - Thermal shutdown**—Indicates that the radio is offline as the AP is operating under thermal management. For more information, see Thermal Shutdown Support in IAP.
- **Radio MAC Address**—The MAC address of the radios connected to the AP.
- **Channel**—The channels assigned to the radios.
- **Power**—The transmit power of the radios.
- **Type**—The type of wireless LAN used for the radios.
- **Clients**—The number of clients connected to the AP.
- **Wireless Networks**—The number of SSIDs configured in the network.
- **Antenna**—The type of antennae. For example, internal and external.
- **Spatial Stream**—Displays the number of spatial streams. By default, the spatial stream value for **Radio 5 GHz** is 8x8. When tri-radio mode is enabled, the spatial stream values for **Radio 5 GHz** and **Radio 5 GHz (Secondary)** is 4x4.

- When the AP radios are set to spectrum scan mode, the **Channel** and **Power** values are empty.
- The tri-radio feature is available only for AP-555. In the **Radios** section, the **Radio 5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.

Data Path

The **Data Path** section displays the topology of clients connected to each of the radios of the AP, which in turn is connected to switches or gateways through VLAN. When you hover over the upstream device in the data path topology, a pop-up displays the **Name**, **Serial Number**, and **Port** details of the upstream devices.

Figure 140 *Data Path*



NOTE

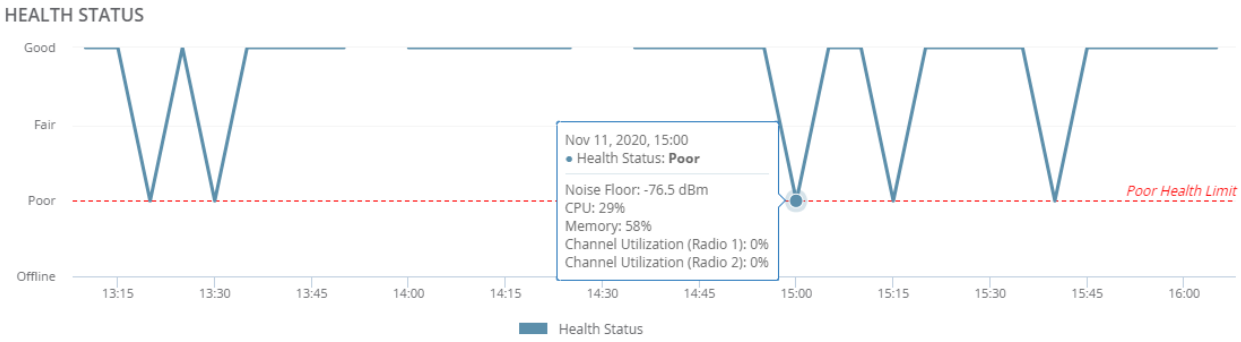
The tri-radio feature is available only for AP-555. In the **Data Path** section, the **5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.

Health Status

The **Health Status** trend graph indicates the health status of the device in the network for the time specified in the time range filter. When you hover the graph, you can view information such as date and time, **Health Status**, **Noise Floor**, **CPU**, **Memory**, **Channel Utilization (Radio 1)**, **Channel Utilization (Radio 2)**, and **Channel Utilization (Radio 3)**.

In the **Health Status** graph, the **Poor Health Limit** text indicates the poor health limit of the device in the network.

Figure 141 *Health Status*



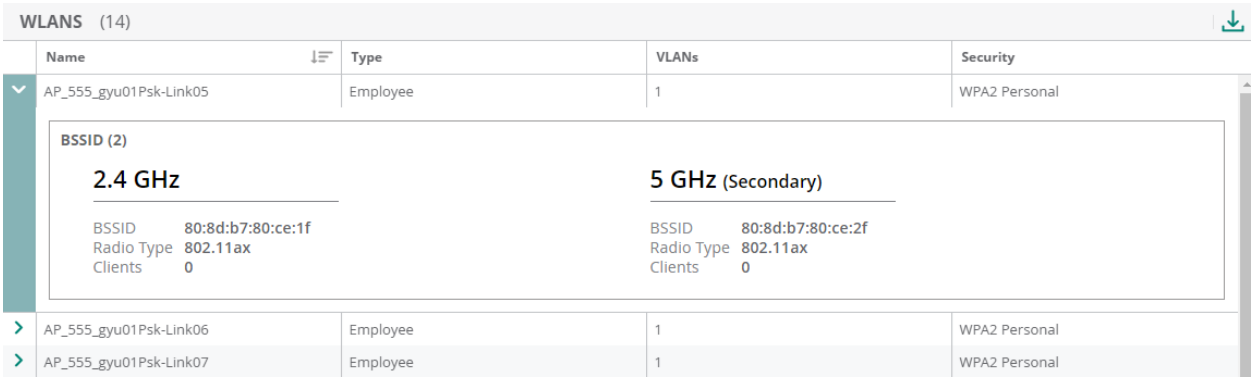
NOTE

The tri-radio feature is available only for AP-555. In the **Health Status** graph, the **Channel Utilization (Radio 3)** data is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.

WLANS

The **WLANS** table provides a list of all the SSIDs configured for the AP.

Figure 142 *WLANS*



The **WLANS** table provides the following information:

- **Name**—Displays the name of the SSID.
- **Type**—Displays the type of the SSID.
- **VLANs**—Displays the VLAN number.
- **Security**—Displays the type of security.

Click › to expand an SSID in the **WLANS** table. When you expand an SSID in the **WLANS** table, you can view the following information for **2.4 GHz**, **5 GHz**, and **5 GHz (Secondary)** radios:

- **BSSID**—Displays the MAC address of the radio.
- **Radio Type**—Dispalys the type of radio.
- **Clients**—Dispalys the number of connected clients.

Click to download the **.csv** file of the **WLANS** table.

NOTE

- In the **.csv** file of the **WLANS** table, the **5 GHz (Secondary)** columns are available only if the tri-radio mode is enabled.
- The tri-radio feature is available only for AP-555. In the **WLANS** table, the **5 GHz (Secondary)** data is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see Rebooting an IAP.
- **Reboot Swarm**—Reboots the AP cluster. For more information, see Rebooting an IAP Cluster .
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see Tech Support for an IAP .
- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see Opening a Remote Console.

Go Live

Aruba Central supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see Enabling Live IAP Monitoring.

Access Point > Overview > AI Insights

In the access point (AP) dashboard, the **AI Insights** tab displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization.

Viewing Access Points > AI Insights

To navigate to the **AI Insights** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **AI Insights** tab.

   The **Insights** page is displayed.

   To exit the AP dashboard, click the back arrow on the filter.

   You can change the time range for the **AI Insights** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** ( ) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

- Red—High priority
- Orange—Medium priority
- Yellow—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. Each insight report provides specific details on the occurrences of these events for ease in debugging. For more information, see The AI Insights Dashboard.

The AP **AI Insights** page displays the following insights:

- Telemetry Information not Received from APs or Radios
- Access Points with High CPU Utilization
- Access Points with High Memory Usage
- Access Points with High Number of Reboots
- Clients with High Roaming Latency
- Clients who Roamed Excessively
- Delayed DNS Request or Response
- DNS Servers Rejected High Number of Queries

- DNS Queries Failed to Reach or Return from the Server
- Clients with High MAC Authentication Failures
- Clients with High 802.1X Authentication Failures
- Clients with High Wi-Fi Security Key-Exchange Failures
- Clients with High Number of Wi-Fi Association Failures
- Clients with Captive Portal Authentication Problems
- Access Points Impacted by High 2.4 GHz Usage
- Access Points Impacted by High 5 GHz Usage
- Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz
- Clients with Low SNR Minutes
- Access Points with Excessive Number of Channel Changes
- Access Points Radios with Frequent Transmit Power Changes

Access Point > Overview > Floor Plan

In the access point (AP) dashboard, the **Floor Plan** tab provides information regarding the current location of the Instant Access Point (IAP).

Viewing the Overview > Floor Plan Tab

To navigate to the **Floor Plan** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Floor Plan** tab.

   The **Floor Plan** tab is displayed.

   To exit the AP dashboard, click the back arrow on the filter.

   You can change the time range for the **Floor Plan** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

The **Floor Plan** tab displays a sitemap and the floor plan showing the current location of the IAP . The sitemap is derived from the Visual RF application, if Visual RF service is enabled for the Aruba Central account. You can also edit the location of the IAP device by clicking the edit icon provided next to the address in the **Floor Plan** tab.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see Rebooting an IAP.
- **Reboot Swarm**—Reboots the AP cluster. For more information, see Rebooting an IAP Cluster .

- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see Tech Support for an IAP .
- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see Opening a Remote Console.

Go Live

Aruba Central supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see Enabling Live IAP Monitoring.

Access Point > Overview > Performance

In the access point (AP) dashboard, the **Performance** tab displays the size of data transmitted through the AP.

Viewing the Overview > Performance Tab

To navigate to the **Performance** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Performance** tab.

   The **Performance** tab is displayed.

To exit the AP dashboard, click the back arrow on the filter.

You can change the time range for the **Performance** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

The **Performance** tab provides the following details:

- **Throughput**

  The **Throughput** graph indicates the size of data sent to and received by the device in bits per second for the wired or wireless networks. For example, Eth 0 or Eth 1 wired network profiles and specific SSIDs of wireless networks. You can also view data for all the wireless SSIDs by selecting **All SSIDS** from the drop-down list. You can view the overall data usage measured in bytes in the **Overall Usage** field.
- **Clients**

  The **Clients** graph indicates the number of clients connected to the device for a selected time range in the time range filter. You can select a specific SSID or all SSIDs, Eth 0, or Eth 1 from the drop-down list provided in the **Clients** section.

When you hover over the **Throughput** and **Quality** graphs, it displays specific data for the selected timestamp.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the access point. For more information, see Rebooting an IAP.
- **Reboot Swarm**—Reboots the AP cluster. For more information, see Rebooting an IAP Cluster .
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the access point. For more information, see Tech Support for an IAP .
- **Console**—Opens the remote console for a CLI session through SSH for an access point. For more information, see Opening a Remote Console.

Go Live

Aruba Central supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see Enabling Live IAP Monitoring.

Access Point > Overview > RF

In the access point (AP) dashboard, the **RF** tab provides details corresponding to 2.4 GHz, 5 GHz, and 5 GHz Secondary radios of the AP.

Viewing the Overview > RF Tab

To navigate to the **RF** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **RF** tab.

   The **RF** tab is displayed.

   To exit the AP dashboard, click the back arrow on the filter.

   You can change the time range for the **RF** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

The **RF** tab provides the following graphs corresponding to **2.4 GHz** and **5 GHz** radio channels of the AP:

- Channel Utilization
- Noise Floor
- Frames - 802.11
- Channel Quality

Channel Utilization

The **Channel Utilization** graph indicates the percentage of channel utilization for the selected time range from the time range filter. The channel utilization information is categorized as follows:

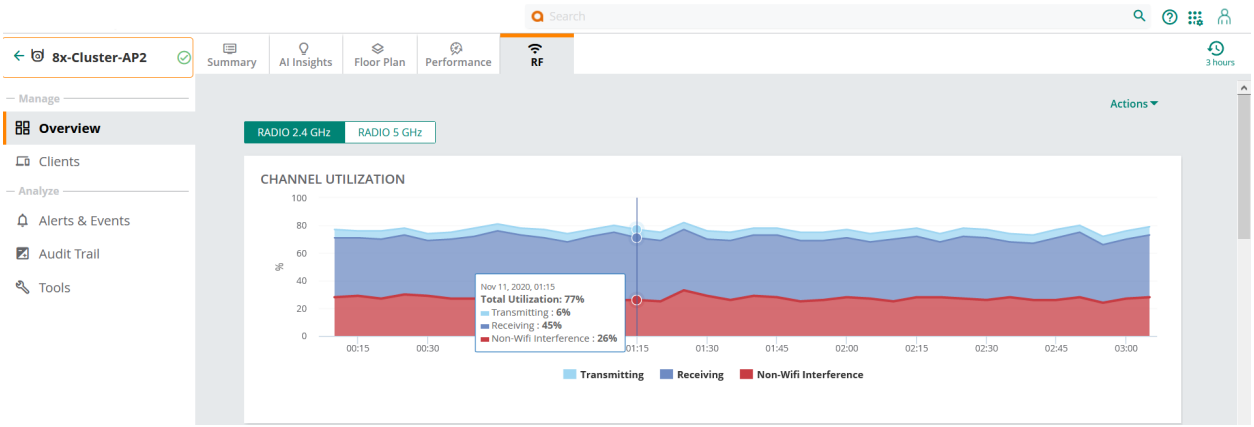
- **Transmitting**—The percentage of channel currently being transmitted.
- **Receiving**—The percentage of channel currently being received.
- **Non-Wifi Interference**—The percentage of channel currently being used by non-Wi-Fi interferers.

NOTE

Total Utilization is the sum of **Transmitting**, **Receiving**, and **Non-Wifi interference**, which indicates the total percentage of channel utilization for the selected time range.

The following figure displays the channel utilization graph for 2.4 GHz radio channel:

Figure 143 *Channel Utilization Graph*



Noise Floor

The **Noise Floor** graph indicates the noise floor detected in the network to which the device belongs.

Frames - 802.11

The **Frames - 802.11** line graph indicates the trend of frames transmitted through the network. The frames can be one of the following types: **Drops**, **Errors**, and **Retries**. The graph indicates the status of data frames that were dropped, encountered errors, retried to be transferred, in a wireless network.

Channel Quality

The **Channel Quality** graph indicates the quality of channel in percentage.

NOTE

- When you hover over the **Channel Utilization**, **Noise Floor**, **Frames - 802.11**, and **Channel Quality** graphs, it displays specific data for the selected timestamp.
- The tri-radio feature is available only for AP-555. In the **RF** tab, the **Radio 5 GHz (Secondary)** tab is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see Rebooting an IAP.
- **Reboot Swarm**—Reboots the AP cluster. For more information, see Rebooting an IAP Cluster.
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see Tech Support for an IAP.

- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see Opening a Remote Console.

Go Live

Aruba Central supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see Enabling Live IAP Monitoring.

Access Point > Overview > Spectrum

In the access point (AP) dashboard, the **Spectrum** tab provides details for all Wifi and non-Wifi devices associated to each radio.

When the radios of Instant Access Point(IAP) are set to spectrum scan mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring IAPs or interfering devices such as microwaves and cordless phones. To enable the spectrum scan feature on a specific radio of an AP, see Access Points Configuration Parameters.

The spectrum scan feature is available only on IAP devices running Aruba Instant 8.5.0.1 firmware version and later.

When the spectrum scan feature is enabled, the IAP does not provide services to clients. The **Spectrum** tab displays the following sections:

- Channel Utilization and Quality
- Interfering Devices
- Actions
- Go Live

Viewing the Overview > Spectrum Tab

To navigate to the **Spectrum** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the AP dashboard context, click the **Spectrum** tab.

   The **Spectrum** tab is displayed.

   To exit the AP dashboard, click the back arrow on the filter.

   You can change the time range for the **Spectrum** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Channel Utilization and Quality

Click the **Chart** icon to view the **Channel Utilization and Quality** details corresponding to **2.4 GHz** and **5 GHz** radios of the AP. Click the **2.4 GHz** and **5 GHz** tabs on the **Channel Utilization and Quality** label to

view the **Channel Utilization** and **Quality** graphs for the radios.

- **Channel Utilization**—The **Channel Utilization** graph indicates the percentage of channel utilization for the **Available**, **Interference**, and **Wi-Fi Utilization** categories associated to **2.4 GHz** and **5 GHz** radios. You can view the following channel metrics when you hover over the **Channel Utilization** bar graph:

Table 169: *Channel Utilization Metrics*

Metrics	Description
Channel	The channel number of the radio.
Available	The percentage of the channel currently available for use.
Interference	The percentage of the channel currently being used by interfering devices.
Microwave	The percentage of the channel currently being used by microwaves. Common residential microwave ovens with a single magnetron are classified as a Microwave. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.
Bluetooth	The percentage of the channel currently being used by bluetooth devices. Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a Bluetooth device. Bluetooth uses a frequency hopping protocol.
Cordless Phone	The percentage of the channel currently being used by cordless phones.
Wi-Fi Utilization	The percentage of the channel currently being used by Wi-Fi devices.

- **Quality**—The **Quality** graph display the channel quality corresponding to each of the WiFi and non-WiFi devices connected to the radios. When you hover over the **Quality** bar graph, the following channel metrics are displayed:

Table 170: *Channel Quality Metrics*

Metrics	Description
Channel	The channel number of the radio.
Quality	Current relative quality of the channel.
Known APs	Number of valid Instant APs identified on the radio channel.
Unknown APs	Number of invalid or rogue Instant APs identified on the radio channel.
Max AP Signal	Signal strength of the Instant AP that has the maximum signal strength on a channel in dBm.
Max Interference	Signal strength of the non-Wi-Fi device that has the highest signal strength in dBm.

Metrics	Description
Max AP SSID	The network SSID with maximum APs.
Max AP BSSID	The network SSID with maximum APs.
SNIR	The measure of SNIR detected in the network in dB.
Noise Floor	The noise at the radio receivers of the radios.

Interfering Devices

Click the **List** icon to view **Interfering Devices** details detected by the spectrum scanner. The page displays a table with following details of interfering devices:

Table 171: *Interfering Devices Table*

Metrics	Description
Type	Device type. This parameter can be any of the following: ■ Audio FF (fixed frequency) ■ Bluetooth ■ Cordless base FH (frequency hopper) ■ Cordless phone FF (fixed frequency) ■ Cordless network FH (frequency hopper) ■ Generic FF (fixed frequency) ■ Generic FH (frequency hopper) ■ Generic interferer ■ Microwave ■ Microwave inverter ■ Video ■ Xbox
ID	ID number assigned to the device by the spectrum monitor. Spectrum monitors assign a unique spectrum ID per device type.
Central Frequency	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device in KHz.
Affected Channels	Radio channels affected by the wireless device.
Signal Strength	Strength of the signal sent from the device measured in dBm.
Duty Cycle	The device duty cycle. This value represents the percent of time the device broadcasts a signal.
First Seen	Time at which the device was first detected.
Last Seen	Time at which the device status was updated.

NOTE

The data displayed in the **Spectrum** tab is refreshed every 15 seconds. Aruba Central displays the last recorded data for 30 minutes, if the device turns offline.

Actions

The **Actions** drop-down list contains the following options:

- **Reboot AP**—Reboots the AP. For more information, see Rebooting an IAP.
- **Reboot Swarm**—Reboots the AP cluster. For more information, see Rebooting an IAP Cluster .
- **Tech Support**—Enables the administrator to generate a tech support dump required for troubleshooting the AP. For more information, see Tech Support for an IAP .
- **Console**—Opens the remote console for a CLI session through SSH for an AP. For more information, see Opening a Remote Console.

Go Live

Aruba Central supports live monitoring of IAPs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data of an AP updated at every 5 seconds. For more information, see Enabling Live IAP Monitoring.

Access Point > Security > VPN

The **VPN** tab provides information on VPN connections associated with the virtual controller along with information on the tunnels and the data usage through each of the tunnels.

Viewing the Security > VPN Tab

To navigate to the **VPN** tab, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of AP is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. Under **Manage**, click **Security** > **VPN**.

   The **VPN** tab is displayed.

   You can change the time range for the **VPN** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

The **VPN** tab provides the following information:

- **VPNC Tunnels Summary**—The section displays information on tunnels with the following details:
  - **Total**—Total tunnels established.
  - **Up**—Number of tunnels currently active.
  - **Down**—Number of tunnels currently inactive.
  - **Peers**—Number of peer tunnels currently active.

The **Tunnel** table displays information on tunnels with the following columns:

- **Tunnel**—The type of the tunnels used in the VPN. For example, primary, secondary, or backup.
- **Status**—The status of the tunnel.
- **Source**—The source address of the tunnel.
- **Destination**—The destination address of the tunnel.

- **Throughput Usage Per VPN**—The **Throughput Usage Per VPN** graph indicates the successful data usage per VPN in Mbps for the primary or backup tunnel selected from the drop-down list. The **Throughput Usage Per VPN** displays a linear graph of sent and received data in the virtual private network.

Rebooting an IAP

You can reboot an Instant Access Point (IAP) using the Aruba Central UI.

To reboot an IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Reboot AP**.

   A **Reboot** dialog box is displayed.
5. Click **Reboot** to reboot the AP.

The AP dashboard takes less than a minute to update the interface status, after the AP is rebooted and reconnected to Aruba Central.

Rebooting an IAP Cluster

You can reboot an Instant Access Point (IAP) cluster using the Aruba Central UI.

To reboot an IAP cluster, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Reboot Swarm**.

   A **Reboot** dialog box is displayed.

5. Click **Yes** to reboot the AP cluster.

The AP dashboard takes less than a minute to update the interface status, after the VC is rebooted and reconnected to Aruba Central.

Tech Support for an IAP

In Aruba Central UI, the administrators can generate a tech support dump required for troubleshooting the Instant Access Point (IAP).

To generate a tech support dump for an IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Tech Support**.

   The **Commands** page is displayed. In the **Commands** page, the **Device Type** and **Available Devices** fields are automatically selected. The `AP Tech Support Dump` command is automatically selected in the **Selected Commands** pane.
5. Click **Run**. The output is displayed in the **Device Output** section.

For more information, see Troubleshooting Access Points.

Opening a Remote Console

In the Aruba Central UI, you can open the remote console for a CLI session through SSH for an Instant Access Point (IAP). You can reset the system configuration of an IAP by erasing the existing configuration on the IAP.

Resetting an IAP through the Console

To reset an IAP through the **Console**, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. In the **Actions** drop-down list, click **Console**.

   A CLI session dialog box is displayed.

5. Execute the `write erase all` command in the command prompt.
6. Reboot the IAP.

   In this procedure, the complete configuration including the **Per AP Settings** on the IAP is reset. After the reboot, the IAP is moved to default group and will not be present in the group to which it was previously attached.

Enabling Live IAP Monitoring

Aruba Central supports live monitoring of Instant Access Points (IAPs) that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data of an IAP updated at every 5 seconds.

Enabling and Disabling Go Live

To enable and disable the live monitoring of an IAP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. Click the **Go Live** button to start live monitoring of the AP.
5. Click the **Stop Live** button to exit live monitoring of the AP.

- The **Go Live** feature is not applicable for offline IAPs. The **Go Live** button remains grayed-out for all the APs that are not associated with IAP devices running Aruba Instant 8.4.0.0 firmware version and above.
- Aruba Central allows you to monitor live data for 15 minutes. After this time period, Aruba Central redirects to the AP dashboard in a non-live mode to display the monitoring details for the time selected in the **Time Range Filter**. For more information on AP dashboard in a non-live mode, see Access Point > Overview > Summary.

AP Details in Go Live Mode

When you click the **Go Live** button, the page displays live graphs based on noise floor, frames, and channel quality of the neighboring RF devices for 15 minutes, until you select **Stop Live** button.

The page displays **Noise Floor**, **Frames**, and **Channel Quality** live graphs for **Radio 2.4 GHz**, **Radio 5 GHz**, and **Radio 5 GHz Secondary** radios.

Important Information

- The Go Live feature is not applicable for offline APs.
- Aruba Central allows you to monitor live data for 15 minutes. After this time period, Aruba Central redirects to the AP dashboard in a non-live mode to display the monitoring details for the time selected in the **Time Range Filter**. For more information on AP dashboard in a non-live mode, see Access Point > Overview > Summary.

- In **Go Live** mode, AP dashboard updates and displays data at every 5 seconds.
- The tri-radio feature is available only for AP-555. In the **Go Live** page, the **Radio 5 GHz (Secondary)** tab is available only if the tri-radio mode is enabled. For more information, see About Tri-Radio Mode.
- The time range selected in the **Time Range Filter** is not applicable when the **Go Live** button is enabled.
- You can monitor live data for multiple APs simultaneously on different tabs.

AP Live Events

Aruba Central allows you to troubleshoot issues related to access points. The AP Live events feature is similar to client live troubleshooting, but in this case, we can enable live events at the AP level. Currently users can subscribe to Radio, VPN, and Spectrum events.

The Instant AP must be running Aruba Instant 8.5.0.0 or later versions to support this feature.

Troubleshooting an AP

Aruba Central allows you to troubleshoot issues related to an AP in real time for detailed analysis.

To troubleshoot an AP at the device level, perform the following steps:

1. In the **Network Operations** app, select an AP from the **Device** list.
   The dashboard context for the selected AP is displayed.
2. Under **Analyze**, click **Live Events**.The **Live Events** page is displayed.

The live troubleshooting session starts automatically. The status of the troubleshooting is displayed every minute. The troubleshooting session runs for a duration of 15 minutes. You can stop live troubleshooting at any point by clicking **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

Access Point > Clients > Clients

In the access point (AP) dashboard, the **Clients** tab displays details of all the clients connected to a specific AP.

Viewing the Access Point > Clients > Clients Tab

To navigate to the **Clients** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.
   The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in the **List** view.

   To exit the Clients dashboard, click the back arrow on the filter.

   You can change the time range for the **Clients** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

   For more information, see All Clients.

Access Point > Alerts & Events > Alerts & Events

In the access point (AP) dashboard, the **Alerts & Events** tab displays details of the alerts and events generated for the AP.

Viewing the Access Point > Alerts & Events > Alerts & Events Tab

To navigate to the **Alerts & Events** tab in the AP dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active AP.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   A list of APs is displayed in the **List** view.
3. Click an AP listed under **Device Name**.

   The dashboard context for the AP is displayed.
4. Under **Analyze**, click **Alerts & Events**.

   The **Alerts & Events** page is displayed in the **List** view.

   To exit the Alerts & Events dashboard, click the back arrow on the filter.

- For more information, see Alerts & Events.
- You can also configure and enable certain categories of Instant AP alerts. For more information, see Access Point Alerts.

Chapter 9
AOS-CX Overview

AOS-CX is a modern and fully programmable operating system built using a database-centric design, which ensures higher availability and dynamic software process changes for reduced downtime. In addition to robust hardware reliability, the AOS-CX operating system includes additional software elements not available with traditional systems, including:

- Automated visibility to help IT organizations scale
- Simplified programmability
- Faster resolution with network insights
- High availability
- Ease of roll-back to previous configurations

The AOS-CX operating system is a modular, database-centric operating system. Every aspect of the switch configuration and state information is modeled in the AOS-CX switch configuration and state database, including configuration information, status of all features, and network analytics. The AOS-CX operating system also includes a time series database, which acts as a built-in network record. The time series database makes the data seamlessly available to Aruba Network Analytics Engine agents that use rules that evaluate network conditions over time.

Aruba Central offers a cloud-based management platform for managing AOS-CX infrastructure. It simplifies switch management with flexible configuration options, monitoring dashboards, and troubleshooting tools.

- Getting Started with AOS-CX Deployments
- Provisioning Factory Default AOS-CX Switches
- Provisioning Pre-Configured AOS-CX Switches
- Using Configuration Templates for AOS-CX Switch Management
- Configuring AOS-CX Switches in UI Groups
- Configuration Workflow for AOS-CX Switches in UI Groups
- Limitations of AOS-CX Switch in Aruba Central

Supported AOS-CX Platforms

To manage your AOS-CX switches using Aruba Central, ensure that the switch software is upgraded to 10.05.0021 or a later version. AOS-CX switches with version 10.05.0021 or earlier might not connect to Aruba Central after ten days of operation. You must upgrade the AOS-CX switch to a recommended software version to connect to Aruba Central.

The following table lists the AOS-CX platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 172: *Supported AOS-CX Switch Series, Software Versions, and Switch Stacking*

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type	Maximum Number of Stack Members	Supported Configuration Group Type (UI / Template)
AOS-CX 6100 Switch Series	10.06.0110 or later	10.06.0110	-N/A-	-N/A-	-N/A-	Template only
AOS-CX 6200 Switch Series	10.05.0021	10.06.0101	Yes **Switch Software Dependency**: 10.05.0021	VSF	8	UI and Template
AOS-CX 6300 Switch Series	10.05.0021	10.06.0101	Yes **Switch Software Dependency**: 10.05.0021	VSF	10	UI and Template
AOS-CX 6300 Switch Series [JL762A] Back 2 Front Power Supply SKU only	10.06.0001 or later	10.06.0101	Yes **Switch Software Dependency**: 10.05.0021	VSF	10	UI and Template
AOS-CX 6405 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	Template only
AOS-CX 6410 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	Template only
AOS-CX 8320 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8325 Switch Series	10.05.0021	10.06.0101	-N/A-	-N/A-	-N/A-	UI and Template
AOS-CX 8360 Switch Series	10.06.0001 or later	10.06.0101	-N/A-	-N/A-	-N/A-	UI and Template

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type	Maximum Number of Stack Members	Supported Configuration Group Type (UI / Template)
AOS-CX 8400 Switch Series	10.06.0001 or later	10.06.0101	-N/A-	-N/A-	-N/A-	Template only

Provisioning and configuring of AOS-CX 6405, 6410, and 8400 switch series and switch stacks is supported only through configuration templates.

Data sheets and technical specifications for the supported switch platforms are available at: https://www.arubanetworks.com/products/networking/switches/.

Getting Started with AOS-CX Deployments

Before you get started with your onboarding and provisioning operations, browse through the list of Supported AOS-CX Platforms in Aruba Central.

Provisioning Workflow

The following sections list the steps required for provisioning AOS-CX switches in Aruba Central.

Provisioning a Factory Default Switch

Like most Aruba devices, AOS-CX switches support ZTP. Switches with factory default configuration have very basic configuration for all ports in VLAN-1. When a new AOS-CX switch (factory default) is powered on, it automatically obtains IP address, connects to Aruba Activate and downloads the provisioning parameters. When the switch identifies Aruba Central as its management entity, it connects to Aruba Central.

To manage AOS-CX switches from Aruba Central, you must onboard the switches to the device inventory and assign a valid subscription.

For step-by-step instructions, see Provisioning Factory Default AOS-CX Switches.

Provisioning a Pre-configured or Locally-Managed Switch

Pre-configured switches have customized configuration; for example, an additional VLAN or static IP address configured on the default.

Aruba Central management service is enabled by default on AOS-CX switches. When the switch is powered on, it identifies Aruba Central as its management entity and connects to Aruba Central.

To manage AOS-CX switches from Aruba Central, you must onboard the switches to the device inventory and assign a valid subscription.

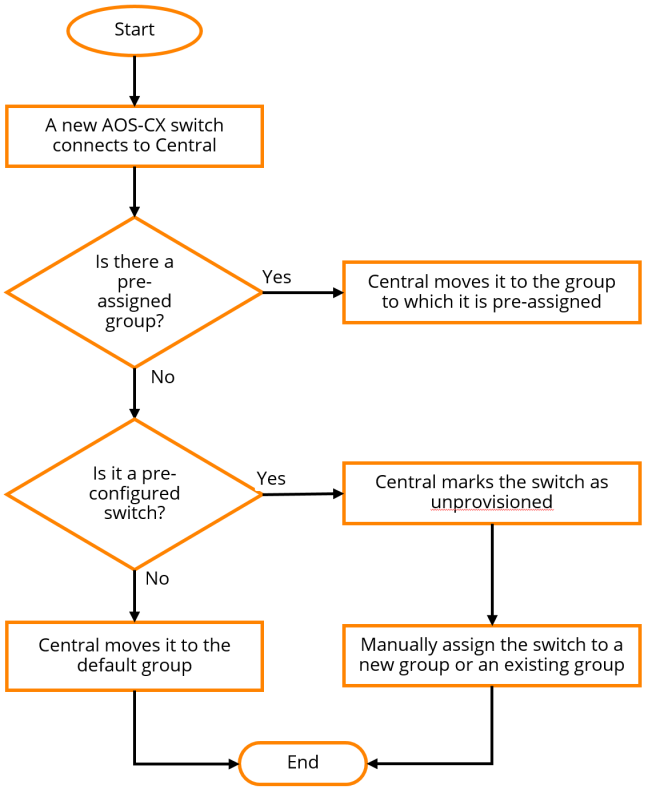
For step-by-step instructions, see Provisioning Pre-Configured AOS-CX Switches.

Group Assignment

Aruba Central supports provisioning AOS-CX switches in template groups. Template groups allow you to configure devices using CLI-based configuration templates.

The following figure illustrates the group assignment workflow in Aruba Central:

Figure 144 *Group Assignment- AOS-CX Switches*



Configuration and Management

Aruba Central supports managing AOS-CX switches configuration using configuration templates only. Ensure that you assign the AOS-CX switches to a template group.

When initially onboarding an AOS-CX switch to Aruba Central, you must manually create the template for the switch in a group, along with the password in plaintext format. You can use the output of the `show running-config` command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches.

For more information on managing AOS-CX switches in Aruba Central, see Using Configuration Templates for AOS-CX Switch Management.

AOS-CX Switch Monitoring

To view the operation status of switches and health of wired access network:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.

For more information, see Monitoring Switches and Switch Stacks.

NOTE

To view AOS-CX switches in the monitoring pages, you must create a template configuration for the switch with the password in plaintext. See Using Configuration Templates for AOS-CX Switch Management.

Viewing VSX Details

Aruba Central displays information about VSX configuration of AOS-CX switches. For more information, see Switch > VSX.

NOTE

Last synced data is displayed in the Switch > VSX page only when VSX synchronization is enabled for the AOS-CX switch. However, enabling VSX synchronization using template configuration in Aruba Central is not recommended. By enabling VSX synchronization, the peer switch may get into an unknown configuration state.

Viewing Topology Map

In Aruba Central, the **Topology** tab in the site dashboard provides a graphical representation of the site including the network layout, details of the devices deployed and health of the WAN uplinks and tunnels. Aruba Central supports AOS-CX switches to be displayed in the **Topology** tab. For more information, see Monitoring Sites in the Topology Tab.

NOTE

To view AOS-CX switches in the topology map, you must create a template configuration for the switch with the password in plaintext. See Using Configuration Templates for AOS-CX Switch Management.

Troubleshooting and Diagnostics

If you are unable to view all details of the AOS-CX switch, then maybe the template configuration was not applied correctly, the password was missing in the template configuration, or the password was not in plaintext. See the audit trail to check the status of the switch. The audit trail should show the device onboarded message for the switch serial number followed by the configuration push and login successful messages. For more information on troubleshooting AOS-CX switch onboarding issues, see Troubleshooting AOS-CX Switch Onboarding Issues.

Configuration Status

The **Configuration Audit** page under **Network Operations** > **Device(s)** > **Switches** in the Aruba Central UI displays errors in configuration sync, template configuration, and a list of configuration overrides. For more information, see Viewing Configuration Status.

The **Configuration Status** page under **Network Operations** > **Device(s)** > **Switches** in the AOS-CX UI configuration page of Aruba Central displays configuration status of the switches, pending changes, and local overrides present in the AOS-CX switches. For more information, see Using Configuration Status on AOS-CX.

Troubleshooting Tools

To troubleshoot AOS-CX switches remotely, use the tools available under **Network Operations** > **Analyze** > **Tools**. For more information, see Using Troubleshooting Tools.

Actions Drop-down

You can also reboot, connect to the remote console of the switch, or generate a tech support dump for troubleshooting the device, by using the tools available under the **Actions** drop-down. The **Actions** drop-down is available in the switch monitoring pages.

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Limitations of AOS-CX Switch in Aruba Central

There are a few limitations while managing and monitoring AOS-CX switches using Aruba Central. The following sections provide details on the limitations while onboarding, configuring, monitoring, and troubleshooting AOS-CX switches using Aruba Central.

Monitor-only mode is not supported for the AOS-CX switches in the UI or template groups. You can add the AOS-CX switches to the UI or template groups to configure, monitor, and troubleshoot the AOS-CX switches.

Onboarding

The following limitations should be taken into consideration when onboarding AOS-CX switches in Aruba Central:

- ZTP does not work on inline data ports for AOS-CX 8320 and 8325 switch series. The following is an example configuration for onboarding AOS-CX 8320 and 8325 switch series to Aruba Central:

```
interface 1/1/1
     no shutdown
     no routing
interface vlan 1
     ip address <IP-ADDRESS/MASK>
ip route 0.0.0.0/0 <IP-GATEWAY>
ip dns server-address <DNS-SERVER>
https-server vrf default
ztp force-provision
```

- After the `erase startup-config` command is executed on the AOS-CX switches, the switches do not onboard to Aruba Central. It is recommended to execute the `erase all zeroize` command, instead of the `erase startup-config` command.
- When an AOS-CX switch is first onboarded to Aruba Central, Aruba Central must perform the following actions, before it can perform events such as rebooting the switch and upgrading the firmware:
  - Login to the switch using the password provided in the template configuration.
  - Apply the template to the switch.

Applying Template

The following limitations should be taken into consideration when applying the template to AOS-CX switches in Aruba Central:

- You must configure the admin password in the template configuration only in plaintext. The format of the password configuration command must be `user admin group administrators password plaintext <string>`.
- If the template for AOS-CX switches contains `%` in the configuration, Aruba Central will not save the configuration.

  Although the `%` character is allowed in AOS-CX switches, for example in banners, the same is not allowed in Aruba Central. In Aruba Central, the `%` character is reserved for variables.
- The maximum number of lines supported in the configuration template is 84000. Beyond this limit, Aruba Central will not apply the template to the AOS-CX switch.
- Onboarding an AOS-CX switch with 10.05 firmware to Aruba Central, using the **Import Configuration as Template** option on the **Add Template** window, fails to import the configuration and displays an error message. In this case, you must manually create the template for the switch using the output of the `show running-config` command. You can successfully import the configuration as a template for an AOS-CX switch with 10.05 firmware, only when the switch is part of a template group and the config-sync status is in-sync.

  To import the configuration as template when onboarding an AOS-CX switch, without the error message, you must upgrade the switch to 10.06 firmware.

Configuring AOS-CX VSF Stack

The following are the VSF stacking limitations of AOS-CX switches in Aruba Central:

Aruba Central supports only a few functions related to AOS-CX switch stack, such as onboarding a stack to Aruba Central and replacing member switches having the same model and part number, through template configuration. All other stacking related functions, such as creating a stack, deleting, or adding a new member to the stack, must be performed offline, that is, outside Aruba Central. These stacking related functions must be performed before or after onboarding the stack to Aruba Central depending on the function.

For example, you must create a stack offline before onboarding the stack to Aruba Central. For more information, see AOS-CX VSF Stack.

AOS-CX VSF Stack Related Functions Not Supported on Aruba Central

The following stack related functions are not supported on Aruba Central:

- Creating a new stack
- Adding a new member to an existing stack
- Deleting a member from the stack
- Replacing a member with different part number
- Modifying standby member ID
- Adding, deleting, and modifying VSF links

Using AOS-CX VSX

The following limitations apply when configuring VSX or viewing VSX data for AOS-CX switches in Aruba Central:

- Enabling VSX synchronization using template configuration in Aruba Central is not recommended. By enabling VSX synchronization, the peer switch might get into an unknown configuration state.
- Last synced data is not displayed on the **VSX** page, in Aruba Central, if VSX synchronization is not enabled.

Managing Firmware Upgrade

To upgrade an AOS-CX switch in Aruba Central, a WAN connection with a minimum speed of 2 Mbps is required. The upgrade activity will time out after a period of 60 minutes.

Troubleshooting

The following are the limitations while troubleshooting AOS-CX switches in Aruba Central:

- For AOS-CX 8320 and 8325 switch series, to use the remote console feature, you must enable SSH server on the VRF that the switch uses to connect to Aruba Central. You must add one of the following commands in the template:
  - If the switch is connecting to Aruba Central using the inline default VRF, add `ssh server vrf default` to the template.
  - If the switch is connecting to Aruba Central using the OOBM management VRF, add `ssh server vrf mgmt` to the template.
- The **Chassis Locate** option, in the **Analyze** > **Tools** > **Device Check** tab, is not displayed for AOS-CX 8320 and 8325 switch series.

Monitoring

In the monitoring pages in Aruba Central, the IP address for the connected wired clients on AOS-CX switches might not be displayed if the Client IP tracker is not enabled on the switch.

To enable Client IP tracker, perform one of following steps:

- Using Template—Add the `client track ip` command to the template at the device and VLAN level.
- Using MultiEdit mode—Add the `client track ip` command in the MultiEdit mode at the device and VLAN level.

For more information, see Switch > Clients > Clients.

For more information on `client track ip` command, see the IP Client Tracker chapter in the *AOS-CX IP Routing Guide*.

Provisioning Factory Default AOS-CX Switches

Switches that run default configuration either after shipped from a factory or a factory reset are referred to as factory default switches. This topic describes the steps for provisioning factory default AOS-CX switches in Aruba Central.

Step 1: Onboard the AOS-CX Switch to Aruba Central

To onboard switches to the device inventory in Aruba Central, complete the following steps:

- Log in to Aruba Central
- Add switches to Aruba Central
- Assign Subscriptions

Step 2: Assign the AOS-CX Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. By default, Aruba Central assigns the factory default switches to default group. You can create a new group and assign switch to the new group.

For more information on creating a group, see Creating a Group.

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**. The Device Inventory page is displayed
2. Select the device that you want to assign to a group.
3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the group is displayed.
2. Under **Maintain**, click **Organization** > **Groups**. The Groups page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 3: Connect the AOS-CX Switch to Aruba Central

Switches with factory default configuration have very basic configuration for all ports in VLAN-1 that is required for obtaining an IP address and automatic provisioning (ZTP). For ZTP, switches must have a valid IP address, DNS, and NTP configuration.

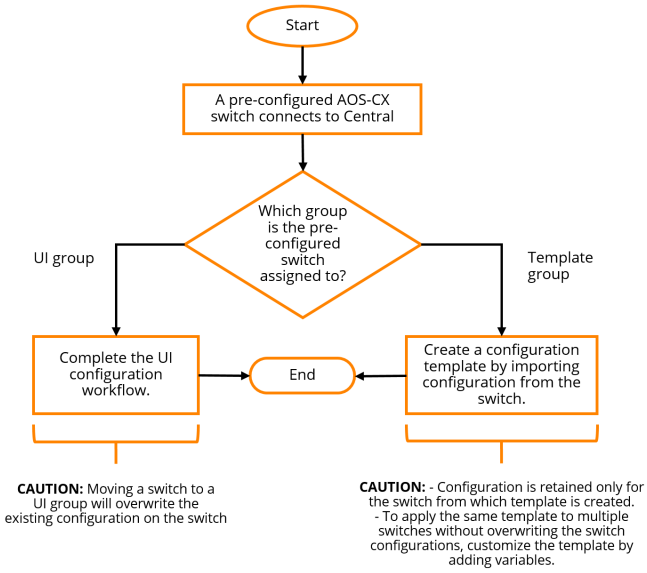
When a factory default switch is powered on and connected to the Internet, it establishes connection with Aruba Activate and downloads the provisioning parameters. If the switch is already added and assigned a subscription, it connects to Aruba Central.

Step 4: Provision the AOS-CX Switch to a Group

When the switch connects to Central, if it is already added to the device inventory and is assigned a subscription in Aruba Central, Aruba Central assigns it to a pre-assigned group. If there is no pre-assigned group, Aruba Central moves the device to the **default** group. Based on your configuration requirements, you create a template group and assign the switch.

The following figure illustrates the provisioning step required for each group type.

Figure 145 *AOS-CX Switch Provisioning Steps Per Group Type*



If the switch is assigned to a new UI group, Aruba Central uses the current configuration of switch as base configuration and applies it to the other switches that join this group later. You can also modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Devices** > **Switches**. For more information, see Configuring AOS-CX Switches in UI Groups.

Provisioning Switches in Template Groups

After assigning the switch to a template group, create a new configuration template. To create a configuration template:

1. In the **Network Operations** app, set the filter to a template group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.

The tabs to configure switches using templates is displayed.

1. Click the **Templates** tab. The Templates page is displayed.
2. Click **+** to add a new template. The **Add Template** window is displayed.
3. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
4. In the **Device Type** drop-down, select **AOS-CX.**
5. Select the switch model and software version. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
   - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
   - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.

6. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

7. Click **Next**. The **Template** tab is displayed.
8. Build a new template by adding the output of the `show running-config` from the switch CLI in the **Template** text box. Ensure that the template text adheres to the guidelines listed in Important Points to Note.

- You must manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the show running-config command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates.
- For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.

9. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.

   The tabs to configure switches using templates is displayed.
   - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
   - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.

5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Provisioning Pre-Configured AOS-CX Switches

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. On AOS-CX switches, Aruba Central is enabled, by default, as their management platform, and therefore the switches connect to Aruba Central automatically.

To onboard a locally-managed or a pre-configured AOS-CX switch to Aruba Central, follow one of the following options:

- Connect the AOS-CX switch directly to Aruba Central. Aruba recommends that you use this option if you want to preserve the current configuration running on the switch. For more information on this procedure, see the workflows described in this topic.
- Reset the switch configuration to factory default and use ZTP to provision the switch. For information on provisioning factory default switches, see Provisioning Factory Default AOS-CX Switches.

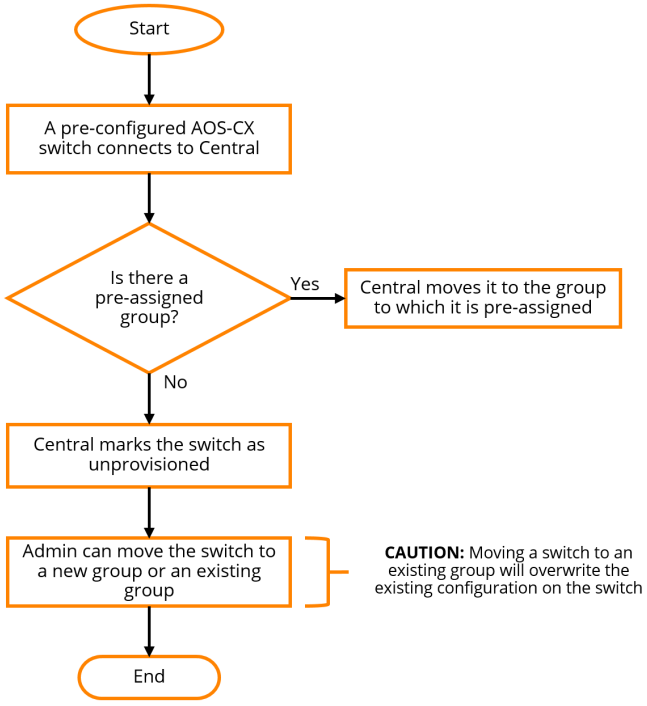
  Aruba Central supports provisioning AOS-CX switches using one of the following methods:
- Pre-provisioning—In this workflow, a switch is added to the device inventory and assigned a group in Aruba Central before it connects to Aruba Central.

  See Workflow 1—Pre-Provisioning an AOS-CX Switch.
- Onboarding connected switches—In this workflow, Aruba Central onboards the switch that attempts to connect and then assigns a group.

  See Workflow 2—Provisioning an AOS-CX Switch On-Demand.

The following figure illustrates provisioning procedure for a pre-configured switch.

Figure 146 *Provisioning Workflow for Pre-Configured Switches*



Workflow 1—Pre-Provisioning an AOS-CX Switch

The pre-provisioning workflow includes the following steps:

- Step 1: Onboard the AOS-CX Switch to Aruba Central
- Step 2: Assign the AOS-CX Switch to a Group
- Step 3: Provision the AOS-CX Switch to a Group
- Step 4: Verify the Configuration Status

Step 1: Onboard the AOS-CX Switch to Aruba Central

To onboard AOS-CX switches to the device inventory in Aruba Central, complete the following steps:

- Log in to Central
- Add switches to Central
- Assign Subscriptions

Step 2: Assign the AOS-CX Switch to a Group

Before assigning a group, determine if the AOS-CX switch must be provisioned in a UI or template group. If you want to preserve the existing configuration on the switch, Aruba recommends that you create a new group for the switch.

For more information on creating a group, see Creating a Group.

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The Device Inventory page is displayed.
2. Select the device that you want to assign to a group.
3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

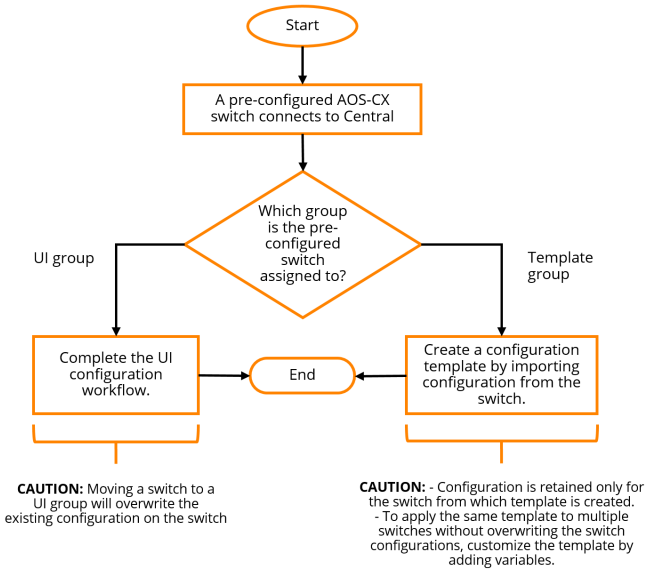
To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization** > **Groups**.
   The Groups page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 3: Provision the AOS-CX Switch to a Group

When the AOS-CX switch connects to Aruba Central, Aruba Central automatically assigns it to the pre-assigned template group.

Figure 147 *Switch Provisioning Steps Per Group Type*



If the switch is assigned to a new UI group, you can modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Devices** > **Switches**. For more information, see Configuring AOS-CX Switches in UI Groups.

You can import the existing switch configuration to a new configuration template and apply this template to other devices in the group. To create a configuration template using the existing configuration on the switch:

1. In the **Network Operations** app, set the filter to a template group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.

   The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba CX**.
8. Select the switch model and software version. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
   - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
   - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.

9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Click **Next**. The **Template** tab is displayed.
11. Build a new template by adding the output of the `show running-config` from the switch CLI in the **Template** text box. Ensure that the template text adheres to the guidelines listed in Important Points to Note.

- You must manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the show running-config command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates.
- For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.
- For AOS-CX switches, the password configured in the template must match the password configured on the switch. Aruba Central cannot override the password that is configured on the switch.

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 4: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
   The tabs to configure switches using templates is displayed.
   - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.

- To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.

4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Workflow 2—Provisioning an AOS-CX Switch On-Demand

To dynamically provision switches on-demand, complete the following steps:

- Step 1: Add the AOS-CX Switch to Aruba Central
- Step 2 Assign a Subscription to the AOS-CX Switch
- Step 3: Provision the AOS-CX Switch to a Group
- Step 4: Verify the Configuration Status

Step 1: Add the AOS-CX Switch to Aruba Central

Add the switch to the Aruba Central device inventory. For more information, see Onboarding Devices.

Step 2 Assign a Subscription to the AOS-CX Switch

To allow Aruba Central to manage the switch, ensure that a valid subscription is assigned to the switch. For more information, see Managing License Assignments.

Step 3: Provision the AOS-CX Switch to a Group

If the switch has a valid license assigned, Aruba Central marks the switch as **unprovisioned**.

To move the device to a UI group:

1. To create a UI group, see Creating a Group.
2. In the **Network Operations** app, set the filter to **Global**.
3. Under **Maintain**, click **Organization** > **Groups**.

   The Groups page is displayed.
4. Select the switch from the list of devices on the right.
5. Drag and drop the switch to the group in the table on the left. A confirmation message is displayed.
6. Click **Yes** to add the switch to the group.

You can modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Devices** > **Switches**. For more information, see Configuring AOS-CX Switches in UI Groups.

To move the device to a template group:

1. To create a template group, see Create a template group.
2. In the **Network Operations** app, set the filter to **Global**.
3. Under **Maintain**, click **Organization** > **Groups**.

   The Groups page is displayed.
4. Select the AOS-CX switch.
5. Drag and drop the switch to the new template group that you just created. Aruba Central adds the switch to the new template group.

6. To build a new configuration template:
   a. In the **Network Operations** app, set the filter to a template group.

      The dashboard context for the group is displayed.
   b. Under **Manage**, click **Devices** > **Switches**.
   c. Click the **Config** icon.

      The tabs to configure switches using templates is displayed.
   d. Click the **Templates** tab. The Templates page is displayed.
   e. Click **+** to add a new template. The **Add Template** window is displayed.
   f. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
   g. In the **Device Type** drop-down, select **Aruba CX**.
   h. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
      - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
      - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
      - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
      - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
      - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
   i. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

   j. Click **Next**. The **Template** tab is displayed.
   k. Build a new template by adding the output of the `show running-config` from the switch CLI in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the Important Points to Note.

- You must manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the show running-config command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates.
- For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.
- For AOS-CX switches, the password configured in the template must match the password configured on the switch. Aruba Central cannot override the password that is configured on the switch.

l. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 4: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
   The tabs to configure switches using templates is displayed.
   - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
   - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Using Configuration Templates for AOS-CX Switch Management

Templates in Aruba Central refer to a set of configuration commands that can be used by administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple switches in a group and thus automate switch deployments.

NOTE

To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on AOS-CX switches.

Creating a Group for Template-Based Configuration

For template-based provisioning, switches must be assigned to a group with template-based configuration method enabled.

For more information, see Managing Groups and Assigning Devices to Groups.

NOTE

The **Import Configuration As Template** feature is supported only on AOS-CX switches running firmware version 10.06 or later.

Creating a Configuration Template

To create a configuration template for switches:

1. In the **Network Operations** app, set the filter to a template group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
   The tabs to configure switches using templates are displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **AOS-CX**.
8. Select the switch model and software version. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
   - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
   - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

NOTE

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Click **Next**. The Template tab is displayed.
11. Build a new template or import configuration information from a switch that is already provisioned in the template group.
    - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the Important Points to Note.
    - To import configuration text from a switch that is already provisioned in the template group:
        a. Click **Import Configuration As Template**.
        b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.
        c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in the Important Points to Note.

- You can manually create the template for the AOS-CX switch in a group, along with the password in plaintext format. You can use the output of the `show running-config` command to create the template. You can also add variables to use the same template for onboarding multiple AOS-CX switches. For more information on variables, see Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates.
- For AOS-CX switches, you must configure the password only in plaintext. Also, the format of password must be `user admin group administrators password plaintext <string>`.

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration

Important Points to Note

Note the following points when adding configuration text to a template:

- The CLI syntax in the switch template must be accurate. Aruba recommends that you validate the configuration syntax on the switch before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- The commands in the template are case-sensitive and cannot contain the **%** character. In the template-based configuration, the **%** character is reserved and is used to denote variables.

The following example illustrates the case discrepancies that the users must avoid in the template text:

```
ssh server vrf default
ssh server vrf mGmt
vsf member 1
    type jl660ab
vlan 1
spanning-tree
```

```
interface Mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
interface 1/1/2
    no shutdown
    no routing
    vlan access 1
interface 1/1/3
    no shutdown
    no routing
    vlan access 1
interface 1/1/4
    no shutdown
    no routing
    vlan access 1
interface 1/1/5
    no shutdown
    no routing
    vlan access 1
interface 1/1/6
    no shutdown
    no routing
    vlan access 1
interface 1/1/7
    no shutdown
    no routing
    vlan access 1
interface 1/1/8
    no shutdown
    no routing
    vlan access 1
interface 1/1/9
    no shutdown
    no routing
    vlan access 1

interface vlan 1
    ip dhcp
!
!
!
!
!
https-server vrf default
```

```
https-server vrf MGMT
```

Configuring AOS-CX Switches in UI Groups

You can configure AOS-CX switches that are added to a UI group, using the UI options and MultiEdit mode. You can configure 6200, 6300, 8320, 8325, 8360 Switch Series using UI options, MultiEdit mode, and templates. You can configure 6405, 6410, and 8400 Switch Series using only templates. To configure AOS-CX switches using templates, see Using Configuration Templates for AOS-CX Switch Management.

The UI options and MultiEdit mode are available only when the AOS-CX switches are added to a UI group. The UI options and MultiEdit mode are not available when the AOS-CX switches are added to a template group.

To configure or view the properties of AOS-CX switches that are added to UI groups, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a UI group in the filter:
     a. Set the filter to a UI group.

        The dashboard context for the UI group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a UI group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.

   The following table describes the different configuration pages and their functions.

Table 173: *Configuring AOS-CX Switches Provisioned in UI Groups*

Feature	Description
Properties	Edit system property settings such as contact, location, time zone, and administrator password. You can also select the VRF to be used and add the DNS and NTP servers. See Configuring System Properties on AOS-CX.
SNMP	Add, edit, or delete the following: ■ SNMP v2c communities ■ SNMP v3 users ■ Trap notifications for SNMP v2c and v3 See Configuring SNMP on AOS-CX.

Feature	Description
Logging	Add, edit, or delete logging servers to view event logs from the AOS-CX switches. Configure FQDN or IP address, log severity level, and the VRF to be used for each of the logging servers. Also configure the global level debug log severity. See Configuring Logging Servers for AOS-CX.
Administrator	Add, edit, or delete server groups to be used for authentication, authorization, and accounting. You must also configure the protocol required to enable connection to these server groups. See Configuring AAA for AOS-CX.
Static Routing	Add, edit, or delete static routes manually and configure destination IP addresses and next hop values, VRF, and the administrative distance. You can add different static routes for different VRFs on the switch. See Configuring Static Routing on AOS-CX.
Ports & Link Aggregations	View and edit port settings such as description, VLAN mode, speed duplex, routing, and the operational status of the port. Add, edit, or delete LAGs by combining different ports and configuring the speed duplex, VLAN mode, aggregation mode, and the operational status of the LAG. See Configuring Ports and LAGs on AOS-CX.
Authentication Servers	Add, edit, or view the RADIUS and TACACS servers for authentication. Add settings such as FQDN or IP address of the servers, authentication port number, response timeout, retry count, and the VRF to be used when communicating with the servers. See Configuring Authentication Servers on AOS-CX.
Authentication	View or edit details about 802.1X and MAC authentication methods. Configure the precedence order and other parameters such as reauthentication timeout, cached reauthentication timeout, and quiet period. See Configuring Authentication on AOS-CX.
Access Control	View or add access policies and rules to permit or deny passage of traffic. See Configuring Access Control on AOS-CX.
VLANs	Add, edit, delete, or view VLANs, and associated parameters such as type of IP assignment, operational status, IP address of the DHCP relay. See Configuring VLANs on AOS-CX.
Loop Prevention	Enable or disable loop protection and spanning tree protocol, and associated parameters such as the mode and priority. Enable or disable various MSTP mode-related settings such as BPDU filter, BPDU protection, admin edge, and root guard. See Configuring Loop Prevention on AOS-CX.

2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.

   The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.

At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.

Search for a switch by entering a search query in the **Contextual Search Engine** field.

For more information about search queries, see Using Device Search on AOS-CX.

The following table describes the options available in the MultiEdit mode of configuring AOS-CX switches.

Table 174: *Configuring AOS-CX Switches Provisioned in UI Groups using the MultiEdit Mode*

Feature	Description
MultiEdit	View and edit configuration on the AOS-CX switches using the CLI syntax. You can also apply predefined set of configuration settings such as NAE to the switches. See Using MultiEdit View for AOS-CX.
View Config	View configuration of AOS-CX switches and find differences in the configuration across switches. See Viewing Configuration on AOS-CX.
Edit Config	Edit configuration for one or more AOS-CX switches in the MultiEdit mode. Edit the entire configuration in a familiar looking CLI with syntax checking, colorization, and command completion. See Editing Configuration on AOS-CX.
Express Config	Apply predefined set of configuration settings such as NAE scripts and device profile to a single or multiple switches. See Express Configuration on AOS-CX.
Device Search	Search for AOS-CX switches in the **Devices** table, in the MultiEdit mode, using search queries such as device attributes, wildcard characters, Boolean operators, and by grouping characters. See Using Device Search on AOS-CX.

3. To view configuration status, pending changes, and local overrides on the switches, click **Configuration Status**.

   This page allows you to commit the pending changes in a configuration. At the device level, this page allows you to change the auto-commit state of the switch.

   For more information, see Using Configuration Status on AOS-CX.

Managing Configuration Overrides

Aruba Central supports two levels of configuration hierarchy:

- Group-level—When you add a switch to a group, or move a switch from one group to, another, the switch inherits the configuration of the group. Any configuration changes made at the group-level are applied to the devices in the group.

Only configurations that are supported at the group-level are applied to the devices. The configurations that are supported only at the device-level are preserved.

- Device-level—Any modifications made at the device-level override the configurations inherited from the group. Local overrides are those modifications that you make on a particular device in a group. Once a local override exists on a device, then any configuration changes performed at the group level will not be applied or inherited to that device.

Configuration overrides are applicable to only those parameters, which are present at both group and device levels.

Managing Passwords for Groups and Devices using UI groups

In Aruba Central, you can set a password for UI groups when creating a new group. This group password is used to onboard the AOS-CX switches to the group. The group password must match with the device password to onboard the device successfully to the group. For more information, see Managing Groups.

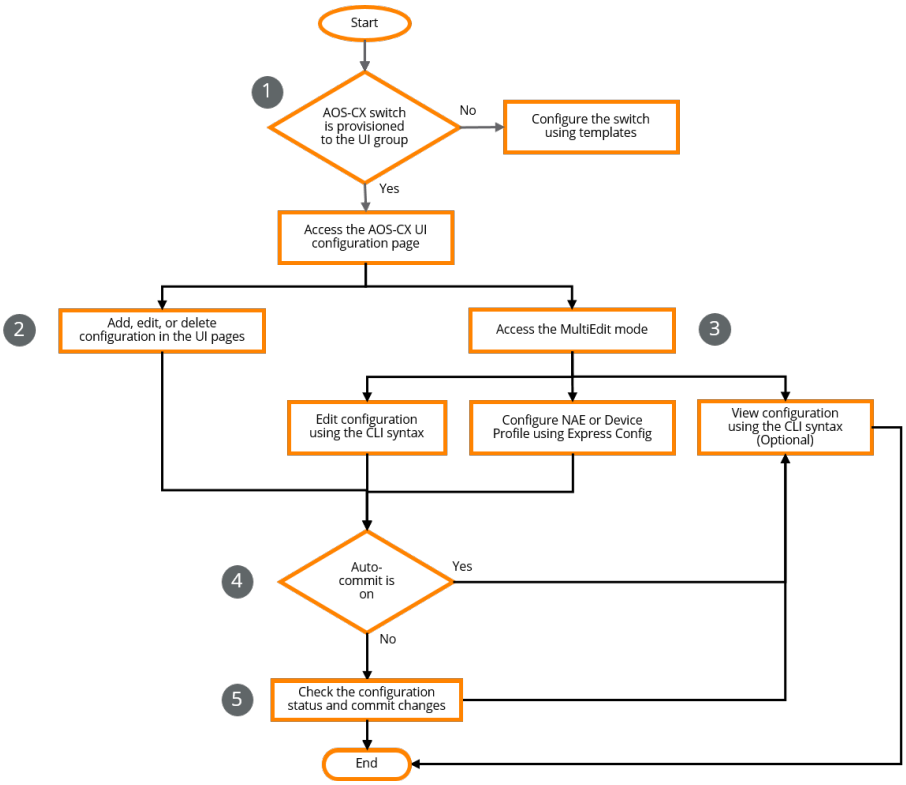
You can use the **Properties** page to change the administrator password for groups and devices. If you set different password at the device-level, then the device can no longer be managed at the group-level. For more information, Configuring System Properties on AOS-CX.

If you upgrade Aruba Central from earlier versions to the latest version, the administrator password is considered blank. Aruba Central prompts the user to specify an administrator password for the devices in the group. You cannot make any configuration update until a new password is set.

Configuration Workflow for AOS-CX Switches in UI Groups

The following workflow explains the process to configure AOS-CX switches using UI options.

Figure 148 *UI Configuration Workflow for AOS-CX Switches*



Workflow Steps

1. Provision an AOS-CX switch to a UI group in Aruba Central. See Getting Started with AOS-CX Deployments.

   When you add AOS-CX switches to a UI group, you can configure them using the following options:
   - Various UI options
   - MultiEdit mode
2. Configure the switch using the different configuration options available on the UI. You can add, edit, or delete configurations using the UI options.

   See Configuring AOS-CX Switches in UI Groups.

3. Configure the switch in the MultiEdit mode—The MuliEdit mode offers a CLI syntax-based configuration functionality for AOS-CX switches. You can view or edit the running configuration on the switch or apply express configuration.

   See Using MultiEdit View for AOS-CX.

   - **Edit Config**—Edit switch configuration using the CLI syntax. You can edit the configuration of switches. After you edit the configuration, you can view the difference between the running configuration and the edited configuration in the same window. See Editing Configuration on AOS-CX.
   - **Express Config**—Apply a predefined set of configuration settings to switches using this option for device profile and NAE configurations. See Express Configuration on AOS-CX.
   - **View Config—**View the running configuration on the switch using this option. The changes made on the UI options, Edit Config, or the Express Config pages will appear on this page only if the Auto-Commit state is on or if the changes are committed manually. See Viewing Configuration on AOS-CX.

4. Depending on the Auto-Commit state of the switch, you can either view the configuration changes immediately or commit the changes first and then view the configuration changes.
   - If the Auto-Commit state is on, Aruba Central applies the configuration changes immediately to the switch. You can view the configuration on the View Config page in the MultiEdit mode.
   - If the Auto-Commit state is off, you must manually commit changes to the switch and then view the configuration.

   See Using Configuration Status on AOS-CX.

5. When the Auto-Commit state is off, check whether there are any pending changes to be applied to the switch, in the Configuration Status page. Commit any pending configuration changes to the switch and view the updated configuration.

Configuring System Properties on AOS-CX

From the Properties page, you can view or configure system property settings such as contact, location, timezone, administrator username, and administrator password for AOS-CX switches. In addition, you can select management VRF or default VRF, and configure DNS and NTP servers for the selected VRF.

To edit system properties, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

d. Under **Manage**, click **Device**.

The AOS-CX UI configuration page is displayed.

2. Click **System** > **Properties**.

The Edit Properties page is displayed.

3. Edit the following properties:

Table 175: *Switches Properties*

Name	Description	Value
Name	Name of the switch. This field is available only at the device level.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Contact	Contact details for the switch.	Name, Email address, or phone number. You can enter up to a maximum of 128 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Location	Location of the switch.	You can enter up to a maximum of 128 characters including letters, numbers, and special characters, except question mark (?) and double quotes (") For example: Portland, Oregon.
Timezone	The time zone corresponding to the location of the switch.	Time zone selected from the drop-down.
VRF	The VRF to be used for communicating with DNS and NTP servers. **NOTE:** If you change the VRF setting, then the existing DNS and NTP server settings will be removed.	**Default** or **Management OOBM**
DNS servers	The IP address of DNS servers for the selected VRF. Click **+** to add another DNS server.	IPv4 address or IPv6 address

Name	Description	Value
	You can add up to three servers.	
NTP servers	The IP address of NTP servers for the selected VRF. Click **+** to add another NTP server. You can add up to three servers.	IPv4 address or IPv6 address
Administrator password	The password for the administrator username. **NOTE:** To manage devices in the group, the password must be same at group and device-levels.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters except question mark (?) and double quotes (").

4. Click **Save**.

Configuring SNMP on AOS-CX

Simple Network Management Protocol (SNMP) SNMP is a TCP/IP standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for events that require administrative attention.

From SNMP page, you can configure SNMP versions v2c or v3 on AOS-CX switches using UI groups.

For more information, see the following topics:

- Configuring SNMPv2c on AOS-CX
- Configuring SNMPv3 on AOS-CX

Configuring SNMPv2c on AOS-CX

You can configure SNMPv2c community settings and trap destinations through the UI.

To configure SNMPv2c on switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
    a. Set the filter to **Global** or a group containing at least one switch.
    b. Under **Manage**, click **Devices** > **Switches**.
    A list of switches is displayed in the **List** view.
    c. Click an AOS-CX switch under **Device Name**.
    The dashboard context for the switch is displayed.
    d. Under **Manage**, click **Device**.
    The AOS-CX UI configuration page is displayed.

2. Click **System** > **SNMP**.
   The SNMP page is displayed.
3. Select **v2c** from the **SNMP** drop-down. The **Read Community** and **Trap Destination** tables are displayed.

Adding an SNMP Community

You can add SNMP communities to restrict access to the switch from the SNMP management stations. The default community name is Public.

To add an SNMP community, complete the following steps:

1. In the **Read Community** table, click **+**. A new row is added in the table.
2. Type the name of the community in the new row. You can enter up to a maximum of 32 characters including letters, numbers, and special characters.
3. Click **Save**.

Editing an SNMP community

To edit an SNMP community, point to the row for the SNMP community, and click the edit icon.

You can edit an SNMP community name only before saving it to Aruba Central. If the SNMP community is saved, then it cannot be edited.

Deleting an SNMP Community

To delete an SNMP community, point to the row for the SNMP community, and click the delete icon.

If you delete an SNMP community, trap destinations that belong to the community will also get deleted.

Adding a Trap Destination

You can add trap destinations to send notifications to SNMP management stations.

To add a trap destination, complete the following steps:

1. In the **Trap Destination** table, click **+**. A new row is added in the table.
2. Configure the following parameters:
    - **IP Address**—Enter a valid IPv4 or IPv6 address of the SNMP host.
    - **VRF**—Select the available VRF on the switch from the drop-down.
    - **Community**—Select the name of the community from the drop-down.

3. Click **Save**.

Editing a Trap Destination

To edit a trap destination, point to the row for the trap destination, and click the edit icon.

You can edit only the community name.

Deleting a Trap Destination

To delete a trap destination, point to the row for the trap destination, and click the delete icon.

Configuring SNMPv3 on AOS-CX

SNMPv3 provides a secured access to SNMP management stations using authentication and privacy protocols. You can add SNMPv3 user and configure notification settings using UI groups.

To configure SNMPv3 on switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.
        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
        The tabs to configure the switch is displayed.
2. Click **System** > **SNMP**.
   The SNMP page is displayed.
3. Select **v3** from the **SNMP** drop-down.
   The **User** and T**rap Destination** tables are displayed.

Adding an SNMPv3 User

You can add SNMPv3 users to provide secured access to SNMP management stations.

To add an SNMPv3 user, complete the following steps:

1. In the **Users** table, click **+**. A new row is added in the table.
2. Configure the following parameters:
   - **Name**—Enter the name of the SNMPv3 user.
   - **Authentication Mode**—Select either **md5** (Message Digest) or **sha** (Secure Hash Algorithm) as the authentication mode to provide secured access to the user. After selecting the authentication

mode, enter the authentication password. The password must be 8 to 32 characters long, and can contain alphabets, numbers, and special characters.

- **Privacy Mode**—Select **aes** (Advanced Encryption Standard) or **des** (Data Encryption Standard) as the privacy mode to provide secured access to the user. After selecting the privacy mode, enter the privacy password. The password must be 8 to 32 characters long, and can contain alphabets, numbers, and special characters.

3. Click **Save**.

Editing an SNMPv3 User

To edit an SNMPv3 user, point to the row for the user, and click the edit icon.

You can edit an SNMPv3 user only before saving it to Aruba Central. If the user is saved to Aruba Central, then it cannot be edited.

Deleting an SNMPv3 User

To delete an SNMPv3 user, point to the row for the user, and click the delete icon.

If you delete the user, then the trap destination where the user is added will also get deleted.

Adding a Trap Destination

You can add trap destinations to send notifications to SNMP management stations.

To add a trap destination, complete the following steps:

1. In the **Trap Destination** table, click **+**. A new row is added in the table.
2. Configure the following parameters:
   - **IP Address**—Enter a valid IPv4 or IPv6 address of the SNMP host.
   - **VRF**—Select the available VRF on the switch from the drop-down.
   - **Name**—Select the user to whom the notifications should be sent.
3. Click **Save**.

Editing a Trap Destination

To edit a trap destination, point to the row for the trap destination, and click the edit icon.

You can only edit the user name.

Deleting a Trap Destination

To delete a trap destination, point to the row for the trap destination, and click the delete icon.

Configuring Logging Servers for AOS-CX

Logging allows you to add syslog servers where the event log messages related to the AOS-CX switches are saved. For each of the syslog server you add, you can configure the severity of the event logs to be saved on these servers. You can also configure the severity level for the debug logs by configuring the severity at the global level. However, you must add a minimum of one syslog server to configure the global severity level.

To configure logging servers, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.

     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.

     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. Click **System** > **Logging**.

   The Logging page is displayed.
3. Select the debug syslog severity level at the global level from the **Level** drop-down.

   This severity level is applied to the debug logs that are saved on the syslog servers. You must add a minimum of one event syslog server before configuring the global severity level.
4. In the **Logging Servers** table, click **+** to add a logging server and configure the following parameters in the Add Logging Server page:

   Table 176: *Logging Server Parameters*

Parameters	Description	Value
FQDN or IP address	FQDN hostname or IP address of the logging server.	IPv4 address in the `x.x.x.x` format or hostname of the server.
Level	Severity level of the events that the logging server must log.	Following severity levels are supported: ▪ **Emergency** ▪ **Critical** ▪ **Alert** ▪ **Error** ▪ **Warning** ▪ **Notice** ▪ **Information** ▪ **Debug**
VRF	VRF on which the logging server is configured.	**Default** or **Management**.

5. Click **Apply** and then click **Save**.
6. To edit parameters of a logging server, select the row in the **Logging Servers** table and click the edit icon.

   The Edit Logging Server page is displayed. You can edit only the event log severity level and the VRF.

7. Click **Apply** and then click **Save**.
8. To delete the syslog server, select the row in the **Logging Servers** table and click the delete icon.
9. Click **OK** in the confirmation pop-up and then click **Save**.

Configuring AAA for AOS-CX

Authentication, Authorization, and Accounting (AAA) is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

From the Administrator page, you can configure the following AAA properties:

- Authentication using TACACS, RADIUS, and local server groups.
- Authorization using TACACS and local server groups.
- Accounting using TACACS, RADIUS, and local server groups.

To configure AAA properties for AOS-CX switches, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. Click **System** > **Administrator**.

   The Administrator page is displayed with Authentication, Authorization, and Accounting tables.
3. You can configure Authentication, Authorization and Accounting from the respective tables.
   - To configure Authentication, click **+** in the **Authentication** table and configure the following parameters:

     Table 177: *Authentication Parameters*

Name	Description	Value
Protocol	The type of protocol to enable connection to the server groups for authentication. You can add one or more protocols by clicking **+** in the Authentication table.	**Console**, **Default**, **HTTPS Server**, and **SSH**.

Name	Description	Value
Server Groups	The list of server groups to be used for authentication. You can select one server group at a time. To add the next server group, click **+** either in the protocol row or any of the server group rows. The server groups are accessed in the top-down order. You can rearrange the order by dragging the server group to a different position using the drag-and-drop icon.	**TACACS**, **RADIUS**, and **Local**.

- To configure Authorization, click **+** in the **Authorization** table and configure the following parameters:

  Table 178: *Authorization parameters*

Name	Description	Value
Protocol	The type of protocol to enable connection to the server groups for authorization. You can add one or more protocols by clicking **+** in the Authorization table.	**Console**, **Default**, and **SSH**.
Server Groups	The list of server groups to be used for authorization. You can select one server group at a time. To add the next server group, click **+** either in the protocol row or any of the server group rows. The server groups are accessed in the top-down order. You can rearrange the order by dragging the server group to a different position using the drag-and-drop icon.	**TACACS**, **Local**, and **None**.

- To configure Accounting, click **+** in the **Accounting** table and configure the following parameters:

  Table 179: *Accounting Parameters*

Name	Description	Value
Protocol	The type of protocol to enable connection to the server groups for accounting. You can add one or more protocols by clicking **+** in the Accounting table.	**Console**, **Default**, **HTTPS Server**, and **SSH**.
Server Groups	The list of server groups to be used for accounting. You can select one server group at a time. To add the next server group, click **+** either in the protocol row or any of the server group rows. The server groups are accessed in the top-down order. You can rearrange the order by dragging the server group to a different position using the drag-and-drop icon.	**TACACS**, **RADIUS**, and **Local**.

4. Click **Save**.

Deleting AAA properties

To delete Authentication, Authorization, or Accounting, point to the row for the AAA property in the respective tables, and click the delete icon.

Configuring Static Routing on AOS-CX

Static routes provide a means for restricting and troubleshooting routed traffic flows. In small networks, static routes provide the simplest and most reliable configuration for routing. Static routes are manually configured in the routing table.

For each static route, you can configure the destination and next hop IP addresses to route the packets, VRF, and the administrative distance. You can add static routes only for the management and default VRFs.

To add static routes on AOS-CX switches, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. Click **Routing** > **Static Routing**.

   The Static Routing page is displayed.
3. In the **Static Routing** table, click **+** to add a static route and configure the following parameters in the Create Static Route page:

   Table 180: *Static Route Parameters*

Parameters	Description	Value
Destination	A valid network or device IP address with subnet mask.	IPv4 or IPv6 address. ■ IPv4 address in the `x.x.x.x/M` format, where `x` is an integer from `0` to `255`, and `/M` is the subnet mask. ■ IPv6 address in the `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/M` format, where `x` is a hexadecimal number from `0` to

Parameters	Description	Value
		F, and /M is the subnet mask.
Next Hop	Address of the next node in the route.	▪ IPv4 or IPv6 address without the subnet mask. ▪ Port number or LAG name that has routing enabled.
VRF	VRF on which the static route is configured.	**Default** or **Management**. When you select **Management**, you can configure only the **Next Hop** field. **NOTE:** When you configure a static route with the Mangment VRF, the configured Next Hop address is updated as the default gateway of the OOBM interface when the address mode of the OOBM interface is configured as static IP.
Distance	The administrative distance helps routers determine the best route when there are multiple routes to the destination. A lower value is recommended.	The default administrative distance for static IP routes is 1, but can be configured to any value in the range 1 to 255.

If the administrative distance is set to a lower value for static routes, switches use the static IP routes as the best route for routing traffic. For example, if the administrative distance for a static route is set to 20 and for an OSPF-based route is set to its default value, 110, then the switch choose the static route as the best route for routing traffic.

4. Click **Save**.

Configuring Ports and LAGs on AOS-CX

Link aggregation group (LAG) bundles multiple physical Ethernet links into one logical link. Link aggregation has the following benefits:

- Increased bandwidth beyond the limits of single link. In an aggregate link, traffic is distributed across the member ports.
- Improved link reliability. The member ports dynamically back up one another. When a member port fails, its traffic is automatically switched to other member ports.

From the Ports and Link Aggregation page, you can view all the ports, configure LAGs, and modify port settings for AOS-CX switches using UI groups.

Adding a LAG

To add a LAG, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. Click **Interfaces** > **Ports & Link Aggregations**. The Ports & Link Aggregations page is displayed with the list of ports configured on the switch.
3. In the **Ports & Link Aggregations** table, click **+** to add a Lag. The Add Lag window is displayed.
4. Configure the following parameters:

Table 181: *Link Aggregation Parameters*

Name	Description	Value
Name	Name of the LAG.	Example: lag1, lag23, lag123.
Description	Description of the LAG.	A maximum of 64 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Port Members	The switch port members for the LAG.	Select from the drop-down list.
Speed Duplex	The speed and duplex configuration for the client traffic. **NOTE:** Speed duplex is shown or hidden depending on the value in Port Members field	Select from the drop-down list.
Routing	Indicates whether routing is enabled. If routing is enabled at the device level, then specify the IP address with subnet mask for the destination network. Format: (x.x.x.x/x). **NOTE:** If **Routing** is enabled at the device level, then port authentication configuration is reset on all the selected ports.	Toggle the switch to on or off position.

Name	Description	Value
VLAN Mode	The operational mode of VLAN. This field is available only when **Routing** is disabled. In the **access** mode , port carries traffic only for the VLAN to which it is assigned. In the **trunk** mode, a port can carry traffic for multiple VLANs.	**trunk** or **access** For **access** mode, an **Access VLAN** can be specified. For **trunk** mode, the **Native VLAN** and **Allowed VLANs** can be configured. You can enter multiple **Allowed VLANs** by specifying the range of VLANs or VLANs separated by comma. For example, 1-7 or 55, 56, 57.
Admin Up	The operational status of the LAG. If the check box is selected, then the LAG can receive and transmit data as long as a cable is connected and no physical or operational problems exists.	Select the check box to enable.
Aggregation Mode	The operational mode of link aggregation control protocol (LACP). LACP operates in these two modes: ■ **LACP active**—When the LACP is operating in active mode on either end of a link, both ports can send Protocol Data Units (PDUs). The active LACP initiates an LACP connection by sending LACPDUs. ■ **LACP passive**—When the LACP is operating in passive mode on a local member port and its peer port, both ports cannot send PDUs. The passive LACP will wait for the remote end to initiate the link.	**None**, **LACP active**, or **LACP passive**.

5. Click **Add**. The configured parameters are displayed in the **Ports & Link Aggregations** table.

Editing a LAG

To edit a LAG, point to the row for the LAG, and click the edit icon.

NOTE

You can edit only one LAG at a time.

Deleting a LAG

To delete a LAG, point to row for the LAG, and click the delete icon.

Editing Ports settings

You can edit port settings by selecting one or more ports. If ports selected have different values configured, then changes made will be deployed on all the selected ports. You can edit the

NOTE

If a port is added to a LAG, then the port will not be displayed in the **Ports and Link Aggregation** table.

To edit ports, complete the following steps:

1. In the **Ports & Link Aggregations** table, select one or more ports you want to edit and click the edit icon.

   The Edit Ports window is displayed.

2. Edit the following parameters:

   Table 183: *Ports Parameters*

Name	Description	Value
Description	Description of the ports. When multiple ports are selected, then you can provide the same description for all the selected ports by selecting a **set same value for all ports** check box. You can also provide different descriptions by clicking on the individual port fields.	A maximum of 64 characters including alphabets and numbers. Special characters are not allowed.
Speed Duplex	The speed and duplex configuration for the client traffic.	Select from the drop-down list. By default, **Speed Duplex** is set to **Auto**.
Routing	Indicates whether routing is enabled. If routing is enabled at the device level, then specify the IP address with subnet mask for the destination network. Format: (x.x.x.x/x), whereas IP address is not required at the group level. **NOTE:** If **Routing** is enabled at the device level, then port authentication configuration is reset on all the selected ports.	Toggle the switch to on or off position.
VLAN Mode	The operational mode of VLAN. This field is available only when **Routing** is disabled. By default, a port is in **access** mode and carries traffic only for the VLAN to which it is assigned. In **trunk** mode, a port can carry traffic for multiple VLANs.	**trunk** or **access** For **access** mode, an **Access VLAN** can be specified. For **trunk** mode, the **Native VLAN** and **Allowed VLANs** can be configured. You can enter multiple **Allowed VLANs** by specifying the range of VLANs or VLANs separated by comma. For example, 1-7 or 55, 56, 57.
Admin Up	The operational status of the port. If the check box is selected, then the port can send and receive data as long as a cable is connected and no physical or operational problems exist.	Select the check box to enable.

3. Click **Save**.

Editing OOBM Port

You can edit the Out of Band Management (OOBM) port at the device level. To edit the OOBM port, complete the following steps:

1. Select the **OOBM** port and click the edit icon.

   The Edit Port OOBM page is displayed.
2. Edit the following parameters:
   - **IP assignment**—Method of IP assignment as **Static** or **DHCP**. Enter the IP address for IP assignment if the selected method is **Static**.
   - **Admin UP**—Operational status of the port. If the check box is selected, then the port can send and receive data as long as a cable is connected and no physical or operational problems exists.
3. Click **Save**.

Configuring Authentication Servers on AOS-CX

From the Server groups page, you can configure RADIUS or TACACS authentication servers to authenticate and authorize the users of an AOS-CX switch. The authentication servers determine if the user has access to the administrative interface.

To configure authentication servers on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. Click **Security** > **Authentication Servers**. The Authentication Servers page is displayed with number of RADIUS and TACACS servers that are configured on the switch.

Configuring a RADIUS Server on AOS-CX

To configure a RADIUS server, complete the following steps:

1. In the **Authentication Servers** table, point to the **RADIUS** server row and click the edit icon. The RADIUS servers page is displayed with the list of RADIUS servers configured on the switch.
2. To add a RADIUS server, click **+**.

   The Add RADIUS window is displayed.

3. Configure the following parameters:

Table 185: *RADIUS Parameters*

Name	Description	Value
FQDN or IP address	The IP address or fully qualified domain name of the RADIUS server.	
Shared secret	The encryption key to be used during authentication sessions with the specified RADIUS server.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Authentication Port	The authentication port number for the specified server.	Range: 1-65535 Default: 1812
Timeout (secs)	The number of seconds to wait for a response from the RADIUS server before trying the next RADIUS server.	Range: 1-60 Default: 5
VRF	The VRF to be used for communicating with the RADIUS server.	**Default** and **Management**
Retry Count	The number of retry attempts for contacting the specified RADIUS server.	Range: 0-5 Default: 1

4. Click **Apply**. The added server is displayed in the RADIUS servers page.

   The server that was added first is accessed first, and if necessary, the second server is accessed second, and so on. You can rearrange the order by dragging the server to a different position using the drag-and-drop icon.
5. Click **Save**.

Configuring TACACS Server on AOS-CX

To configure a TACACS server, complete the following steps:

1. In the **Authentication Servers** table, point to the **TACACS** server row and click the edit icon. The TACACS servers page is displayed with the list of TACACS servers configured on the switch.
2. To add a TACACS server, click **+**.

   The Add TACACS window is displayed.

3. Configure the following parameters:

Table 186: *TACACS Parameters*

Name	Description	Value
FQDN or IP address	The IP address or fully qualified domain name of the TACACS server.	
Shared secret	The encryption key to be used during authentication sessions with the specified TACACS server.	You can enter up to a maximum of 32 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Authentication Port	The authentication port number for the specified TACACS server.	Range: 1-65535 Default: 49
Timeout (secs)	The number of seconds to wait for a response from the TACACS server before trying the next TACACS server.	Range: 1-60 Default: 5
VRF	The VRF to be used for communicating with the TACACS server.	**Default** and **Management**

4. Click **Apply**. The added server is displayed in the TACACS servers page.

   The server that was added first is accessed first, and if necessary, the second server is accessed second, and so on. You can rearrange the order by dragging the server to a different position using the drag-and-drop icon.
5. Click **Save**.

Configuring Authentication on AOS-CX

Aruba Central supports the following authentication methods for AOS-CX switches:

- 802.1X Authentication—Used for authenticating the identity of a user before providing network access. 802.1x authentication consists of three components:
  - Supplicant: Device that tries to access the LAN.
  - Authenticator: A network device, such as an Ethernet switch that authenticates the supplicant.
  - Authentication Server: Typically a host running software supporting the RADIUS and EAP protocols that provides an authentication service to the authenticator.
- MAC Authentication—Used for authenticating devices based on their physical MAC addresses. For MAC authentication, the MAC address of a machine must match an approved list of MAC addresses defined on the RADIUS server.

At the global level, **802.1X Authentication** uses the **EAP** (Extensible Authentication Protocol) mode to communicate with the RADIUS server. In the case of **MAC authentication**, you can either select **PAP** (Password Authentication Protocol) mode or **CHAP** (Challenge-Handshake Authentication Protocol) mode to communicate with RADIUS servers.

You must configure at least one RADIUS server to use 802.1X or MAC authentication.

To configure authentication at port level, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. Click **Security** > **Authentication**.

   The Authentication page is displayed.
3. In the **Ports** table, select one or more ports for which you want to configure authentication, and click the edit icon.

   The Edit Ports page is displayed.
4. Configure the following parameters:

   Table 187: *Configuring Authentication*

Name	Description	Value
Authentication	The method of authentication.	Select any one of the following authentication methods: ■ **None**—Disables authentication. By default, the authentication is disabled. ■ **802.1X**—Enables 802.1X method for authentication. ■ **MAC**—Enables MAC method for authentication ■ **802.1X, then MAC**—Enables both 802.1X and MAC authentication methods and sets the precedence to 802.1X authentication. ■ **MAC, then**

Name	Description	Value
		802.1X—Enables both 802.1X and MAC authentication methods and sets the precedence to MAC authentication.
Client Limit	The maximum number of clients to be allowed on the port.	Enter up to a maximum of 256 clients. Default: 1
Reauthentication Timeout	The time (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the re-authentication occurs. By default, this field is disabled and the default value is displayed. To edit the default value, select the check box and specify the value.	Default: 3600 seconds
Cached Reauthentication Timeout	The time (in seconds) when cached re-authentication is allowed on the port. By default, this field is disabled and the default value is displayed. To edit the default value, select the check box and specify the value.	Default: 30 seconds
Quiet Period	The time (in seconds) during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails.	Default: 60 seconds

5. Click **Apply**. The authentication parameters are displayed in the **Ports** table.
6. Click **Save**.

Configuring Access Control on AOS-CX

Access control allows you to permit or deny traffic based on network addresses, protocols, service ports, and other packet attributes. An Access policy defines a set of rules based on network traffic addressing and uses these rules to permit or deny the passage of traffic through the switch. The permit action allows the traffic to continue through the switch and the deny action causes the traffic to be discarded (dropped).

From the Access Control page, you can add access policies and set different rules for the access policies using UI groups.

Adding an Access Policy

You can add access policies by defining traffic rules. A policy can be applied to an individual front plane port, a Link Aggregation Group (LAG) interface, or a VLAN.

To add an access policy, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
  a. Set the filter to **Global** or a group containing at least one switch.
  b. Under **Manage**, click **Devices** > **Switches**.
     A list of switches is displayed in the **List** view.
  c. Click an AOS-CX switch under **Device Name**.
     The dashboard context for the switch is displayed.
  d. Under **Manage**, click **Device**.
     The AOS-CX UI configuration page is displayed.

2. Click **Security** > **Access Control**.
   The Access Control page is displayed with the name of the policy.
3. In the **Access Control** table, click **+** to add a policy.
   The Add policy page is displayed.
4. Configure the following parameters:

Table 188: *Access Policy Parameters*

Name	Description	Value
Name	The name of the access policy.	A maximum of 64 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Direction	The traffic direction for Ports and LAGs. The available directions are: ■ **Inbound**—Controls the incoming traffic on the selected ports or LAGs. ■ **Outbound**—Controls the outgoing traffic on the selected ports or LAGs.	**Inbound** or **Outbound**
Ports & LAGs	The ports and LAGs on which the policy is applied.	Select a value from the drop-down list.
Direction	The traffic direction for VLANs. The available directions are: ■ **Inbound**—Controls the incoming traffic on the layer 2 interface VLANs. ■ **Outbound**—Controls the outgoing traffic on the layer 2 interface VLANs. ■ **Routed Inbound**—Controls the incoming traffic on the layer 3 interface VLANs. ■ **Routed Outbound**—Controls the outgoing traffic on the layer 3 interface VLANs.	**Inbound**, **Outbound**, **Routed Inbound**, or **Routed Outbound**.
VLANs	The VLANs on which the policy is applied. The list of layer 2 and layer 3 interface VLANs are displayed based on the **Direction** selection.	Select one or more VLANs from the drop-down list.

5. Click **Apply**. The Access Control table is displayed with the number of ports & LAGs, and VLANs configured on inbound and outbound traffic.

Editing an Access Policy

To edit a policy, point to the row for the policy, and click the edit icon.

Deleting an Access Policy

To delete a policy, point to the row for the policy, and click the delete icon.

Adding a Rule for Policy

You can add access rules for a policy to either allow or deny the traffic passing through the switch.

To add a access rule, complete the following steps:

1. In the **Access Control** table, select the policy for which you want to add a rule by clicking on the policy.

   The Policy Rules page is displayed.
2. In the **Policy Rules** table, click **+** to add a rule.

   The Add rule for policy "<*policy name*">page is displayed.
3. Configure the following parameters:

Table 189: *Access Rules Parameters*

Name	Description	Value
Action	The action for the traffic passing through the switch.	**Permit** or **Deny**
Description	Description for the rule.	A maximum of 256 characters including letters, numbers, and special characters, except question mark (?) and double quotes (").
Source type	The type of source for which you want to apply a policy.	**Any**, **Network**, or **Host**. If you select Network, enter the IP address and Mask . If you select Host, enter the IP address.
Destination type	The type of destination for which you want to apply a policy.	**Any**, **Network**, or **Host**. If you select Network, enter the IP address and Mask . If you select Host, enter the IP address.
Protocol	The type of data transfer protocol. If you select SCTP, TCP, or UDP the Source port and Destination port fields are displayed.	Protocol types: **Any**, **AH**, **ESP**, **GRE**, **ICMP**, **IGMP**, **IP**, **OSPF**, **PIM**, **SCTP**, **TCP**, and **UDP**.

Name	Description	Value
Source Port	The port numbers of source. You can specify a single port in the **Source Port** field or range of ports in the **Source Port** and **Source Port Max** fields. For example, if you want to specify the source port range as 1 to 7, then specify 1 in the **Source Port** field and 7 in the **Source Port Max** field.	An integer
Source Port Max	The end port number in the range of source ports. This field is applicable only if you want to configure a range of source ports.	An integer
Destination Port	The port numbers of destination. You can specify a single port in the **Destination Port** or range of ports in the **Destination Port** and **Destination Port Max** fields. For example, if you want to specify port range as 1 to 7, then specify 1 in the **Destination Port** field and 7 in the **Destination Port Max** field.	An integer
Destination Port Max	The end port number in the range of destination ports. This field is applicable only if you want to configure a range of destination ports.	An integer

4. To create another rule , select **Stay and create another** check box and add a new rule.
5. Click **Apply**. The new rules are displayed in the Policy Rules table.
   By default, the rules are sequenced in the order in which they are added. You can rearrange the sequence by dragging the rule to the position you want using the drag-and -drop icon.
6. Click **Save**.

Editing a Rule

To edit a rule, point to the row for the rule, and click the edit icon.

Deleting a Rule

To delete a rule, point to the row for the rule, and click the delete icon.

Configuring VLANs on AOS-CX

VLANs are primarily used to provide network segmentation at layer 2. VLANs enable the grouping of users by logical function instead of physical location. VLANs make managing bandwidth usage within networks possible by:

- Allowing grouping of high-bandwidth users on low-traffic segments
- Organizing users from different LAN segments according to their need for common resources and individual protocols

- Improving traffic control at the edge of networks by separating traffic of different protocol types
- Enhancing network security by creating subnets to control in-band access to specific network resources

From VLANs page, you can add VLANs and manage VLAN settings such as name, description, admin status, and IP assignment for AOS-CX switches.

For AOS-CX 6200 and 6300 switch series, VLAN 1 (DEFAULT_VLAN_1) is associated with all interfaces on the switch. The DHCP assignment of IP address is available only on the default VLAN.

You can add only one VLAN at a time.

Adding a VLAN

To add a VLAN, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click an AOS-CX switch under **Device Name**.
        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
        The AOS-CX UI configuration page is displayed.
2. Click **Bridging** > **VLANs**.
   The VLANs page is displayed with a list of VLANs.
3. In the **VLANs** table, click **+** to add a VLAN and configure the following parameters.

Table 190: *Configuring and Viewing VLAN Parameters*

Name	Description	Value
ID	The VLAN ID number.	Following are the different ranges for the VLANs: ■ AOS-CX 6200, 6300, and 8360 switch series—2 to 4094 ■ AOS-CX 8320 and 8325 switch series—2 to 4040 ■ UI group-level context —2 to 4094

Name	Description	Value
Name	The name of the VLAN.	Only letters (a-z) and numbers (0-9) are allowed.
Description	The description of the VLAN.	Letters, numbers, and special characters are allowed except question mark (?) and double quotes (").
Admin UP	The operational status of the VLAN. The VLAN can forward packets only when the check box is selected.	Select the check box to enable.
Voice	The VLAN support for voice.	Select the check box to enable.
IP Assignment	The method of IP assignment. The options to enter the IP address is displayed only when you select **Static**. This field is available only at the device level. **NOTE:** The DHCP option is available only for the default VLAN on AOS-CX 6200 and 6300 switch series.	**Static**, **DHCP**, or **None** Default: **None**
IP Address	The IP address with subnet mask for IP assignment. This field is enabled only when you select **Static** from the **IP address assignment** drop-down and available only at the device level.	IPv4 address or IPv6 address with subnet mask Format: (x.x.x.x/x).
DHCP Relay	The IP address of the DHCP relay server. This field is enabled only when you select **DHCP** or **Static** from the **IP address assignment** drop-down and available only at the device level. This option is not available for AOS-CX 6200 switch series.	IPv4 address

4. Click **Add**.

   The VLAN information is displayed in the VLANs table.

Editing a VLAN

To edit a VLAN, point to the row for the VLAN, and click the edit icon. You can select only one VLAN at a time for editing.

You cannot edit the name of the default VLAN and admin status.

Deleting a VLAN

To delete a VLAN, point to the row for the VLAN, and click the delete icon. Deleting VLAN at device level and modifying configuration at group level will not add the VLAN again on the device. You can select only one VLAN at a time for deleting.

You cannot delete the default VLAN.

Configuring Loop Prevention on AOS-CX

Loop prevention provides protection against infinite loops by transmitting loop protocol packets out of the switch ports. You can enable loop prevention by configuring one of the following methods:

- Loop protection at the interface level (ports, LAGs).

  Loop protection at the interface level:
  - can find loops by sending loop protection packets on each port or LAG on which loop protection is enabled.
  - is useful when spanning tree protocols cannot prevent loops at the edge of the network.
  - can be used to find loops in untagged layer 2 links and on tagged VLANs.
  - can be configured either when the spanning tree protocol is configured on the interfaces or not.
- Spanning tree protocol at both global and interface level.

  Spanning tree protocols such as MSTP and RPVST help prevent loops in networks by blocking redundant links.

Loop protection and spanning tree are always disabled by default on AOS-CX switches. To configure loop protection and spanning tree for switches provisioned in the UI groups, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. Click **Bridging** > **Loop Prevention**. The Loop Prevention page is displayed.

   The **Ports** table displays the following information:

   Table 191: *Information in the Ports Table*

Column	Description
Number	Port number or the name of the LAG.
Description	Description of the port or LAG interface that you configure on the **Ports & Link Aggregations** page.
LAG Members	List of port numbers that are grouped to form the LAG.

Column	Description
Loop Protection	Displays whether loop protection is enabled or disabled for that interface.

3. To enable spanning tree, move the **Spanning Tree** toggle switch to the on position.

   Configure the following parameters:

   - **Mode**—Select **MSTP** from the drop-down list.

     You can configure various MSTP parameters for the ports in the switches.

You cannot select **RPVST** from the **Mode** drop-down. To configure RPVST mode for spanning tree, you must use Edit Config in the **MultiEdit** mode and configure using the CLI commands.

However, after configuring the mode as **RPVST**, if you want to change the mode to MSTP, you can select **MSTP** in the **Mode** drop-down.

   - **Priority**—Priority of the UI group.

     At the group level, the priority is listed in multiples of 4096. A range from `0` to `61440` is supported. The default value is `32768`.

4. To configure MSTP parameters for ports, select the row(s) in the **Ports** table and click the edit icon.

The Loop Prevention page is displayed with the following parameters.

Table 192: *MSTP Parameters for Ports and LAGs*

Parameters	Description
Loop Protection	Move the toggle switch to enable or disable loop protection on the interfaces.
Spanning Tree	
Priority	A number used to identify the root bridge in an STP instance. The priority is listed in multiples of `16` in the drop-down. The priority ranges from `0` to `240`. The default priority is `128`. The switch with the lowest value has the highest priority and is considered the root bridge. A higher numerical value means a lower priority; thus, the highest priority is `0`.
BPDU Protection	Security feature used to protect the active STP topology by preventing manipulated BPDU packets from entering the STP domain. Select the check box to enable BPDU protection on the interface.
BPDU Filter	Enables control of STP participation for each port. The feature can be used to exclude specific ports from becoming part of STP operations. A port or LAG with the BPDU filter enabled ignores incoming BPDU packets and stays locked in the STP forwarding state. Select the check box to enable BPDU filter on the interface.
Admin-Edge	Configures the interface in the forwarding state. Select the check box to enable Admin edge on the interface. **NOTE:** If Admin edge is not configured on the switch, the default port type is admin-

Parameters	Description
	network.
Root Guard	Configures the interface to prevent from being configured as a root port when it receives superior STP BPDUs. Select the check box to enable root guard on the interface.

5. To save the changes, click **Apply**.

Using MultiEdit View for AOS-CX

This section describes the configuration and viewing procedures for the AOS-CX switches in the MultiEdit mode.

To configure or view details of the switches provisioned in UI groups, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.

   The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.

At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.

   For more information about search queries, see Using Device Search on AOS-CX.

   The following table describes the columns in the **Devices** table.

Table 193: *Columns in the Devices Table in the MultiEdit Mode*

Column	Function
Name	Name of the AOS-CX switch.
Firmware Version	Firmware version installed on the switch.
Config Modified	Timestamp when the configuration on the switch was last modified.
Status	Status of the switch, whether **Online** or **Offline**.
Config Status	Status of the configuration sync between Aruba Central and the switch. ■ **Sync**—Configuration is in sync between Aruba Central and the switch. ■ **Not in sync (Connection error)**—Configuration is not in sync due to a connection error. ■ **Not in sync (Modified outside Central)**—Configuration is not in sync because configuration was modified outside Aruba Central. ■ **Not in sync (Pushing config)**—Configuration is not in sync because Aruba Central is still pushing configuration to the switch.
NAE Status	Consolidated status of the NAE agents running on the switch. Following are the supported values: ■ **Critical**—The agent has encountered a critical error during execution. ■ **Major**—The agent has encountered a major error during execution. ■ **Minor**—The agent has encountered a minor error during execution. ■ **Normal**—The agent is actively monitoring network conditions and handling events. ■ **Disabled**—The agent is disabled. ■ **Unknown**—The agent status is unknown.
MAC Address	MAC address of the switch.
IP Address	IP address of the switch.
Serial	Serial number of the switch.
Model	Model number of the switch.

The MultiEdit mode provides an option to view or edit switch configuration or apply predefined configurations to the switches.

- Viewing Configuration on AOS-CX
- Editing Configuration on AOS-CX
- Express Configuration on AOS-CX

Viewing Configuration on AOS-CX

View configuration of switches and find differences in the configuration across switches in the MultiEdit mode.

To view switch configuration in the MultiEdit mode, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.

   The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.

At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**. Go to step 6.

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.

   For more information about search queries, see Using Device Search on AOS-CX.
4. In the **Devices** table, select one or more switches by clicking the corresponding rows.

   A pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.
5. To view the configuration of switches, click **View Config**.
   - If you select a single switch, the View Configuration page is displayed. The running switch configuration is displayed in the **Configuration** window.
   - If you select multiple switches, the View Multi-Device Configuration page is displayed with the following panes:
     - **Devices**—Lists the selected switch names.
       Select the switches for which you want to view the configuration by selecting the corresponding check box.
     - **Configuration**—Displays the aggregate running configuration of all selected switches.

   The following features are supported in the view page:
   - Configuration that is same across all switches is displayed as normal text.
   - Differences in configuration is displayed as one of the following:
     - Highlighted parameters (in green)—When parameter value differs across switches. Hover over the parameter to view the list of switches that have this parameter.
     - Entire line differences—Entire line differences are displayed by highlighting the lines along with a description mentioning the switch name that has this line in the configuration. When more

than one switch contains this line, a summary of the number of switches is displayed. For example, 2/7 is displayed if two out of seven switches that are selected contain this line in the configuration. To view the list of switches, hover over this summary.

To view the values of these parameters, right click on the parameter. The **View Parameters** pane is displayed. If the parameter is already configured on a switch, the value is displayed. Else, **N/A** is displayed.

Editing Configuration on AOS-CX

Edit configuration for one or more switches in the MultiEdit mode. Edit the entire configuration in a familiar looking CLI with syntax checking, colorization, and command completion.

To edit and review switch configuration in the MultiEdit mode, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.

   The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.

At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**. Go to step 6.

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.

   For more information about search queries, see Using Device Search on AOS-CX.
4. In the **Devices** table, select one or multiple switches by clicking the corresponding rows.

   A pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**.
5. To edit the configuration of switches, click **Edit Config**.
   - If you select a single switch, the Edit Configuration page is displayed.
   - If you select multiple switches, the Edit Multi-Device Configuration page is displayed with the following panes:

- **Devices**—Lists the selected switch names.

  Select the switches for which you want to edit the configuration by clicking the row corresponding to the switches.
- **Configuration**—Displays the aggregate running configuration of all switches.

In both the pages, the following views are available:

- **Editor View**—Displays the aggregate running configuration on the switches in the **Configuration** pane. Edit the configuration in this view.

  When editing multiple switches, the **Devices** pane is also displayed. Select the check box for the switches you want to edit. The following features are supported in the **Editor View**:
  - Configuration that is same across all switches is displayed as normal text.
  - Differences in configuration is displayed as one of the following:
    - Highlighted parameters (in green)—When parameter value differs across switches. Hover over the parameter to view the list of switches that have this parameter.
    - Entire line differences—Entire line differences are displayed by highlighting the lines along with a description mentioning the switch name that has this line in the configuration. When more than one switch contains this line, a summary of the number of switches is displayed. For example, 2/7 is displayed if two out of seven switches that are selected contain this line in the configuration. To view the list of switches, hover over this summary.

    To modify the values of these parameters, right-click the parameter. The **Modify Parameters** pane is displayed.
    a. If the parameter is already configured on a switch, you can modify the value. Otherwise, **N/A** is displayed for the value and it cannot be modified.
    b. If you want to apply the same value to all selected switches, select the **Set same value for all devices** check box.
    c. To save the changes click **Save Changes** in the **Modify Parameters** pane.

  Clicking **Save** at the bottom of the **Editor View** discards the changes made in the **Modify Parameters** pane.

  - Command completion and help text are available by pressing the CTRL+SPACE key combination.
    An inline drop-down is displayed with the available commands or parameters within commands. To insert a command or parameter, select an option and press TAB.
  - Syntax errors are marked (in red) directly under the incorrect text.
  - If a command line is not inserted in the correct position, the line is automatically moved to the correct position in the configuration.
    For example, if the configuration contains information for VLAN IDs 1 to 3, and you are adding VLAN 4 after VLAN 1 in the configuration, the editor moves the VLAN 4 command line after VLAN 3.
- **Diff View**—Displays the difference between changes made in the **Editor View** and the running configuration on a switch. In this view, two panes, **Running** and **Candidate**, are displayed. When viewing details of multiple switches, select a switch from the drop-down.
  - The **Running** pane displays the running configuration on the switch.
  - The **Candidate** pane highlights the changes made in the **Editor View** in addition to displaying the running configuration on the switch. You cannot edit the switch configuration in this view.

6. Edit the configuration in the **Editor View**, and click **Save**.

Express Configuration on AOS-CX

Express configuration provides a way to efficiently apply a predefined set of configuration settings to switches. Each set of configuration settings can contain settings for Network Analytics Engine (NAE) or device profile features.

To apply express configuration, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.
2. To enable MultiEdit mode, move the **MultiEdit** toggle switch to the on position.

   The **Device-Level Configuration** page is displayed with the list of devices displayed in the **Devices** table.

At the device level, the **Devices** table lists only the switch that you have selected. Also, a pop-up is displayed on the bottom-right corner of the page with the options **View Config**, **Edit Config**, and **Express Config**. Go to step 6.

3. Search for a switch by entering a search query in the **Contextual Search Engine** field.

   For more information about search queries, see Using Device Search on AOS-CX.
4. In the **Devices** table, select one or more switches by clicking the corresponding rows.

   A pop-up is displayed on the bottom-right corner of the page with options **View Config**, **Edit Config**, or **Express Config**.
5. Click **Express Config**.

   The Express Config (N) window is displayed. Where N represents the number of switches selected.
6. Select the required feature from the drop-down. The following features are supported:
   - Device Profile
   - Network Analytics Engine

7. Configure the following parameters corresponding to the selected feature:

Table 194: *Device Profile Parameters*

Name	Description	Value
Enable	Enables or disables the device profile configuration on the switches.	Select or clear the check box.
Profile Name	Name of the device profile.	This field is pre-configured and cannot be edited.
VLAN Mode	VLAN mode for the device profile. Depending on the VLAN mode, configure one of the following: ▪ **Access**: ◦ **Access vlan**—ID of the access VLAN. ▪ **Trunk:** ◦ **Native vlan—**ID of the native VLAN. ◦ **Allowed vlan list—**Single or a range of allowed VLAN IDs.	Integer in the range `1` to `4094`.
PoE Priority	PoE priority for the device.	**Low**, **High**, **Critical**
Allow Jumbo frames	Enables or disables processing of jumbo frames by the switches.	Select or clear the check box.

Table 195: *Network Analytics Engine Parameters*

Name	Description
NAE Script Name	Name of the NAE script. You can also configure the agent parameters. The following NAE scripts are supported: ▪ **software_device_health_monitor.1.6**—Monitors overall software device health. ▪ **hardware_device_health_monitor.1.6**—Monitors overall hardware device health. ▪ **application_health_monitor.1.1**—Monitors application health using TCP SYN and ACK packets, and VoIP IP SLA sessions. ▪ **network_health_monitor.1.3**—Monitors overall network health of device. ▪ **stp_health_monitor.3.1**—Monitors health of ports that are involved in spanning tree protocol.

8. Click **Save**.

You can view the express configuration that you apply in the **Configuration Status** page if the **Auto-Commit** state is off, or in the **View Config** page if the **Auto-Commit** state is on. For more information on viewing the pending changes, local overrides, and the configuration status, see Using Configuration Status on AOS-CX.

Using Device Search on AOS-CX

In the MultiEdit mode, the Contextual Search Engine allows you to filter a set of AOS-CX switches using search queries. The search queries can contain one or more search terms in the format, label:value. For example: model:6300F, where model is the label and 6300F is the value. When a search query contains a list of terms, by default, all terms are required to match. For example, the search query "model:8400 current-

firmware:10.04.0001" will return only 8400 switches running 10.04.0001 firmware. The filtered switch details are displayed in the Devices table.

The search queries can contain the following information:

- Device attributes—Attributes that denote the device details such as the model and current-firmware.
- Wildcard characters—Asterisk (*) and question mark (?) are allowed in search queries.
- Boolean operators—For complex queries, you can use the boolean operators AND, OR, NOT, + (the plus sign), and - (the minus sign).
- Grouping characters—Multiple search terms with logical operators can be grouped using parenthesis ().

You must use quotes (" ") for any strings with spaces and for the default, running-config, and startup-config search. A default search is specified by entering quoted text instead of a label:value search term. The default search runs the search against the running configurations of the devices. For example, entering "ntp server172.16.0.100" searches for that string in the running configuration of all managed devices in the MultiEdit mode. Multiple search terms can be used in a query and can be combined using logical operators.

Searching for Devices

To access Contextual Search Engine and perform search, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one switch. The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon to view the switch configuration dashboard.
4. Slide the **MultiEdit** toggle switch to the on position to enable MultiEdit mode. The **Devices** table displays the list of devices in the selected group.
5. Hover over the values in the table cells to view the labels that can be used in the search query. For example, if you hover over a cell in the Status column, a pop-up is displayed with the label that can be used in the search term and an example.
6. In the **Contextual Search Engine** field, enter a search query, and click **Search & Filter** to filter a set of switches. The Devices table lists the devices that match the search query.

Device Attributes

The following table lists the field names that can be used in the search query as device attributes.

Table 196: *List of Field Names*

Field Name	Definition	Example
active-image	Active image location	active-image:primary
chassis	Name of the chassis if available	chassis:1
config-auto-commit	Configuration auto commit state	config-auto-commit:On config-auto-commit:Off
config-failure-reasons	Reason for configuration failure when the configuration-state is "Not in sync"	config-failure-reasons:”Connection error” config-failure-reasons:"Configuration conflicts" config-failure-reasons:"Internal error" config-failure-reasons:"Modified outside Central" config-failure-reasons:"Initial group config pending" config-failure-reasons:"Pushing config"

Field Name	Definition	Example
		config-failure-reasons:"Connection error with pending changes" config-failure-reasons:"Auto commit off"
configuration-state	Configuration sync state	configuration-state:Sync
current-firmware	Current firmware version	current-firmware:10.02.0001
default-image	Default image location	default-image:secondary
fabric-card	Name of the fabric cards, if available	fabric-card:1\/1
firmware-version	Firmware version on the device	firmware-version:FL.10.1
hw-serial	Serial number of attached hardware	hw-serial:TW0989W
ip-address	Management IP address	ip-address:172.16.0.100
label	Label assigned to the device	label:Floor1
last-sync-time	Last time when configuration in central and device are in sync	last-sync-time:2020-08-27 last-sync-time:2020-08-27T19 last-sync-time:2020-08-27T19:01:20Z last-sync-time:[2020-08-27T19:01:20Z TO *] last-sync-time:[2020-08-27 TO 2020-08-28] last-sync-time:[2020-08-27T20 TO 2020-08-27T23] last-sync-time:[2020-08-27T19:00:00 TO 2020-08-27T23:00:00] last-sync-time:[2020-08-27T11:30:00Z TO 2020-08-27T23:00:00Z]
line-card	Name of the line cards, if available	line-card:1\/1
local-override	Device local override is enabled or not	local-override:Yes local-override:No
mac-address	Base MAC address	mac-address:e7c7dc-32f000
management-module	Name of the management module, if available	management-module:1\/1
manufacturer	Manufacturer name	manufacturer:Aruba
model	Model number	model:6300F
nae-status	NAE status of the switch	nae-status:normal
name	The devices user-defined name	name:cx_6300F_ERIA000001
part-number	Product names of the device and attached hardware	part-number:JL635A

Field Name	Definition	Example
power-supply	Name of the power-supply, if available	power-supply:1V1
primary-version	Primary image version	primary-version:GL.10.11
product-name	Product names of the device and attached hardware	product-name:"8325 Mgmt Mod"
product-number	Product number of the device	product-number:8325
running-config	Contents of the running configuration (this is the default search field)	running-config:"ospf"
running-config-modified	Date and time of latest running configuration change	running-config-modified:2020-08-27 running-config-modified:2020-08-27T19 running-config-modified:2020-08-27T19:01:20Z running-config-modified:[2020-08-27T19:01:20Z TO *] running-config-modified:[2020-08-27 TO 2020-08-28] running-config-modified:[2020-08-27T20 TO 2020-08-27T23] running-config-modified:[2020-08-27T19:00:00 TO 2020-08-27T23:00:00] running-config-modified:[2020-08-27T11:30:00Z TO 2020-08-27T23:00:00Z]
running-deployed-by	User who deployed running configuration	running-deployed-by:system
secondary-version	Secondary image version	secondary-version:GL.10.11
serial	Serial number	serial:SGIA000001
site	Site assigned to the device	site:"Santa Clara"
startup-config	Contents of the start-up configuration	startup-config:"ntp server 192.168.0.7"
startup-config-modified	Date and time of latest start-up configuration change	startup-config-modified:2020-08-27 startup-config-modified:2020-08-27T19 startup-config-modified:2020-08-27T19:01:20Z startup-config-modified:[2020-08-27T19:01:20Z TO *] startup-config-modified:[2020-08-27 TO 2020-08-28] startup-config-modified:[2020-08-27T20 TO 2020-08-27T23] startup-config-modified:[2020-08-27T19:00:00 TO 2020-08-27T23:00:00] startup-config-modified:[2020-08-27T11:30:00Z TO 2020-08-27T23:00:00Z]
startup-deployed-by	User who deployed start-up configuration	startup-deployed-by:system
status	Device status	status:Online status:Offline

Field Name	Definition	Example
system-contact	SNMP system contact	system-contact:JohnSmith
system-location	SNMP system location	system-location:Zurich

Wildcard Characters

Wildcard characters are used in search queries to match one or more other characters. The valid wildcard characters are asterisk (*) and question mark (?).

Use asterisk (*) to match multiple characters in a search query. For example, the search query Serial:SG* will return all the devices starting with SG, such as SG0010223, SG0110224, SG1110225, and so on.

Use question mark (?) to match a single character in a search query . For example, the search query Serial:SG001022? will return all the devices starting with SG001022 series replacing the last digit, such as SG0010221, SG0010222, SG0010223, and so on.

Search queries with wildcard characters must be used without quotes. For example: Serial:SG*.

Reserved Characters

Reserved characters are used for performing operations in search queries. For example, the plus (+) and minus (-) symbols are used as Boolean operators. Parenthesis () is used to group search queries. Reserved characters include + - && || ! ( ) { } [ ] ^ " ~ * ? : \.

If reserved characters appear in searches, then they must be preceded by an escape character such as a backslash (\). If the search terms are enclosed in quotes, then you need not add a backslash (\) before the reserved characters. For example, system-location:"santaclara(office)". If the search terms are not enclosed in quotes, then you must add a backslash (\) before the reserved characters. For example, system-location:santaclara\(office\).

Operators

The following table lists the operators that can be used in search queries.

Table 197: *List of Operators*

Operator	Example	Result
AND	model:8400 AND current-firmware:10.04.000	Returns all 8400 model switches running the 10.04.000 firmware version.

Operator	Example	Result
OR	model:8400 OR current-firmware:10.04.000	Returns all 8400 model switches, all the switches running 10.04.000 firmware version, or both.
NOT	model:8400 NOT current-firmware:10.04.000	Returns all 8400 model switches, but not switches running 10.04.000 firmware version.
+ (Includes)	model:8400 + running-config:"access-list ip hvac_segmentation"	Returns all 8400 model switches that contain the ACL named "hvac_ segmentation" in their running configuration.
- (Excludes)	model:8400 - running-config:"access-list ip hvac_segmentation"	Returns 8400 model switches that do not have the ACL named "hvac_ segmentation" in their running configuration.
( ) (Grouping)	(model:8400 OR model:6300) AND NOT current-firmware:10.04.0001	Returns all 8400 and 6300 model switches that are not running firmware version 10.04.000.

Sample Queries

The following table lists some sample queries that can be used as search queries.

Table 198: *List of Sample Queries*

Query	Result
"ospf"	Switches that contain the string "ospf" in their running configuration file.
model:8400 current-firmware:10.04.0001	Model 8400 switches running firmware version 10.04.0001.
model:8400 -current-firmware:10.04.0001	All 8400 switches that are not running version 10.04.0001.
(model:8400 OR model:6300) AND NOT current-firmware:10.04.0001	All 8400 and 6300 switches that are not running version 10.04.0001.
model:6300 -running-config:"access-list ip hvac_ segmentation"	Model 6300 switches that do not have the ACL named "hvac_segmentation" in their running configuration.
hostname-AUS-05-.*	Devices with a hostname matching the regular expression. For example, in a deployment where host names are encoded as (<site>-<building>-<floor>-<number>).
site:Aruba*	Devices with the Ssite name starting with Aruba.

Using Configuration Status on AOS-CX

Aruba Central provides an audit dashboard for reviewing configuration changes for the AOS-CX switches provisioned in UI groups. The Configuration Status page displays the configuration status of the switches, pending changes, and local overrides present in the AOS-CX switches. It also provides options to push uncommitted changes to the switches.

To view and commit the configuration changes, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to a group.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **AOS-CX** or **Config** icon to view the AOS-CX switch configuration dashboard.
   - To select a switch:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click an AOS-CX switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The AOS-CX UI configuration page is displayed.

2. Click **Configuration Status**.

   The Configuration Status page is displayed with details about the configuration status of AOS-CX switches.

   The page displays the following information at the group and device levels:

   - At the group level:
     - **Auto-commit Changes State** section—Click a number to view corresponding results filtered in the **Auto Commit State** column in the **Switches** table.
       - **Devices auto-commit state**—Count of switches that have the auto-commit state on and off.
     - **Configuration Issues** section—Click a number to view corresponding results filtered in the **Config Status** column in the **Switches** table.
       - **Pending changes**—Count of switches that have configuration changes that are pending commitment to the switch.
       - **Configuration errors**—Count of switches for which errors in the pending configuration caused an attempted commit to fail.

       In the **Config Status** column, click the link corresponding to the status to view the pending changes in a configuration or the **Error - Configuration conflicts** link to view any issues in a pending configuration. For more information, see Viewing and Committing Configuration Issues and Pending Changes at the Group Level.
     - **Local Overrides** section—Click a number to view corresponding results filtered in the **Local Overrides** column in the **Switches** table.
       - **Switches with overrides**—Count of switches that have device level configuration changes.
       - **Switches without overrides**—Count of switches that do not have device level configuration changes.
   - At the device level:
     - **Auto-commit Changes State** section—Enable or disable the auto-commit mode by moving the toggle switch to the on or off position.
       - Toggle switch in the on position—Displays a message that the configuration changes will be committed to the device immediately.
       - Toggle switch in the off position—Displays a message that the configuration changes will not be committed to the device immediately.
     - **Configuration State Issues** section—Displays a message defining the status of configuration on the switch. For a list of all status messages, see the description of the **Config Status** column in Table 199.

       Click the **Pending Changes** link to view the pending changes in a configuration or the **Error - Configuration conflicts** link to view any issues in a pending configuration. For more information, see Viewing and Committing Configuration Issues and Pending Changes at the Group Level.
     - **Overrides** section—Displays a message to indicate whether there are any overrides in the switch configuration at the device level or not.

3. Click the number in the sections to apply the corresponding filter in the **Switches** table.

   The **Switches** table displays the following information:

The **Switches** table appears only at the group level.

Table 199: *Details in the Switches Tables*

Column	Description	Value
Name	Name of the switch.	
Auto Commit State	Status of the auto commit option for the switch.	**On**, **Off**
Config Status	Status of switch configuration between the device and Aruba Central. The following statuses are available: ▪ **Error - Configuration conflicts** ▪ **Error - Internal error** ▪ **Error - Login pending** ▪ **Error - Modified outside Central** ▪ **Offline** ▪ **Pending changes** ▪ **Pending changes - Offline** ▪ **Pending group configuration** ▪ **Synchronized** ▪ **Synchronizing**	
Local Overrides	Indicates whether any overrides exist in the switches.	**Yes**, **No**

Viewing and Committing Configuration Issues and Pending Changes at the Group Level

To view and commit configuration issues and pending changes in AOS-CX switches at the group level, complete the following steps:

1. To view the pending changes in a configuration click the link corresponding to the following statuses in the **Config Status** column for the switch:
   - **Error - Internal error**
   - **Error - Modified outside Central**
   - **Pending changes**
   - **Pending changes - Offline**
   - **Synchronizing**

   The Pending Configuration Changes window is displayed for that switch. This window displays the running and pending configurations of the switch and lets you review the changes made in configuration.
2. Click one of the following buttons depending on the status:
   - Click **Commit Now**—Displayed only when the user has modify permissions for the group, and when auto-commit state is off and there are pending changes but no errors.

     Click this button to push the pending changes to the switch.
   - Click **Close**—Click this button to close the Pending Configuration Changes window without modifying the switch configuration.
3. To view issues with a pending configuration, click the **Error - Configuration conflicts** link in the **Config Status** column for the switch.

The Configuration Conflicts window is displayed for that switch. This window displays a description for each error and the line number in the configuration file where the error has occurred.

The line number displayed in the Configuration Conflicts window might not be same as in the configuration editor. You must look for the correct line in the editor by searching the command where the error occurs.

4. Click **Close**.

Viewing and Committing Configuration Issues and Pending Changes at the Device Level

To view and commit configuration issues and pending changes in AOS-CX switches at the device level, complete the following steps:

1. To view the pending changes in a configuration click the **Pending Changes** link in the **Configuration State Issues** section.

   The Pending Configuration Changes window is displayed for that switch. This window displays the running and pending configurations of the switch and lets you review the changes made in configuration.

   If the pending changes do not have any errors, the **Commit Now** button is displayed, both in the **Configuration State Issues** section and in the Pending Configuration Changes window.
2. Click **Commit Now** to push the pending changes to the switch.
3. To view issues with a pending configuration, click the **Error - Configuration conflicts** link in the **Configuration State Issues** section.

   The Configuration Conflicts window is displayed for that switch. This window displays a description for each error and the line number in the configuration file where the error has occurred.

The line number displayed in the Configuration Conflicts window might not be same as in the configuration editor. You must look for the correct line in the editor by searching the command where the error occurs.

4. Click **Close**.

AOS-CX VSF Stack

A switch stack is a set of switches that are interconnected through stacking ports. By default, the first switch in a stack becomes the Conductor and the second switch in a stack becomes the Standby. The remaining switches become Members of the stack. The following table lists the AOS-CX switches that support stacking:

Table 200: *AOS-CX Switch Stacking Support*

Switch Platform	Maximum Number of Stack Members	Minimum Supported Version	Recommended Version	Supported Stack Type	Supported Configuration Group Type for Stacking (UI / Template)
AOS-CX 6200 Switch Series	8	10.05.0060	10.06.0101	VSF	UI and Template

Table 200: *AOS-CX Switch Stacking Support*

Switch Platform	Maximum Number of Stack Members	Minimum Supported Version	Recommended Version	Supported Stack Type	Supported Configuration Group Type for Stacking (UI / Template)
AOS-CX 6300 Switch Series	10	10.05.0060	10.06.0101	VSF	UI and Template

For more information on topology and configuration of switch stacks, see the *AOS-CX Virtual Switching Framework (VSF) Guide* for the respective switch series.

This section contains the following topics:

- AOS-CX Switch Stacking Functions Supported in Aruba Central
- AOS-CX Switch Stacking Functions not Supported in Aruba Central
- General Recommendations
- Monitoring AOS-CX Switch Stacks
- Viewing AOS-CX Switch Stacks in Site Topology

AOS-CX Switch Stacking Functions Supported in Aruba Central

Aruba Central supports only a few functions of AOS-CX switch stack, such as onboarding a stack to Aruba Central and pushing switch configuration from Aruba Central using UI options, MultiEdit, or templates. All other stacking-topology related activities, such as creating a stack, deleting, or adding a new member to the stack, replacing a stack member, must be performed offline, that is, outside Aruba Central.

The following stacking related functions are supported on Aruba Central:

The AOS-CX switch stack must be set up using the CLI or the AOS-CX mobile application before onboarding on to Aruba Central.

- Onboarding a VSF stack to Aruba Central
- Rebooting a conductor
- VSF switchover

AOS-CX Switch Stacking Functions not Supported in Aruba Central

The following stacking related functions are not supported on Aruba Central and must be performed outside Aruba Central, after taking the stack offline from Aruba Central:

- Setting up an AOS-CX switch stack
- Adding a new member to an existing stack
- Adding a new VSF link
- Deleting a member from the VSF stack
- Splitting or merging a stack
- Replacing a VSF member with same model and part number
- Reassigning standby or other members to the stack

For information on these configurations, see the *AOS-CX Virtual Switching Framework (VSF) Guide* for the respective switch series and the ArubaOS-CX VSF Best Practices document.

General Recommendations

Following are the general recommendations to note when configuring an AOS-CX switch stack:

- To maximize available VSF link bandwidth, use the following DAC cables for VSF links:
  - AOS-CX 6300 Switch Series: 50G
  - AOS-CX 6200 Switch Series: 10G
- All VSF link ports in a stack must operate at the same speed (10G, 25G, or 50G).
- For maximum stack resiliency, the conductor and secondary switches should be the same model with redundant power supplies connected to different circuits. This is required to minimize the probability of a single-source power failure that may disable both the stack conductor and standby switches.
- A secondary member must always be defined to assume the VSF standby role.
- The out-of-band management (OOBM) ports on the conductor and secondary members must be connected to each other, either directly or through a dedicated management network. This is required to utilize the VSF split detection, which must always be enabled.

Monitoring AOS-CX Switch Stacks

See Monitoring Switches and Switch Stacks.

Viewing AOS-CX Switch Stacks in Site Topology

See Monitoring Sites in the Topology Tab.

This section contains the following topics:

Onboarding AOS-CX VSF Stack to Aruba Central

To onboard an AOS-CX VSF stack to Aruba Central, complete the following procedure:

1. Setup the switch stack using the Aruba CX mobile application or the CLI.

   This step must be performed outside Aruba Central.

   For information , see ArubaOS-CX VSF Best Practices. Although this document is created for AOS-CX 6300 switches, it is also applicable to AOS-CX 6200 switches.
2. Add and subscribe the conductor, standby, and all members in the AOS-CX stack to Aruba Central. All the switches in the AOS-CX stack must be licensed in Aruba Central.

   For information on adding and subscribing devices, see Onboarding Devices and Managing License Assignments.
3. Create a template group or UI group for the AOS-CX VSF stack in Aruba Central.

In the template group, all user-defined template variables for the conductor and standby devices should contain the same values, to ensure template consistency after a stack failover event. For information on variables for template-based configuration, see Managing Variable Files.

4. Assign the stack members to the template or UI group from any of the following pages:
   - **Device Inventory** page under **Global Settings** in **Account Home**
   - **Groups** page under **Maintain** > **Organization**, in the **Network Operations** app.

   For more information on assigning a stack, see Assigning Devices to Groups.

NOTE

You can move a stack either from a template group to a UI group or from one UI group to another UI group. If you want to move a stack from a UI group to a template group, then you need to re-onboard the stack to Aruba Central.

5. To push switch configurations to the conductor and members in the AOS-CX VSF stack from Aruba Central, use one of the following ways:
   - Template group—Create a configuration template in the template group for the AOS-CX VSF stack.

NOTE

Copy the details of the `show running config` command of the AOS-CX VSF stack from the conductor and paste it in the template. Ensure to update the password in plaintext.

   - UI group—Use UI options and MultiEdit mode in the AOS-CX switch configuration dashboard. The UI options and MultiEdit mode are available only when the AOS-CX VSF stacks are added to a UI group. For more information, see Configuring AOS-CX Switches in UI Groups.

NOTE

Port-specific configurations such as **Ports & Link Aggregations**, **Authentication Servers**, **Authentication**, **Access Control**, **Authentication**, **VLANs**, **Loop Prevention**, and **Static Routing** can be configured on stack members only at the device level.

Replacing an AOS-CX VSF Stack Member (Same Model and Part Number)

Aruba Central allows you to replace a member of the AOS-CX VSF stack only if the switch model and part number are same. You can replace either the conductor, standby, or any other member of the stack.

Replacing the Conductor

To replace the conductor in the VSF stack, complete the following procedure:

1. Disable Aruba Central from the switch CLI.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

2. Shut down the conductor member in the stack.
3. Wait for the standby member to become the conductor.
4. Replace the switch.
5. Configure the new switch and the VSF links to the new switch.
6. Move the VSF link from the old switch to the new switch.
7. Enable Aruba Central from the switch CLI.

   If this does not work, run the `https-server session close all` command.

```
switch(config-aruba-central)# enable
```

OR

```
switch# https-server session close all
```

8. Switchover to the new conductor in the switch CLI.

Replacing the Standby or Other Members

To replace the standby or any other member of the VSF stack, complete the following procedure:

1. Disable Aruba Central from the switch CLI.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

2. Shut down the member in the stack.
3. Configure the new switch and the VSF links to the new switch.
4. Renumber the VSF member using the `vsf renumber-to` command.
   For example, if the member ID of the old switch was `2`, renumber the new VSF member to `2`.
5. Move the VSF link DAC cable from the old switch to the new switch.
6. Enable Aruba Central from the switch CLI.
   If this does not work, run the `https-server session close all` command.

```
switch(config-aruba-central)# enable
```

OR

```
switch# https-server session close all
```

7. Verify the status of the Aruba Central after the new switch reboots.

Removing an AOS-CX VSF Stack Member

You can remove a member from the AOS-CX VSF stack in Aruba Central. It involves completing procedures both in Aruba Central and the switch CLI.

To remove a member in the VSF stack, complete the following procedure:

1. Disable Aruba Central from the switch CLI.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

2. Wait for the stack to display as offline in the List view.
3. Delete the stack from the template group or UI group in Aruba Central.

   See Deleting an Offline Switch.
4. Remove the member from the VSF stack in the switch CLI by running the following commands:

   For example, in a three-member stack, run the following commands to remove member 3.

```
switch# configure
switch(config)# no vsf member 3
The specified switch will be unconfigured and rebooted
Do you want to continue (y/n)? y
```

5. Disconnect the physical VSF links for the member.
6. In the case of template group, update the template in template group Aruba Central with the configuration from the remaining stack.
7. Enable Aruba Central from the switch CLI.

   If this does not work, run the `https-server session close all` command.

```
switch(config-aruba-central)# enable
```

   OR

```
switch# https-server session close all
```

8. In the case of UI group, after enabling Aruba Central, complete the following steps:
   a. Move the stack to the UI group.
   b. Copy the running configuration of the stack to the MultiEdit mode using the **Edit Config** option.
   c. Save the running configuration.

Changing a AOS-CX VSF Stack to Standalone Switches

To change a AOS-CX VSF stack in Aruba Central to standalone switches, complete the following steps:

1. Make a note of the serial numbers of switches that are part of the stack.
2. Disable Aruba Central from the switch CLI.

```
switch# configure
switch(config)# aruba-central
switch(config-aruba-central)# disable
```

3. Wait for the stack to display as offline in the List view.
4. Delete the stack from Aruba Central.

   See Deleting an Offline Switch.
5. Run the `erase all zeroize` command on the switch CLI of the conductor. This causes the switches to will reboot, rollback to factory defaults, and function as standalone switches.
6. On each switch, enable Aruba Central from the switch CLI. The switches will connect back to Aruba Central as standalone devices and will be added to the **default** group. You can verify the serial

number of the switches once they are onboarded and move the switches to template or UI group as required.

```
switch(config-aruba-central)# enable
```

The password for AOS-CX switch will be *SERIALNUM*_central, until the switches are moved to template or UI group and custom password is set.

Chapter 10
AOS-Switches Overview

Aruba switches enable secure, role-based network access for wired users and devices, independent of their location or application. With Aruba switches, enterprises can deploy a consistent and secure access to network resources based on the type of users, client devices, and connection methods.

Aruba Central offers a cloud-based management platform for managing Aruba switch infrastructure. It simplifies switch management with flexible configuration options, monitoring dashboards, and troubleshooting tools.

- Getting Started with AOS-Switch Deployments
- Provisioning Factory Default AOS-Switches
- Provisioning Pre-Configured AOS-Switches
- Using Configuration Templates for AOS-Switch Management
- Configuring or Viewing AOS-Switch Properties in UI Groups
- AOS-Switch Stack
- Monitoring Switches and Switch Stacks

Supported AOS-Switch Platforms

- Aruba Central uses the SSL certificate by GeoTrust Certificate Authority for device termination and web services. As the SSL certificate is about to expire, Aruba is replacing it with a new certificate from another trusted Certificate Authority. During the certificate upgrade window, all devices managed by Aruba Central will be disconnected. After the upgrade, the devices reconnect to Aruba Central and resume their services with Aruba Central. However, for AOS-Switches to reconnect to Aruba Central after the certificate upgrade, you must ensure that the switches are upgraded to the recommended software version listed in Table 201.
- Aruba Central does not support switch software versions below 16.08 release for firmware upgrade. In addition, only the latest three switch software versions of all major release versions will be available for firmware upgrade from Aruba Central. For example, if the latest switch software version released is 16.10.0011, the following versions will be available for firmware upgrade: 16.10.0009, 16.10.0010 and 16.10.0011.
- Changing AOS-Switches firmware from latest version to earlier major versions is not recommended if the switches are managed in UI groups. For features that are not supported or not managed in Aruba Central on earlier AOS-Switch versions, changing firmware to earlier major versions might result in loss of configuration.

The following tables list the switch platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 201: *Supported AOS-Switch Series, Software Versions, and Switch Stacking*

Switch Platform	Supported Software Versions	Recommended Software Versions	Switch Stacking Support	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2530 Switch Series	YA/YB.16.05.0008 or later	YA/YB.16.10.0013	N/A	N/A	N/A
Aruba 2540 Switch Series	YC.16.03.0004 or later	YC.16.10.0013	N/A	N/A	N/A
Aruba 2920 Switch Series	WB.16.03.0004 or later	WB.16.10.0013	Yes **Switch Software Dependency**: WB.16.04.0008 or later	BPS	UI and Template
Aruba 2930F Switch Series	WC.16.03.0004 or later	WC.16.10.0014	Yes **Switch Software Dependency**: WC.16.07.0002 or later	VSF	UI and Template
Aruba 2930M Switch Series	WC.16.04.0008 or later	WC.16.10.0014	Yes **Switch Software Dependency**: WC.16.06.0006 or later	BPS	UI and Template
Aruba 3810 Switch Series	KB.16.03.0004 or later	KB.16.10.0014	Yes **Switch Software Dependency**: KB.16.07.0002 or later	BPS	UI and Template
Aruba 5400R Switch Series	KB.16.04.0008 or later	KB.16.10.0014	Yes **Switch Software Dependency**: KB.16.06.0008 or later	VSF	Template only

Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central.

Table 202: *Supported Aruba Mobility Access Switch Series and Software Versions*

Mobility Access Switch Series	Supported Software Versions
■ S1500-12P ■ S1500-24P ■ S2500-24P ■ S3500-24T	ArubaOS 7.3.2.6 ArubaOS 7.4.0.3 ArubaOS 7.4.0.4 ArubaOS 7.4.0.5 ArubaOS 7.4.0.6

Data sheets and technical specifications for the supported switch platforms are available at: https://www.arubanetworks.com/products/networking/switches/

Getting Started with AOS-Switch Deployments

Before you get started with your onboarding and provisioning operations, browse through the list of AOS-Switches supported in Aruba Central.

Provisioning Workflow

The following sections list the steps required for provisioning switches in Aruba Central.

Provisioning a Factory Default AOS-Switch

Like most Aruba devices, AOS-Switches support ZTP. Switches with factory default configuration have very basic configuration for all ports in VLAN-1. When a new switch (factory default) is powered on, it automatically obtains IP address, connects to Aruba Activate and downloads the provisioning parameters. When the switch identifies Aruba Central as its management entity, it connects to Aruba Central.

To manage switches from Aruba Central, you must onboard the switches to the device inventory and assign a valid subscription.

For step-by-step instructions, see Provisioning Factory Default AOS-Switches.

Provisioning a Pre-configured or Locally-Managed Switch

Pre-configured switches have customized configuration; for example, an additional VLAN or static IP address configured on the default.

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. These switches do not automatically identify Aruba Central as their management platform, therefore you must manually enable the Aruba Central management service on these switches to allow them to connect to Aruba Central.

For step-by-step instructions, see Provisioning Pre-Configured AOS-Switches.

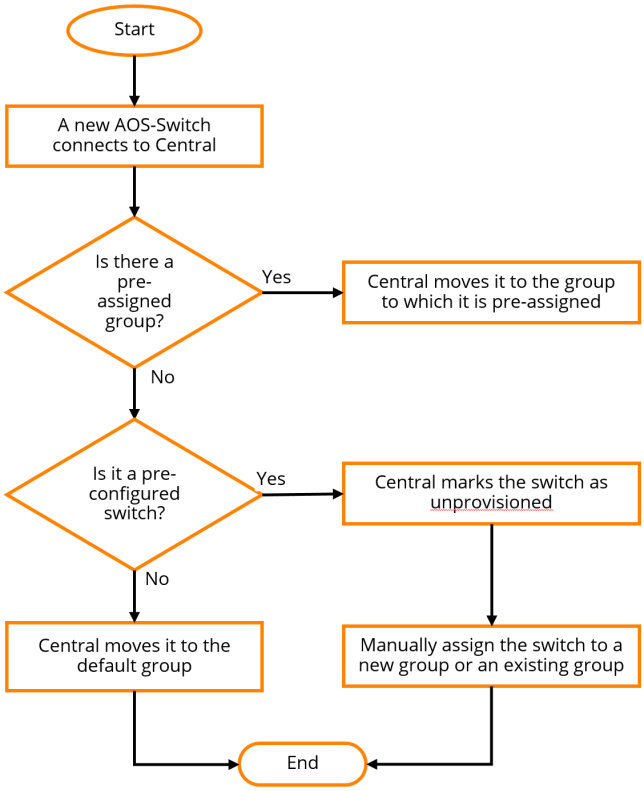
Group Assignment

Aruba Central supports provisioning switches in one of the following types of groups:

- UI group—Allows you to customize and manage device parameters using the UI workflows, that is, the menu options and tabs available under **Network Operations**.
- Template Group—Allows you to configure devices using CLI-based configuration templates.

The following figure illustrates the group assignment workflow in Aruba Central:

Figure 149 *Group Assignment-Switches*



Configuration and Management

Aruba Central supports managing switch configuration using UI workflows or configuration templates. Based on your configuration requirements, ensure that you assign switches to either UI group or template group.

For more information on managing switches in Aruba Central, see the following topics:

- Using Configuration Templates for AOS-Switch Management
- Configuring or Viewing AOS-Switch Properties in UI Groups

Switch Monitoring

To view the operation status of switches and health of wired access network:

- In the **Network Operations** app, use the filter to select a group that has switches.
- Under **Manage**, click **Devices** > **Switches**.

For more information, see Monitoring Your Network on page 1671.

Troubleshooting and Diagnostics

The **Configuration Audit** page under **Network Operations** > **Device(s)** > **Switches** in the Aruba Central UI displays errors in configuration sync, templates, and a list of configuration overrides. For more information, see Viewing Configuration Status.

To troubleshoot switches remotely, use the tools available under **Network Operations** > **Analyze** > **Tools**. For more information, see Using Troubleshooting Tools.

Provisioning Factory Default AOS-Switches

Switches that run default configuration either after shipped from a factory or a factory reset are referred to as factory default switches. This topic describes the steps for provisioning factory default switches in Aruba Central.

- Step 1: Onboard the AOS-Switch to Aruba Central
- Step 2: Assign the AOS-Switch to a Group
- Step 3: Connect the AOS-Switch to Aruba Central
- Step 4: Provision the AOS-Switch to a Group
- Step 5: Verify the Configuration Status

Step 1: Onboard the AOS-Switch to Aruba Central

To onboard switches to the device inventory in Aruba Central, complete the following steps:

- Log in to Aruba Central
- Add switches to Aruba Central
- Assign Subscriptions

Step 2: Assign the AOS-Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. By default, Aruba Central assigns the factory default switches to default group. You can create a new group and assign switch to the new group.

For more information on creating a group, see Creating a Group.

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**. The Device Inventory page is displayed
2. Select the device that you want to assign to a group.
3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

   To assign a device to a group from the **Network Operations** app:

6. In the **Network Operations** app, set the filter to **Global**.

   The dashboard context for the group is displayed.
7. Under **Maintain**, click **Organization** > **Groups**. The Groups page is displayed.
8. From the devices table on the right, select the device that you want to assign to a new group.
9. Drag and drop the device to the group to which you want to assign the device.

Step 3: Connect the AOS-Switch to Aruba Central

Switches with factory default configuration have very basic configuration for all ports in VLAN-1 that is required for obtaining an IP address and automatic provisioning (ZTP). For ZTP, switches must have a valid IP address, DNS, and NTP configuration.

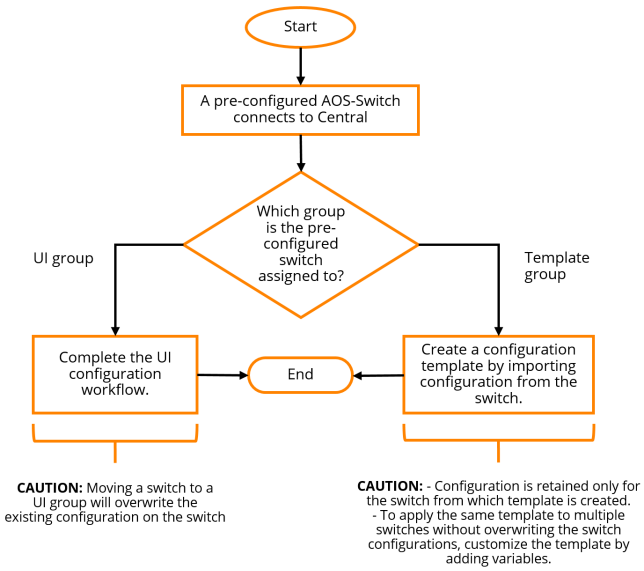
When a factory default switch is powered on and connected to the Internet, it establishes connection with Aruba Activate and downloads the provisioning parameters. If the switch is already added and assigned a subscription, it connects to Aruba Central.

Step 4: Provision the AOS-Switch to a Group

When the switch connects to Central, if it is already added to the device inventory and is assigned a subscription in Aruba Central, Aruba Central assigns it to a pre-assigned group. If there is no pre-assigned group, Aruba Central moves the device to the **default** group. Based on your configuration requirements, you create a UI group or template group and assign the switch.

The following figure illustrates the provisioning step required for each group type.

Figure 150 *Switch Provisioning Steps Per Group Type*



If the switch is assigned to a new UI group, Aruba Central uses the current configuration of switch as base configuration and applies it to the other switches that join this group later. You can also modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Devices** > **Switches**. For more information, see Configuring or Viewing AOS-Switch Properties in UI Groups.

Provisioning AOS-Switches in Template Groups

If you have assigned the switch to a template group, create a new configuration template. To create a configuration template:

1. In the **Network Operations** app, set the filter to a template group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
   The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba Switch**.

8. Select the switch model and software version. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
   - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
   - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Click **Next**. The **Template** tab is displayed.
11. Build a new template or import configuration information from a switch that is already provisioned in the template group.
    - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in Using Configuration Templates for AOS-Switch Management.
    - To import configuration text from a switch that is already provisioned in the template group:
      a. Click **Import Configuration As Template**.
      b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.

- Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements. For more information, see Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates .

  For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.

c. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.

   For more information on variables, see Managing Variable Files.

d. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:
   - **Download .CSV**
   - **Download plain text (.txt)**

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration

Step 5: Verify the Configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.

   The dashboard context for the group is displayed.
2. Click the **Config** icon.

   The tabs to configure switches using templates is displayed.
   - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
   - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
3. To view template errors, click **View Template Errors**.
4. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
5. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Provisioning Pre-Configured AOS-Switches

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. These switches do not automatically identify Aruba Central as their management platform, therefore you must manually enable the Aruba Central management service on these switches to allow them to connect to Aruba Central.

Aruba Central does not support adding pre-configured switches to a UI group. Pre-configured switches that have pre-assigned UI switch groups are added to the Unassigned Devices group. To provision a pre-configured switch to a UI group or move a switch from a template group to a UI group, complete the following steps:

1. Clear the switch configuration.
2. Delete the device from Aruba Central.
3. Provision the switch as a new device in a UI group.

To onboard a locally-managed or a pre-configured switch to Aruba Central, follow one of the following options:

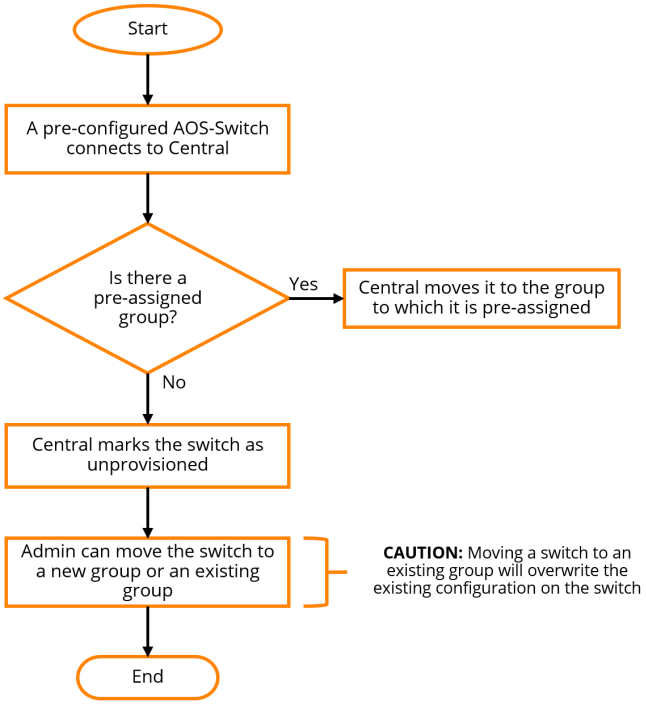
- Manually enable Aruba Central management service on the switch and connect it to Aruba Central. Aruba recommends that you use this option if you want to preserve the current configuration running on the switch. For more information on this procedure, see the workflows described in this topic.
- Reset the switch configuration to factory default and use ZTP to provision the switch. For information on provisioning factory default switches, see Provisioning Factory Default AOS-Switches.
- Aruba Central supports provisioning switches using one of the following methods:
- Pre-provisioning—In this workflow, a switch is added to the device inventory and assigned a group in Aruba Central before it connects to Aruba Central.

  See Workflow 1—Pre-Provisioning an AOS-Switch.
- Onboarding connected switches—In this workflow, Aruba Central onboards the switch that attempts to connect and then assigns a group.

  See Workflow 2—Provisioning an AOS-Switch On-Demand.

The following figure illustrates provisioning procedure for a pre-configured switch.

Figure 151 *Provisioning Workflow for Pre-Configured Switches*



Workflow 1—Pre-Provisioning an AOS-Switch

The pre-provisioning workflow includes the following steps:

- Step 1: Onboard the AOS-Switch to Aruba Central
- Step 2: Assign the AOS-Switch to a Group
- Step 3: Enable Aruba Central Management Service on the AOS-Switch
- Step 4: Provision the AOS-Switch to a Group
- Step 5: Verify the configuration Status

Step 1: Onboard the AOS-Switch to Aruba Central

To onboard switches to the device inventory in Aruba Central, complete the following steps:

- Log in to Aruba Central
- Add switches to Aruba Central
- Assign Subscriptions

Step 2: Assign the AOS-Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. If you want to preserve the existing configuration on the switch, Aruba recommends that you create a new group for the switch.

For more information on creating a group, see Creating a Group.

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
   The Device Inventory page is displayed
2. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization** > **Groups**.
   The Groups page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 3: Enable Aruba Central Management Service on the AOS-Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central, unless it is configured to identify Aruba Central as its management entity. To manage such a device from Aruba Central, you must manually enable the provisioning and management service on the switch.

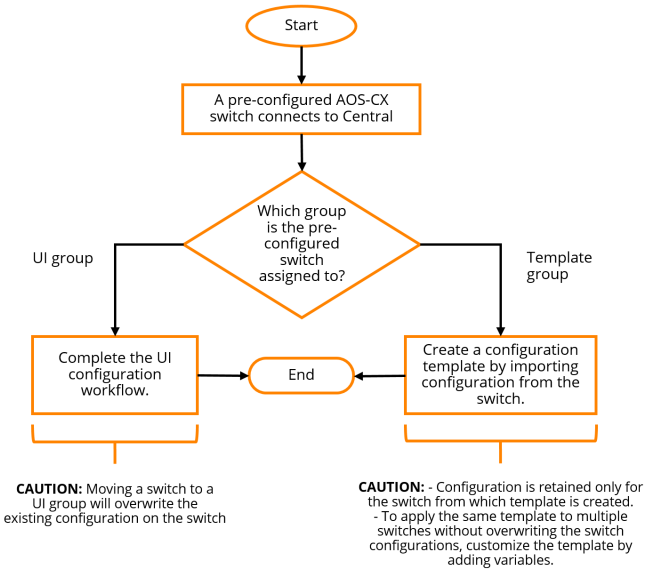
1. Verify if the Activate provisioning service is enabled by executing the following command at the switch CLI:

```
switch)# show activate provision
configuration and Status - Activate Provision Service
Activate Provision Service    : Enabled
Activate Server Address       : device.arubanetworks.com
If the Activate provision service  is not enabled, execute the following
command at the switch CLI:
(switch)# activate provision enable
To enable switches to automatically connect to Aruba Central, enforce ZTP on
the switch:
(switch)# activate provision force
The switch establishes connection with Activate and is directed to Aruba
Central. If the switch is already added to the device inventory and is
assigned a subscription, Aruba Central assigns it to a pre-assigned group.
```

Step 4: Provision the AOS-Switch to a Group

When the switch connects to Aruba Central, Aruba Central automatically assigns it to the pre-assigned group. The following figure illustrates the provisioning steps for each group type.

Figure 152 *Switch Provisioning Steps Per Group Type*



If the switch is assigned to a new UI group, you can modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Devices** > **Switches**. For more information, see Configuring or Viewing AOS-Switch Properties in UI Groups.

If you have assigned the switch to a template group, you can import the existing configuration to a new configuration template and apply this template to other devices in the group. To create a configuration template using the existing configuration on the switch:

1. In the **Network Operations** app, set the filter to a template group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.

   The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba Switch**.
8. Select the switch model and software version. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
   - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.
   - A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.

9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Click **Next**. The **Template** tab is displayed.
11. Build a new template or import configuration information from a switch that is already provisioned in the template group.
    - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in Using Configuration Templates for AOS-Switch Management.
    - To import configuration text from a switch that is already provisioned in the template group:
        a. Click **Import Configuration As Template**.
        b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.
        c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in Using Configuration Templates for AOS-Switch Management.

- Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply only to the switch from which the template was created. To apply the template to multiple switches in the group without overwriting the switch configurations, customize the template by adding variables. For more information on configuration templates and variable definitions, see Using Configuration Templates for AOS-Switch Management and Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates.
  For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.

        d. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.

            For more information on variables, see Managing Variable Files.

        e. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:

- **Download .CSV**
- **Download plain text (.txt)**

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
   The tabs to configure switches using templates is displayed.
   - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
   - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Workflow 2—Provisioning an AOS-Switch On-Demand

To dynamically provision switches on-demand, complete the following steps:

- Step 1: Enable Aruba Central Management Service on the AOS-Switch
- Step 2: Add the AOS-Switch to Aruba Central
- Step 3: Assign a Subscription
- Step 4: Provision the AOS-Switch to a Group
- Step 5: Verify the configuration Status

Step 1: Enable Aruba Central Management Service on the AOS-Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central, unless it is configured to identify Aruba Central as its management entity. To manage such a device from Aruba Central, you must manually enable the provisioning and management service on the switch.

1. Verify if the Activate provisioning service is enabled by executing the following command at the switch CLI:

```
switch)# show activate provision
configuration and Status - Activate Provision Service
Activate Provision Service   : Enabled
Activate Server Address      : device.arubanetworks.com
```

2. If the Activate provision service is not enabled, execute the following command at the switch CLI:

```
(switch)# activate provision enable
```

3. To enable switches to automatically connect to Aruba Central, enforce ZTP on the switch:

```
(switch)# activate provision force
```

The switch establishes connection with Activate. Activate directs the switch to Aruba Central.

Step 2: Add the AOS-Switch to Aruba Central

Add the switch to the Aruba Central device inventory. For more information, see Onboarding Devices.

Step 3: Assign a Subscription

To allow Aruba Central to manage the switch, ensure that a valid subscription is assigned to the switch. For more information, see Managing License Assignments.

Step 4: Provision the AOS-Switch to a Group

If the switch has a valid subscription assigned, Aruba Central marks the switch as **unprovisioned**. To preserve the switch configuration, move it to a new group.

To move the device to a template group:

1. Create a template group.
2. On the **Groups** page, select the switch.
3. Drag and drop the switch to the new template group that you just created. Aruba Central adds the switch to the new template group.
4. To import switch configuration to a new configuration template:
    a. In the **Network Operations** app, set the filter to a template group.
    The dashboard context for the group is displayed.
    b. Under **Manage**, click **Devices** > **Switches**.
    c. Click the **Config** icon.
    The tabs to configure switches using templates is displayed.
    d. Click the **Templates** tab. The Templates page is displayed.
    e. Click **+** to add a new template. The **Add Template** window is displayed.
    f. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
    g. In the **Device Type** drop-down, select **Aruba Switch**.
    h. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
        - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
        - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
        - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.

- A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.

i. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

j. Click **Next**. The **Template** tab is displayed.

k. Build a new template or import configuration information from a switch that is already provisioned in the template group. See step 11.

- Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply only to the switch from which the template was created. To apply the template to multiple switches in the group without overwriting the switch configurations, customize the template by adding variables. For more information on configuration templates and variable definitions, see Using Configuration Templates for AOS-Switch Management and Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates. For more information about using password commands, see the Configuring Username and Password Security chapter in the *ArubaOS-Switch Access Security Guide*.

l. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.

For more information on variables, see Managing Variable Files.

m. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:
- **Download .CSV**
- **Download plain text (.txt)**

n. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the configuration Status

To verify the configuration status:

1. In the **Network Operations** app, set the filter to a template group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.

   The tabs to configure switches using templates is displayed.
   - To verify the configuration status for the template group, click **Configuration Audit**. The **Configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
   - To view configuration errors for a specific device, select a switch from the filter bar. The **Configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **View Details** under **Configuration Status**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Managing Password in Configuration Templates

All IAP and switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the switch does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command.

When configuring a password, you must add the `include-credentials` command in the template. This command stores the password in the **running-config** file associated with the switch. Aruba Central automatically executes this command while reading the switch configuration.
For AOS-CX switches, you must configure the password only in plaintext.

Password for Switches

The following format of the passwords can be set on AOS-Switch series:

```
password manager plaintext &lt;string&gt;
password manager sha1 &lt;string&gt;
password manager sha256 &lt;string&gt;
password manager user-name &lt;string&gt; plaintext &lt;string&gt;
password manager user-name &lt;string&gt; sha1 &lt;string&gt;
password manager user-name &lt;string&gt; sha256 &lt;string&gt;
```

The following format of the passwords can be set on AOS-CX switches:

```
user admin group administrators password plaintext <string>
```

Password for APs

The following format of the passwords can be set on the APs:

```
mgmt-user &lt;STRING:username:User_name&gt; { &lt;STRING:password:Password&gt; }
hash-mgmt-user &lt;STRING:username:User_name&gt; password cleartext
&lt;STRING:cleartext_password:Password&gt;
hash-mgmt-user &lt;STRING:username:User_name&gt; password hash &lt;STRING:hash_
password:Password&gt;
```

Setting Password using Variables

User cannot enter the entire password line in a variable. The following examples show the valid and invalid format for entering password using a variable.

Valid format where the variable contains only the password (for example, `%pass_var% = Aruba@123`) for the device:

```
hostname "Aruba-2930M-24G"
password manager plaintext "%pass_var%"
include-credentials
no cwmp enable
```

Invalid format where the variable contains the password command (for example, `%pass_var% = password manager plaintext Aruba@123`) for the device:

```
hostname "Aruba-2930M-24G"
%pass_var%
include-credentials
no cwmp enable
```

Configuring AOS-Switches

Aruba Central supports provisioning switches in UI and template groups. Aruba Central supports basic configuration options in the UI.

The users can also assign switches to template groups and use configuration templates and variables to manage switches from Aruba Central.

See the following topics for more information on managing switches and switch stacks in Aruba Central:

- Using Configuration Templates for AOS-Switch Management
- Configuring or Viewing AOS-Switch Properties in UI Groups
- AOS-Switch Stack

CA Certificate Installation using API and Templates

This feature is supported for switches with a minimum firmware version of 16.09.

Aruba Central supports the installation of CA certificates through templates and APIs. Typically, an administrator uses an NB API to push the CA certificate to the Aruba Central certificate store. The certificates must be pushed to the certificate store of the same tenant. After that, use the ArubaOS-Switch CLI commands in an Aruba Central template to push the certificate as part of the configuration audit.

If the certificate push or install process is not successful, the Aruba Central audit logs display the specific failure. Only those certificates that are installed through Aruba Central are monitored by Aruba Central. Other switch certificates are not supported for monitoring.

Use the following command to push the CA certificate: `cert-prof name "<name of cert>"`

For example, if the certificate name is **ca_cert_1**, the following is the format of the command: `cert-prof name "ca_cert_1"`.

Points to Note

- Unlike IAPs and Gateways, where a certificate cannot be deleted if it is referenced in a template or a variable, in switches, users can delete a certificate even if it is referenced in a template or a variable.
- Deleting an existing certificate and creating a new certificate with the same name but with different certificate data does not guarantee that the new certificate is installed for switches. Re-apply the template or variable to ensure that the change is propagated.

Using Configuration Templates for AOS-Switch Management

Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple switches in a group and thus automate switch deployments.

To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on AOS-Switch.

Creating a Group for Template-Based Configuration

For template-based provisioning, switches must be assigned to a group with template-based configuration method enabled.

For more information, see Managing Groups and Assigning Devices to Groups.

Creating a Configuration Template

To create a configuration template for switches:

1. In the **Network Operations** app, set the filter to a template group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the **Config** icon.
   The tabs to configure switches using templates is displayed.
4. Click the **Templates** tab. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. In the **Basic Info** tab, enter a name for the template in the **Template Name** field.
7. In the **Device Type** drop-down, select **Aruba Switch**.
8. Select the switch model and software version. You can specify any of the following combinations:
   - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
   - **ALL** for **Model** and a software version for **Version**—To apply the template to all switch models running the selected software version.
   - **ALL** for **Version** and a switch model for **Model**—To apply the template to a switch model and all software versions supported by the selected switch model.

- A switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a switch model and a software version takes precedence over the template that is created for all platforms and versions.

9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

- The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.
- If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.
- If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Click **Next**. The Template tab is displayed.
11. Build a new template or import configuration information from a switch that is already provisioned in the template group.
    - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the Important Points to Note.

      To import configuration text from a switch that is already provisioned in the template group:
      a. Click **Import Configuration As Template**.
      b. From the search box, select the switch from which you want to import the configuration. The imported configuration is displayed in the **Template** text box.
      c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in the Important Points to Note.

- Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements. For more information on variable definitions, see Managing Variable Files.
- All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see Managing Password in Configuration Templates.
  For more information about using password commands, see the Configuring Username and Password Security chapter in the *HPE ArubaOS-Switch Access Security Guide*.

      d. To view the variables present in the imported configuration template, click **Show Variables List**. The Variables in Template column is displayed.

         For more information on variables, see Managing Variable Files.
      e. To download the variables as a CSV or plain text file, click the download icon and select one of the following options:

- **Download .CSV**
- **Download plain text (.txt)**

12. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Important Points to Note

Note the following points when adding configuration text to a template:

- The CLI syntax in the switch template must be accurate. Aruba recommends that you validate the configuration syntax on the switch before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- The commands in the template are case-sensitive.

When configuring a password, you must add the `include-credentials` command in the template. This command stores the password in the **running-config** file associated with the switch. Aruba Central automatically executes this command while reading the switch configuration.

The following example illustrates the case discrepancies that the users must avoid in the template text:

```
trunk E1-E4 trk1 trunk
interface Trk1
  dhcp-snooping trust
  exit

trunk E1-E4 trk1 trunk
switch-interconnect trk1

trunk E5-E6 trk2 trunk
vlan 5
  name "VLAN5"
  untagged Trk2
  tagged Trk1
 isolate-list Trk1
  ip igmp forcedfastleave Trk1
  ip igmp blocked Trk1
  ip igmp forward Trk1
  forbid Trk1

loop-protect Trk2

trunk E1-E4 trk1 trunk
trunk E4-E5 trk2 trunk
spanning-tree Trk1 priority 4
spanning-tree Trk2 admin-edge-port

trunk A2-A4 trk1 trunk
igmp fastlearn Trk1
```

```
trunk E4-E5 trk2 trunk
ip source-binding 2 4.5.6.7 b05ada-96a4a0 Trk2

[no] ip source-binding trap OutOfResources

snmp-server mib hpSwitchAuthMIB ..

snmp-server mib hpicfMACsec unsecured-access ..

[no] lldp config <P-PORT-LIST> dot1TlvEnable ..

[no] lldp config <P-PORT-LIST> medTlvEnable ..
no lldp config <P-PORT-LIST> medPortLocation..

[no] lldp config <P-PORT-LIST> dot3TlvEnable ..

[no] lldp config <P-PORT-LIST> basicTlvEnable ..

[no] lldp config <P-PORT-LIST> ipAddrEnable <lldp-ip>

trunk-load-balance L4-based
trunk-load-balance L3-based
```

Best Practices

Aruba recommends you to follow the below steps to use configuration templates in managing switches:

1. Configure the switch.
2. Add the switch to Aruba Central.
3. Create the template, You can use **Import template** option to import an existing template created for switches.
4. Modify the template based on the user requirement. For example, addition or removal of variables.
5. Save the edited template.

Configuring or Viewing AOS-Switch Properties in UI Groups

This section describes the configuration and viewing procedures for the switches in the UI groups.

Aruba Central does not support adding pre-configured switches to a UI group. Pre-configured switches that have pre-assigned UI switch groups are added to the Unassigned Devices group. To provision a pre-configured switch to a UI group or move a switch from a template group to a UI group, complete the following steps:

1. Clear the switch configuration.
2. Delete the device from Aruba Central.
3. Provision the switch as a new device in a UI group.

To configure or view properties of the switches provisioned in UI groups, perform the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click the **config** icon to edit the switch properties. Tabs to access different configuration pages are displayed.

   The following table describes the different configuration pages and their functions.

Table 203: *Tabs for Configuring Switches Provisioned in a UI Group*

Tab	Function
Switches	Configure or view general switch properties, such as, hostname, type of IP addressing, and so on. See Configuring or Viewing Switch Properties.
Stacks	Create stacks, add members, or view stacking details such as stack type, stack id, topology, and so on. See Configuring AOS-Switch Stacks Using UI Groups.
Ports	Assign or view port properties, such as, PoE, access policies, and trunk groups. See Configuring Switch Ports on AOS-Switches
PoE	Configure or view PoE settings for each port. See Configuring PoE Settings on AOS-Switch Ports.
Trunk Groups	Configure or view trunk groups and their associated properties, such as, members of the trunk group, type of trunk group, and so on. See Configuring Trunk Groups on AOS-Switches in UI Groups.
VLANs	Configure or view VLANs and the associated ports and access policies. See Configuring VLANs on AOS-Switches
Spanning Tree	Configure or view spanning tree protocol and its associated properties. See Enabling Spanning Tree Protocol on AOS-Switches
Loop Protection	Configure or view loop protection and its associated properties. See Configuring Loop Protection on AOS-Switch Ports.
Access Policies	Add or view access policies.

Tab	Function
	See Configuring Access Policies on AOS-Switches.
DHCP Snooping	Configure or view DHCP snooping, authorized DHCP servers IP addresses, and their associated properties. See Configuring DHCP Snooping on AOS-Switches.
Port Rate Limit	View or specify bandwidth to be used for inbound or outbound traffic for each port. See Configuring Port Rate Limit on AOS-Switches.
RADIUS	Configure or view RADIUS (Remote Authentication Dial-In User Service) server settings on switches. See Configuring RADIUS Server Settings on AOS-Switches.
Downloadable User Role	Enable Downloadable User Role option and configure ClearPass settings to download user-roles, policy, and class from the ClearPass Policy Manager server. See Configuring Downloadable User Role on AOS-Switches.
Tunnel Node Server	Configure or view tunneled node on switches. See Configuring Tunnel Node Server on AOS-Switches.
Authentication	Configure or view 802.1X authentication, MAC authentication, and Authentication order and priority for switches. See Configuring Authentication for AOS-Switches.
Access/DNS	Configure or view the administrator and operator logins. See Configuring System Parameters for AOS-Switches.
Time	Configure time synchronization in switches. See Configuring Time Synchronization on AOS-Switches.
SNMP	Configure SNMP versions v2c and v3 on switches. See Configuring SNMP on AOS-Switches.
CDP	Configure CDP and its associated properties. See Configuring CDP on AOS-Switches.
Routing	Configure or view a specific routing path to a gateway. See Configuring Routing on AOS-Switches.
DHCP	Enable DHCP server and add DHCP pools on switches. See Configuring DHCP on AOS-Switches.
IGMP	Configure IGMP and its associated properties. See Configuring IGMP on AOS-Switches.
QoS	Create QoS traffic policies. define QoS classes and change the priorities of traffic on switches. See Configuring QoS Settings on AOS-Switches.
Device Profie	Configure or view device profile settings on switches. See Configuring Device Profile.
Configuration Audit	View configuration sync errors and overrides. See Viewing Configuration Status.

Configuring or Viewing Switch Properties

When you add a switch to a group, the switch inherits the configuration of the group.

It is not recommended to add a switch with an existing configuration to a group that already has a defined configuration. Aruba Central permits device-level overrides, however the overrides are resolved or preserved based on the requirements.

You can create a new group and add a pre-configured switch to that group so that the group inherits the configuration of the switch. If the switch inherits the group configuration, the configuration parameters are already defined. If required, you can edit these parameters. All factory default switches are provisioned in a new group and these parameters can also be defined at the group level.

To edit the configuration parameters for the switch in an UI group, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click the **Switches** tab.
   The **Switches** page is displayed with the following information.

Table 204: *Switches Parameters*

Name	Description	Value
MAC Address	MAC address of the switch.	Property inherited from the switch.
Hostname	Name of the host.	A string.
IP Assignment	Method of IP assignment as static or DHCP.	**Static** or **DHCP**.
IP Address	IP address for static IP assignment.	IPv4 address.
Netmask	Netmask for static IP assignment.	Netmask address.
Default Gateway	Default gateway for static IP assignment.	IPv4 address.
Location	Location of the switch.	For example: Portland, Oregon.

Name	Description	Value
Contact	Email address or phone number.	For example: admin@xyzcompany.com.

3. To edit the switch configuration parameters, select the row you want to edit and click the edit icon. The Edit Switches window is displayed.
4. Edit the required parameters.

In the Switches page, you can edit only Hostname, Location, and Contact information. Use the VLANs page to configure IP Assignment, IP address, Netmask and Default Gateway parameters. For more information, see Configuring VLANs on AOS-Switches.

5. Click **OK**.
6. Click **Save Settings**.

Configuring Switch Ports on AOS-Switches

To view the port details of a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.
        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
        The tabs to configure the switch is displayed.
2. Click **Interface** > **Ports**. The Ports page is displayed with the list of ports configured on the switch.
   For the Aruba Mobility Access Switches, the Ports page displays the following information:

Table 205: *Ports Page—Mobility Access Switches*

Name	Description	Value
Port Number	Indicates the number assigned to the switch port.	Dependent on the type of switch.

Name	Description	Value
Admin Status	Indicates the operational status of the port.	**Up** or **Down**.
Port Mode	Indicates the mode of operation. The port can be configured to function in **Trunk** or **Access** mode.	**Trunk Mode** or **Access Mode**. By default, a port is in **Access** mode and carries traffic only for the VLAN to which it is assigned. In **Trunk** mode, a port can carry traffic for multiple VLANs.
VLAN	Shows the VLAN to which the port is assigned. Based on the port mode, you can assign different types of VLAN.	■ For **Access** mode, an **Access VLAN** can be specified. ■ For **Trunk** mode, the **Native VLAN** and **Allowed VLAN** can be configured.
Auto Negotiation	Indicates the status of the Auto Negotiation.	■ If auto negotiation is enabled, the **Speed** and **Duplex** fields are automatically set to **Auto**. ■ If auto negotiation is disabled, the speed can be set to 10 Mbps, 100 Mbps, or 1 Gbps and the duplex mode can be set to half or full.
Speed/Duplex	Displays the speed and duplex configuration settings for the client traffic.	
Trusted	Indicates if the port is trusted.	

For AOS-Switches, the Ports page displays the following information:

Table 206: *Ports Page—AOS-Switches*

Name	Description	Value
Port Number	Indicates the number assigned to the switch port.	Dependent on the switch type.
Name	Name of the port for easy identification. You can add or edit port names. However, do not delete port names as it may cause config push to fail. The config push failure may also arise if you move a switch from a group configured with port names to a new group. This issue is only applicable to switch firmware versions earlier than 16.08.0002.	For example: UPLINK-SRVR-ROOM.
Admin Status	Allows you to set the operational status of the port.	**Up** or **Down**
Speed-Duplex (Mbps)	Allows you to set the maximum bandwidth of the port traffic.	Select from drop-down menu. Default is **Auto**.
Tunneled	Indicates whether the port is tunneled or not.	**Enable** or **Disable**

Name	Description	Value
		To configure a Tunnel Node Server, see Configuring Tunnel Node Server on AOS-Switches
DHCP Snooping	Status of port to filter DHCP messages received at the port.	**Trust** or **Untrust** See Configuring DHCP Snooping on AOS-Switches.
Access Policy (In)	Allows you to apply an existing access policy for the inbound traffic on the port.	Select from drop-down menu. See Configuring Access Policies on AOS-Switches.
Access Policy (Out)	Allows you to apply an existing access policy for the outbound traffic on the port.	Select from drop-down menu. See Configuring Access Policies on AOS-Switches.
Trunk Group	Displays the name of the trunk group to which the port is assigned.	To configure a Trunk Group, see Configuring Trunk Groups on AOS-Switches in UI Groups.

3. Select the port row, click **Edit**. The Edit Ports window is displayed.
4. Configure the required parameters.
5. Click **Save**.

Support for Flexible Modules and SFP Ports

In Aruba Central, you can manage Flexible modules and SFP ports using template and UI groups. Flexible modules and SFP ports are supported on both standalone switches and switch stacks. In the case of standalone switches in UI groups, the Flexible modules and SFP ports can be managed only if the AOS-Switches are running 16.10.0010 or later firmware versions. These ports are available for configuration at both group and device-levels.

At the group-level, the port numbers for Flexible modules and SFP ports are listed in the Ports page as alphanumeric characters (A1-A4 and B1-B4) . At the device-level, only the ports that are listed in the Ports page can push the configuration updates to Aruba Central.

When you insert a new module, you might need to reboot or re-sync the device to detect the ports in Aruba Central. If the Flexible modules and SFP ports are successfully detected, the audit trail displays the following message: **Additional Alphanumeric SFP ports are detected**. The Flexible modules and SFP ports will not be removed from Central even when the modules are removed physically from the device.

Configuring PoE Settings on AOS-Switch Ports

Power over Ethernet (PoE) is a technology that allows the switches to deliver power to the powered devices (PD). If you have switches provisioned in UI groups, you can enable or disable PoE operation on switch ports. The PoE page displays the configuration details of all PoE enabled ports.

To configure the PoE settings of a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Interface** > **PoE**. The PoE page is displayed.
3. Select the port(s) you want to edit and click **Edit**.
   The **Edit Power Over Ethernet Settings** window is displayed.
4. Configure the following parameters:

Table 207: *PoE Parameters*

Name	Description	Value
Port	The number assigned to the switch port. The port number is auto-generated and cannot be changed in the settings.	Auto-generated port number
PoE	The status of the PoE operation on the port. When PoE is enabled, the switch sends power to the powered device (PD).	Enabled or Disabled
Priority	The PoE priority level of the port. If there is not enough power available to provision all active PoE ports, then PoE ports at priority level as critical are powered first, then high and low priority at the last.	Low, High or Critical
LLDP MED TLV (PoE)	The status of the LLDP MED TLV configuration. Switches use LLDP to repeatedly query the PD to discover the power requirement and send the exact power required.	Enabled or Disabled

Name	Description	Value
LLDP Dot3 TLV (PoE+)	The status of the LLDP Dot3 TLV configuration.	Enabled or Disabled
Allocation By	The PoE power allocation method used for the port. If usage is selected, then the allocation is made based on the automatic allocation by the PD. If class is selected, then the allocation is made based on class of the PD.	Usage or Class
Pre Std Detect	The status of support for pre-standard devices. When this option is enabled, switch supports some pre-802.3af devices.	Enabled or Disabled
Configured type	The user-defined identifier for the port to identify its intended use.	A string

The status of LLDP in PoE page is displayed as Enabled only if one or both LLDP settings (LLDP MED TLV (PoE) and LLDP Dot3 TLV (PoE+)) are enabled for the port.

5. Click **OK**.
6. Click **Save Settings**.

Configuring VLANs on AOS-Switches

AOS-Switches support the following types of VLANs:

- Port-based VLANs—In the case of trusted interfaces, all untagged traffic is assigned a VLAN based on the incoming port.
- Tag-based VLANs—In the case of trusted interfaces, all tagged traffic is assigned a VLAN based on the incoming tag.

The Aruba Mobility Access Switch also supports the following types of VLANs:

- Voice VLANs—You can use voice VLANs to separate voice traffic from data traffic when the voice and data traffic are carried over the same Ethernet link.
- MAC-based VLANs—In the case of untrusted interfaces, you can associate a client to a VLAN based on the source MAC of the packet. Based on the MAC, you can assign a role to the user after authentication.

Adding VLAN Details

By default, all ports in the Switches are assigned to VLAN 1. However, if the ports are assigned to different VLANs, the VLANs page displays their details.

To add a VLAN, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
  a. Set the filter to **Global** or a group containing at least one switch.
  b. Under **Manage**, click **Devices** > **Switches**.

     A list of switches is displayed in the **List** view.
  c. Click a switch under **Device Name**.

     The dashboard context for the switch is displayed.
  d. Under **Manage**, click **Device**.

     The tabs to configure the switch is displayed.

2. Click **Interface** > **VLANs**. The VLANs page is displayed.
3. In the **VLANs Settings** accordion, click **+** to add a VLAN and configure the following parameters.

Table 208: *Configuring and Viewing VLAN Parameters*

Name	Description	Value
Name	The name of the VLAN.	A string
IP Assignment	The method of IP assignment. The static option is displayed only at the device level. The options to assign Primary VLAN and Management VLAN are displayed only when you select Static or DHCP.	**Static**, **DHCP**, or **Disabled** Default: **DHCP**
IP Address	The IP address for static IP assignment. This field is enabled only when you select **Static** from the **IP Assignment** drop-down.	IPv4 address
Netmask	The netmask for static IP assignment. This field is enabled only when you select **Static** from the **IP Assignment** drop-down.	IPv4 address
DHCP Server	Indicates whether the switch is configured as the DHCP server on the VLAN. ■ This field is enabled only when you select **Static** from the **IP Assignment** drop-down. ■ You can enable **DHCP Server** option only when there are no DHCP Helper IP addresses configured.	Toggle switch to the on or off position
DHCP Helper IP	IP address of the DHCP helper server for that VLAN. ■ You can configure a maximum of 16 DHCP helper IP addresses for each VLAN. ■ You can configure DHCP Helper IP addresses only when **DHCP Server** option is disabled.	IPv4 address
Voice	Indicates whether support for voice VLANs are enabled for the VLAN interface.	Toggle switch to the on or off position
Primary VLAN	Indicates whether the VLAN is assigned as the primary VLAN for the switches. To assign primary VLAN, at least one tagged or untagged port should be configured. This is a mandatory field.	Toggle switch to the on or off position

Name	Description	Value
Management VLAN	Indicates whether the VLAN is assigned as the management VLAN for the switches.	Toggle switch to the on or off position
Default Gateway	Default gateway for static IP assignment. This field is enabled only when you select Static from the IP Assignment drop-down.	IPv4 address
Jumbo	Indicates whether jumbo packet handling is enabled for the VLAN interface.	Toggle switch to the on or off position
Access Policy (In)	The security policy that you want to apply for the inbound traffic.	See Configuring Access Policies on AOS-Switches.
Access Policy (Out)	The security policy that you want to apply for the outbound traffic.	
VLAN Access Policy (In)	The security policy that you want to apply for the bridged and routed inbound packets on the VLAN.	
VLAN Access Policy (Out)	The security policy that you want to apply for the bridged and routed outbound packets on the VLAN.	

4. To configure the VLAN ports, complete the following steps:
   a. In the **Ports** table, select the port number(s).
   b. Select any of the following port modes:
      - **Tagged Ports**
      - **Untagged Ports**
      - **None**
5. To assign the VLAN to a trunk group, select the trunk group in the **Trunk Groups** table.
6. Click **OK**.
7. Click **Save Settings**.

When you upgrade to Aruba Central version 2.5.2, the static IP address configured at group level for VLANs is migrated to device level and preserved as overrides. The static IP assignment is available only at the device level.

Editing the VLAN Details

To edit the details of a VLAN, point to the row for the VLAN, and click the edit icon in the **Actions** column, and configure the parameters.

Deleting VLAN Details

To delete the VLAN details, complete the following steps:

1. Ensure that the VLANs are not tagged to any ports.
2. Point to the row for the VLAN, and click the edit icon in the **Actions** column.

VLAN 1 is the primary VLAN and cannot be deleted.

Configuring DHCP Relay Settings

You can configure a switch as a DHCP relay agent for transmitting DHCP messages between the DHCP server and client. You can also configure the option-82 feature for the switch to include DHCP relay information in the forwarded DHCP request messages.

To configure a switch as a DHCP relay agent, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Interface** > **VLANs**. The VLANs page is displayed.
3. Expand the **DHCP Relay Settings** accordion.
4. To enable DHCP relay, move the **DHCP Relay** toggle switch to the on position.

DHCP Relay option is enabled by default.

5. To enable option-82 feature, move the **DHCP Relay Option 82** toggle switch to the on position.
6. Click **Save Settings**.

Configuring Trunk Groups on AOS-Switches in UI Groups

If you have switches provisioned in an UI group, Aruba Central enables you to configure port trunking on these switches using the UI workflows. The network administrator can configure a trunk group on switches to create one logical link or a trunk by aggregating multiple links. The trunk link functions as a high-speed link to provide increased bandwidth.

A trunk group is a set of up to eight ports configured as members of the same port trunk.

Table 209: *Trunk Group configuration Support Per AOS-Switch Platform*

AOS-Switch Platform	Valid Trunk Groups
Aruba 2540 Switch Series	Trk1-Trk26
Aruba 2920 Switch Series Aruba 2930F Switch Series Aruba 2930M Switch Series	Trk1-Trk60

AOS-Switch Platform	Valid Trunk Groups
Aruba 2530 Switch Series	Trk1-Trk24
Aruba 3810 Switch Series	Trk1-Trk144

The following are some guidelines:

- All ports in the same trunk group must be of the same trunk type (LACP or trunk.)
- The names of the trunk groups include the prefix **Trk** followed by the numbers in a sequential order. For example, Trk1, Trk2 and so on.
- When STP is enabled on the switch, the STP configuration is applied for all ports at the trunk group level. Individual ports cannot be configured for STP or VLAN operation.

Adding Trunk Groups on AOS-Switches

To configure a trunk group on switches:

Ensure that the switches are onboarded and provisioned to a UI group in Aruba Central.

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Interface** > **Trunk Groups**. The Trunk Groups page is displayed.
3. In the **Trunk Groups** table, click **+** to add a trunk group and configure the following parameters:

Table 210: *Trunk Groups Page—AOS-Switches*

Name	Description	Value
Name	Indicates the number assigned to the switch port.	String.
Type	A name of the port for easy identification.	**Trunk** or **LACP**.
Untagged VLANs	If the switch ports are untagged, select a VLAN from the Untagged VLAN list.	Select from drop-down menu.

Name	Description	Value
Tagged VLANs	If the switch ports are tagged, select the VLANs from the Tagged VLAN list.	Select from drop-down menu.
Ports	Select the ports for trunking. You can use up to eight ports for link aggregation. The ports in a trunk group need not be consecutive.	Select from drop-down menu.
DHCP Snooping	Select the status of port to filter DHCP messages received at the port.	**Trust** or **Untrust**. Default is **Untrust**.

4. Click **OK**.
5. Click **Save Settings**.

Editing Trunk Groups on AOS-Switches

To edit details of a trunk group, point to the row for the trunk group, and click the edit icon and configure the parameters.

Deleting Trunk Groups on AOS-Switches

To delete a trunk group, point to the row for the trunk group, and click the delete icon.

Enabling Spanning Tree Protocol on AOS-Switches

This is a beta feature and not recommended for a production environment.

The Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic, based on global (bridge) and local (port) parameters you can configure.

STP is always disabled by default on AOS-Switches. To configure STP for switches provisioned in the UI groups:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

d. Under **Manage**, click **Device**.

The tabs to configure the switch is displayed.

2. Click **Interface** > **Spanning Tree**. The Spanning Tree page is displayed.
3. Enable MSTP if you want to avoid bridge loops between network nodes and to maintain a single active path between the network nodes. MSTP will be enabled for all VLANs assigned to switch ports. If you have a trunk group configured for the switches in the group, MSTP is enabled at the trunk level.
4. Set the priority of the UI group.
5. To configure MSTP parameters for ports, select the port row(s) in **Port Settings**, click **Edit**.
6. To configure MSTP parameters for trunks, select the trunk group row(s) in **Trunk Group Settings**, click **Edit**.
7. Configure the following MSTP parameters for ports or trunks of individual switches:

Table 211: *Viewing or Configuring Port and Trunk Settings*

Name	Description	Value
Priority	A number used to identify the root bridge in an STP instance. The switch with the lowest value has the highest priority and is the root bridge. A higher numerical value means a lower priority; thus, the highest priority is 0. When the switches in a network select their root bridge, two parameters are considered, the STP priority and the MAC address of the switch. All AOS-Switches have a default STP priority of 8. So the switch with the lowest MAC automatically gets selected as a root bridge. This is not a recommended process as it randomizes the selection of the root bridge.	0 – 8 Default: 8
BPDU Protection	A security feature used to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, BPDU protection is applied to the edge ports and access ports connected to end-user devices that do not run STP. If STP BPDU packets are received on a protected port, the port is disabled and the network manager is alerted via SNMP traps.	**Enable** or **Disable** Default: **Disable**
BPDU Filter	Enables control of STP participation for each port. The feature can be used to exclude specific ports from becoming part of STP operations. A port with the BPDU filter enabled ignores incoming BPDU packets and stays locked in the STP forwarding state. All other ports maintain their role. Recommended ports for BPDU filter: Ports or trunks connected to client devices.	**Enable** or **Disable** Default: **Disable**
Admin-Edge	When set, the port directly goes into forwarding state. This configuration is not recommended for ports which connect to infrastructure devices. A BPDU guard also assists when a port inadvertently goes into a forwarding state.	**Enable** or **Disable** Default: **Disable**
Root Guard	Sets the port to ignore superior BPDUs to prevent the switch from becoming the Root Port.	**Enable** or **Disable** Default: **Disable**
Trunk Group	Sets the trunk group to which the port is assigned.	**Enable** or **Disable** Default: **Disable**

Configuring Loop Protection on AOS-Switch Ports

Enabling loop protection consumes CPU resources.

Loop protection provides protection against loops by transmitting loop protocol packets out of ports. For switches provisioned in UI groups, administrators can enable or disable loop protection on the switch ports or trunks by using the menu options available under the Network Operations app.

Loop protection is always disabled by default on AOS-Switches. To configure loop protection for switches provisioned in the UI groups:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Interface** > **Loop Protection**. The Loop Protection page is displayed.
3. Depending on whether you want to configure a port or trunk, complete one of the following steps:
   - In the **Port Settings** tab, select the port(s), and click **Edit**.
   - In the **Trunk Group Settings** tab, select the trunk(s), and click **Edit**.

Table 212: *Viewing or Configuring Port Settings*

Name	Description	Value
Port	The number assigned to the switch port.	0 – 65535
Loop Protection	Enables or disables loop protection.	**Enable** or **Disable** Default: **Disable**
Trunk Group	Name of the trunk group to which the port belongs.	Dependent on the switch type.

Table 213: *Viewing or Configuring Trunk Group Settings*

Name	Description	Value
Trunk Group	Name of the trunk group to which the port belongs.	Dependent on the switch type.
Loop Protection	Enables or disables loop protection.	**Enable** or **Disable** Default: **Disable**

4. Select **Enable** in the Loop Protection drop-down.
5. Click **OK**.
6. Click **Save Settings**.

Configuring Port Rate Limit on AOS-Switches

Rate limiting allows allocating a specific bandwidth for the incoming and outgoing traffic from each port. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

Port rate limit is always disabled by default on AOS-Switches. To configure port rate limit for switches provisioned in the UI groups:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Security** > **Port Rate Limit**. The Port Rate Limit page is displayed.
3. Under **Port Rate Limit**, select the port or ports you want to modify and click **Edit**.
4. Set the value of **Limit** to **Traffic by Category** if you prefer to set individual limitations. Else, set the value of **Limit** to **All Traffic** to set a collective limitation.

Percentage limits are based on link speed. For example, if a 100 Mbps port negotiates a link at 100 Mbps and the inbound rate-limit is configured at 50%, then the traffic flow through that port is limited to no more than 50 Mbps. Similarly, if the same port negotiates a 10 Mbps link, then it allows no more than 5 Mbps of inbound traffic. Configuring a rate limit of 0 (zero) on a port blocks all traffic on that port. However, if this is the desired behavior on the port, disable the port instead of configuring a rate limit of 0.

   a. If you select **All Traffic**, rate limit is placed on all packets received from unknown sources. Move the slider to **Enable** and then enter the values for **IN** and **OUT** in percentage values.
   b. If you select **Traffic by Category**, refer to the following table to set the correct parameters.

Table 214: *Traffic by Category Parameters*

Name	Description	Value
Broadcast	Sets a rate limit on broadcast traffic.	Expressed as percentage of the total bandwidth.
Multicast	Indicates the operational status of the port.	
Unknown Unicast	Indicates the mode of operation. The port can be configured to function in Trunk or Access mode.	
ICMP	Sets a rate limit on ICMP traffic.	

Configuring RADIUS Server Settings on AOS-Switches

Aruba Central allows you to configure RADIUS (Remote Authentication Dial-In User Service) server settings on switches.

To configure a RADIUS server, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
     The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.
     A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.
     The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
     The tabs to configure the switch is displayed.
2. Click **Security** > **RADIUS**. The RADIUS page is displayed.
3. Click **+** to add a RADIUS server. The Add RADIUS Server window is displayed.

4. Configure the following parameters.

Table 215: *RADIUS Parameters*

Name	Description	Value
Server IP	The IP address of the RADIUS server.	
Port	The destination port for authentication requests to the specified RADIUS server.	Default: 1812
Shared Key	The encryption key for use during authentication sessions with the specified RADIUS server.	You can enter up to a maximum of 32 characters including alphabets, numbers, and special characters.
Confirm Shared Key	Retype the shared key.	
Dynamic Authorization	Indicates whether the dynamic authorization is enabled. When enabled, the RADIUS server can dynamically terminate or change the authorization parameters used in an active client session on the switch.	Toggle switch to the on or off position
ClearPass Server	Indicates whether the ClearPass server is enabled on the RADIUS server.	Toggle switch to the on or off position

5. Click **Save**.

Editing a RADIUS Server Settings

To edit a RADIUS server, point to the row for the server, and click the edit icon.

NOTE

If you have only one RADIUS server with ClearPass enabled and **Downloadable User Role** is enabled, then you cannot disable ClearPass server for the RADIUS server.

Deleting a RADIUS Server Settings

To delete a RADIUS server, point to the row for the server, and click the delete icon.

NOTE

If the **Downloadable User Role** option is enabled, then at least one RADIUS server must be configured with ClearPass server. Hence, you cannot delete the last RADIUS server on which ClearPass server is enabled.

Configuring Downloadable User Role on AOS-Switches

Aruba Central allows you to enable Downloadable User Role and configure ClearPass settings to download user-roles, policy, and class from the ClearPass Policy Manager server.

NOTE

Downloadable User Role configuration is not supported on Aruba 2530 Switch Series.

To enable Downloadable User Role and configure ClearPass server settings, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Security** > **Downloadable User Role**. The Downloadable User Role page is displayed.
3. Slide the **Downloadable User Role** toggle switch to on position to allow switch to download user-roles.

To enable downloadable user role, ClearPass server must be configured in the **RADIUS** page.The **Downloadable User Role** toggle is disabled if ClearPass server is not enabled for any of the RADIUS settings. For more information, see Configuring RADIUS Server Settings on AOS-Switches.

4. Configure the following ClearPass Settings:

   Table 216: *ClearPass Settings*

Name	Description
User Name	Enter the ClearPass Policy Manager administrator username.
Password	Enter the password to access ClearPass server.
Confirm Password	Retype the password.
Retry Interval	Specify the retry interval to download TA certificate. This certificate is used to authenticate ClearPass server before downloading the user-role. Range: 0-5.

5. Click **Save Settings**.

Configuring CDP on AOS-Switches

Cisco Discovery Protocol (CDP) is used to share information about connected network devices. It is used to share information such as device type, model, interfaces, IP addresses, operating system versions, and VLANs. You can configure CDP modes for the switch.

To enable CDP for the switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **System** > **CDP**. The CDP page is displayed.
3. To enable CDP for the switch, move the **CDP** toggle switch to the on position.
4. Select any of the following modes from the **Mode** drop-down:
   - **rx-only**—Switch only receives CDP information from other connected devices and stores this information in the database. However, it does not send its own information to other devices.
   - **pass-through**—CDP information passes through the switch to other connected devices.
   - **pre-standard-voice**—Enables CDP-compatible voice VLAN discovery with pre-standard VoIP phones.
5. Click **Save Settings**.

Configuring Tunnel Node Server on AOS-Switches

Aruba Central allows you to configure tunneled node on switches. The tunneled node connects to one or more client devices at the edge of the network and then establishes a secure Generic Routing Encapsulation (GRE) tunnel to the controlling concentrator server. You can configure either Port-Based Tunnel or User-Based Tunnel using UI groups.

To modify the reserved VLAN, change the mode to **No Tunnel** and click **Save Settings**, then change the mode back to **User-Based Tunnel**.

The **Tunnel Node Server** configuration cannot be modified when tunneled clients are active.

To configure a tunneled node on the switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
  a. Set the filter to **Global** or a group containing at least one switch.
  b. Under **Manage**, click **Devices** > **Switches**.
     A list of switches is displayed in the **List** view.
  c. Click a switch under **Device Name**.
     The dashboard context for the switch is displayed.
  d. Under **Manage**, click **Device**.
     The tabs to configure the switch is displayed.

2. Click **Security** > **Tunnel Node Server**. The Tunnel Node Server page is displayed.
3. Configure the following parameters.

Name	Description	Value
Mode	The mode of tunneling from the drop-down: ■ **No Tunnel**—Switch does not tunnel traffic. ■ **Port-Based Tunnel**—Allows the switch to tunnel traffic to an Aruba controller on a per-port basis. ■ **User-Based Tunnel**—Allows the switch to tunnel traffic to an Aruba controller on an assigned user role basis.	**Port- Based Tunnel** , **User- Based Tunnel**, or **No Tunnel**
Primary Gateway IP	The IP address of the primary gateway.	A valid IPv4 address
Backup Gateway IP	The IP address of the backup gateway. This field is optional.	A valid IPv4 address
Reserved VLAN	The reserved VLAN ID to tunnel traffic to an Aruba controller. This field is available only for User-Based tunnel. The default VLAN or a VLAN that is already configured cannot be used as a reserved VLAN. To view the list of configured VLANs, navigate to **Interface** > **VLANs**.	Numeric value

4. Click **Save Settings**.

For more detailed information, refer to Dynamic Segmentation white paper at https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf

Configuring Authentication for AOS-Switches

Aruba Central supports enabling 802.1X and MAC authentication for switches. You can enable and configure 802.1X authentication of clients at the switch and port level, and enable authentication of 802.1X

access through a RADIUS server using either EAP or CHAP protocol. You can also enable and configure ports to authenticate clients based on MAC addresses.

See the following topics for more information on authentication:

- 802.1X Authentication
- MAC Authentication
- Configuring Authentication Order and Priority

802.1X Authentication

802.1X is a method for authenticating the identity of a user before providing network access. Aruba Central supports internal RADIUS server and external RADIUS server for 802.1X authentication.

Configuring 802.1X Authentication

To configure 802.1X authentication for the switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Security** > **Authentication**. The Authentication page is displayed.
3. Expand the **802.1X Authentication** accordion.
4. To enable 802.1x Authentication at group level in the group context, slide the toggle switch to on position.
5. In the **Authentication Method** from the drop-down, select either **EAP** or **CHAP**.

If you select EAP or CHAP, you must configure the RADIUS server.

   The Port Settings table displays the number of ports and the parameters configured for the ports.
6. Select one or more ports for which you want to enable 802.1X authentication, and click the edit icon. The Edit Ports Selected window is displayed.
7. Select **Enable** from the **802.1X** drop-down.

8. Configure the following parameters.

Table 217: *Configuring 802.1X Authentication*

Name	Description	Value
Client Limit	The maximum number of clients to allow on the port.	Default: 0
UnAuthorized VLAN ID	The VLAN to use for an unauthorized client.	Default:0
Authorized VLAN ID	The VLAN to use for an authorized client.	Default: 0
Reauth Period	The time (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the re-authentication occurs. When set to 0, re-authentication is disabled.	Default: 300 seconds
Cached Reauth Period	The time (in seconds) when cached re-authentication is allowed on the port.	Default: 0
Log off Period	The time (in seconds) that the switch enforces for an implicit logoff.	Default: 300 seconds
Quiet Period	The time (in seconds) during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails.	Default: 60 seconds
Tx Period	The time (in seconds) the port waits to retransmit the next EAPOL PDU during an authentication session.	Default: 30 seconds
Server Timeout	The time (in seconds) that the switch waits for a server response to an authentication request	Default: 300 seconds
Supplicant Timeout	The time (in seconds) that the switch waits for a supplicant response to an EAP request. If the supplicant does not respond within the configured time frame, the session times out.	Default: 300 seconds

9. Click **Save Settings**.

MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. For MAC authentication, the MAC address of a machine must match an approved list of manually defined addresses on the switch.

MAC authentication can be used alone or it can be combined with 802.1X authentication.

To configure MAC authentication for the switch ports, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

b. Under **Manage**, click **Devices** > **Switches**.
c. Click the **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
  a. Set the filter to **Global** or a group containing at least one switch.
  b. Under **Manage**, click **Devices** > **Switches**.

     A list of switches is displayed in the **List** view.
  c. Click a switch under **Device Name**.

     The dashboard context for the switch is displayed.
  d. Under **Manage**, click **Device**.

     The tabs to configure the switch is displayed.

2. Click **Security** > **Authentication**.
3. In the **Authentication** tab, expand the MAC Authentication accordion. The Port Settings table displays the parameters configured for the port.
4. Select one or more ports for which you want to enable MAC authentication and click the edit icon. The Edit Ports Selected window is displayed.
5. Select **Enable** from the **MAC Auth** drop-down.
6. Configure the following parameters.

Table 218: *Configuring MAC Authentication*

Name	Description	Value
Client Limit	The maximum number of clients to allow on the port.	Default: 0
UnAuthorized VLAN ID	The VLAN to use for an unauthorized client.	Default: 0
Authorized VLAN ID	The VLAN to use for an authorized client.	Default: 0
Reauth Period	The time (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the re-authentication occurs. When set to 0, re-authentication is disabled.	Default: 300 seconds
Cached Reauth Period	The time (in seconds) when cached re-authentication is allowed on the port.	Default: 0
Log off Period	The time (in seconds) that the switch enforces for an implicit logoff.	Default: 300 seconds
Quiet Period	The time (in seconds) during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the max-requests parameter fails.	Default: 60 seconds

7. Click **Save Settings**.

Configuring Authentication Order and Priority

Users can set the authentication order and priority for the 802.1X and MAC authentication methods for each port. The switch attempts to authenticate a client based on the authentication order and priority settings.

- If both 802.1X and MAC authentication are enabled on the same port without configuring authentication order and priority , then both the authentication methods are triggered in parallel and might cause issues for the clients.
- If authentication order and priority are configured, then authentication requests are processed sequentially and authentication method with high priority is used to access the client. If both 802.1X and MAC authentication are enabled on the same port, and 802.1X authentication is set as the first authentication method and MAC authentication is set as the first authentication priority , then MAC authentication is used to authenticate the clients.
- If only one authentication method is enabled on the port, then the switch will not consider authentication order and priority for authentication.

Authentication order and priority configuration is not supported on the Aruba 2920 Switch Series.

To configure the authentication order and priority, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Security** > **Authentication**. The Authentication page is displayed.
3. Expand the **Authentication Order and Priority** accordion. The Ports Settings table displays the Authentication Order and Authentication Priority specified for the ports.
4. Click **+** to add ports with authentication order and priority. The Add Ports window is displayed.
5. Configure the following parameters:
   - **Ports**—Select one or more ports for setting authentication order and priority.
   - **Authentication Order**—Select either **802.1X** or **MAC** as the first method for authentication. For example, if you select **802.1X** as the first authentication method, then **802.1X** is used first for authenticating clients on the port.

- **Authentication Priority**—Select either **802.1X** or **MAC** as the first priority for authentication. Authentication priority takes precedence over authentication order, and the authentication method with higher priority is used to access clients.

6. Click **Save**.

Editing the Authentication Order and Priority

To edit the authentication order and priority, select one or more ports for which you want to modify authentication order and priority, and click the edit icon.

When editing multiple ports, if authentication order and priority are different on ports, then the existing settings are preserved. You can override the existing settings by selecting an order or a priority.

Deleting the Authentication Order and Priority

To delete the authentication order and priority, select one or more ports for which you want to delete authentication order and priority, and click the delete icon.

Configuring Access Policies on AOS-Switches

Aruba Central does not support access policy configuration on Aruba Mobility Access Switches.

To restrict certain types of traffic on physical ports of AOS-Switches, you can configure ACLs from the Aruba Central UI.

To create an access policy, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
     b. Under Manage, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under Manage, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.
        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
        The tabs to configure the switch is displayed.
2. Click **Security** > **Access Policy**. The Access Policy page is displayed.
3. Click **+** to add a new access policy. The **New Access Policy** page is displayed.
4. Enter a name for the policy.
5. Click **Add**.
6. To add a rule to the access policy, click + under **Rules for test**, and configure the following parameters:

Table 219: *Configuring Rules for Access Policies*

Name	Description	Value
Source	Select a source of the traffic for which you want to an access rule.	■ **Any**, **Network**, or **Host** ■ For **Network**, specify IP address and mask ■ For **Host**, specify IP address
Destination	Select a destination.	■ **Any**, **Network**, or **Host** ■ For **Network**, specify IP address and mask ■ For **Host**, specify IP address
Protocol	Select the type of protocol from the drop-down. If you select SCTP, TCP, or UDP, the source ports and destination ports fields are displayed.	Protocol types-GRE, ESP, AH, OSPF, PIM, VRRP, ICMP, IGMP, IP, SCTP, TCP, UDP, IP_IN_IP and IPv6_IN_IP.
Action	The action that the switch must perform on the traffic received at a port.	**Permit** or **Deny**

7. Click **OK**.
8. Click **Save Settings**.

The access policies must be applied to a switch port and the VLAN assigned to a port. For more information on access policy assignment to ports and VLANs, see the following topics:

- Configuring Switch Ports on AOS-Switches
- Configuring VLANs on AOS-Switches

Configuring SNMP on AOS-Switches

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing and monitoring the devices connected to a network by collecting, organizing and modifying information about managed devices on IP networks.

In Aruba Central, you can configure either SNMP versions V2C or V3 using UI groups. By default, SNMP is disabled on the AOS-Switches.

SNMP settings can be configured only when a switch is installed with the firmware version of 16.09 or later.

For more information, see the following topics:

- Configuring SNMPv2c on AOS-Switches
- Configuring SNMPv3 on AOS-Switches
- Disabling SNMP on AOS-Switches

Configuring SNMPv2c on AOS-Switches

You can configure SNMPv2c community settings and trap settings through the UI.

To enable SNMPv2c on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **System** > **SNMP**. The SNMP page is displayed.
3. Select **SNMP mode** as **V2C** from the drop-down to enable SNMPv2C. Changing SNMP mode from V3 to V2C displays a confirmation message window stating that changing SNMP mode will remove existing SNMP configuration.

   Changing SNMP mode from **V3** to **V2C** displays a confirmation message window stating that changing SNMP mode will remove existing SNMP configuration. Type REMOVE in the text box and click **Proceed**.

Configuring Community Settings

You can add or delete SNMP communities to restrict access to the switch.

Adding a Read Community

To add an SNMP community, complete the following steps:

1. In the **SNMP** page, expand the **Community Settings** accordion.
   The **Read Community** table displays the list of communities that have read-only access.
2. To add a read community, click **+**. The Add Community window is displayed.
3. Enter the name of the community in the **Community** text box and click **OK**.

Deleting a Read Community

To delete a read community, point to the row for the trap destination, and click the delete icon.

Configuring Trap Settings

You can configure authentication, trap destination, and trap categories using trap settings.

Adding a Trap Destination

To add a trap destination, complete the following steps:

1. In the **SNMP** page, expand the **Trap Settings** accordion.
2. To add a read destination, click **+**. The Add Trap Destination window is displayed.

3. Configure the following parameters:
4. The **Trap Destination** table displays the following information:
   - **Destination IP**—The destination IP address for sending the trap.
   - **Community**—The community name used for sending the trap.
5. Click **OK**

Deleting a Trap Destination

To delete a trap destination, point to the row for the trap destination, and click the delete icon.

Enabling Trap Categories

To enable trap categories, complete the following steps:

1. In the **Trap Settings** accordion, select the authentication type used to connect to the SNMP server from the **Authentication** drop-down.
2. In the **Trap Category** table, select the check box for the trap category you want to enable.
3. Click **Save Settings**.

The availability of trap categories differs based on the device model.

Configuring SNMPv3 on AOS-Switches

SNMPv3 provides a secured access to SNMP management stations using authentication and privacy protocols. You can add SNMPv3 user and configure notification settings using UI groups.

To enable SNMPv3 on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **System** > **SNMP**. The SNMP page is displayed.
3. Select **SNMP mode** as **V3** from the drop-down to enable SNMPv3.

   Changing SNMP mode from **V2C** to **V3** displays a confirmation message window stating that changing SNMP mode will remove existing SNMP configuration. Type REMOVE in the text box and click **Proceed**.

NOTE

You must add at least one user to enable SNMPv3.

Configuring User Settings

You can add SNMPv3 users to provide secured access to SNMP management stations.

Adding an SNMPv3 User

To add an SNMPv3 user, complete the following steps:

1. In the **SNMP** page, expand the **User/Notification Settings** accordion.
   The **Users** table displays the list of users with associated authentication mode and privacy mode.
2. To add an SNMPv3 user, click **+**. The Add User window is displayed.
3. Configure the following parameters:
   - **User Name**—Enter the user name.
   - **Authentication Mode**—Select either **MD5** (Message Digest) or **SHA** (Secure Hash Algorithm) as the authentication mode to provide secured access to the user.
   - **Password**—Enter the authentication password.
   - **Confirm Password**—Re-enter the authentication password.
   - **Privacy Mode**—Select **AES** (Advanced Encryption Standard) or **DES** (Data Encryption Standard) as the privacy mode to provide secured access to the user.
   - **Privacy Password**—Enter the privacy password.
   - **Confirm Privacy Password**—Re-enter the privacy password.
4. Click **OK**.
   By default, SNMPv3 users are assigned to the managerpriv group.

Editing an SNMPv3 User

To edit an SNMPv3 user, point to the row for the user, and click the edit icon.

Deleting an SNMPv3 User

To delete an SNMPv3 user, point to the row for the user, and click the delete icon.

Configuring Notification Settings

You can configure notification settings to send notifications to SNMPv3 users.

Adding an SNMPv3 Notification

To add a notification, complete the following steps:

1. In the **SNMP** page, expand the **User/Notification Settings** accordion.
   The **Notifications** table displays the list of users with associated IP addresses for sending notifications.
2. To add a notification, click **+**. The Add Notification window is displayed.
3. Configure the following parameters:
   - **IP address**—Enter the destination IP address for sending notifications.
   - **User Name**—Select the user to whom the notifications should be sent.
4. Click **OK**.

Editing an SNMPv3 Notification

To edit a notification, point to the row for the notification, and click the edit icon.

NOTE

You can edit only the user name.

Deleting an SNMPv3 Notification

To delete an SNMPv3 user, point to the row for the notification, and click the delete icon.

Enabling Trap Categories

To enable trap categories, complete the following steps:

1. In the **Trap Settings** accordion, select the authentication type used to connect to the SNMP server from the **Authentication** drop-down.
2. In the **Trap Category** table, select the check box for the trap category you want to enable.
3. Click **Save Settings**.

NOTE

The availability of trap categories differs based on the device model.

Disabling SNMP on AOS-Switches

You can disable SNMP on AOS-Switches. Disabling SNMP will remove all the existing SNMP configurations.

To disable SNMP, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **System** > **SNMP**. The SNMP page is displayed.
3. Select **SNMP mode** as **Disable** from the drop-down to disable SNMP.

   Changing SNMP mode from **V2C** or **V3** to **Disable** displays a confirmation message window stating that changing SNMP mode will remove existing SNMP configuration. Type REMOVE in the text box and click **Proceed**.
4. Click **Save Settings**.

Configuring DHCP on AOS-Switches

Dynamic Host Configuration Protocol (DHCP) is a protocol that enables a server to automatically assign IP addresses to hosts. The server uses the configured IP address pools or ranges to assign to hosts. You can configure multiple IP pools to not have duplicate or overlapping IP subnets. You can configure the IP address pools with various options to share with the hosts. For example, network address, subnet mask, DNS server address.

In Aruba Central 2.5.3, **DHCP Pools** configuration is renamed to **DHCP** and moved from the **IP Settings** tab to the **System** tab.

To enable the DHCP service and to add DHCP pools on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.
        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
        The tabs to configure the switch is displayed.
2. Click **System** > **DHCP**. The DHCP page is displayed.

Aruba 2530 Switch Series do not support DHCP server on the device platform. Hence, Aruba Central pushes the group-level configuration for DHCP to all applicable devices in the group except the Aruba 2530 Switch Series.
If any of the devices is running a lower version, a warning message is displayed, and the DHCP configuration changes are pushed only to the devices that support the DHCP. If the devices are upgraded to a supported version or moved out of the group, the warning message will not be displayed.

3. To activate the DHCP service, move the **DHCP Server** toggle switch to the on position.
   The DHCP service can be enabled only if there is a valid DHCP pool.

4. To add a new DHCP pool, click + in the **DHCP Pools** table and configure the following parameters:

Table 220: *Configuring a DHCP Pool*

Name	Description	Value
Name	Name of the pool.	A string.
Network	A valid network IP address to assigned to the DHCP pool.	IPv4 address.
Netmask	Netmask of the DHCP pool.	Subnet mask.
Lease Time	The lease time for the DHCP pool in days-hours-minutes format.	You can set a maximum value of 365 days 23 hours and 59 minutes in the DD-HH-MM format.
Default Router	IP address of the default router in the subnet.	You can add up to 8 IP addresses.
DNS Server	Address of the DNS server. To add multiple DNS servers, click +.	You can add up to 8 DNS servers.
Netbios Server	Address of the Netbios server. The Netbios server address configuration is not required for Mobility Access Switches. To add multiple Netbios servers, click +.	You can add up to 8 Netbios servers. For Mobility Access Switches, an option called WINS Server is available.
IP Address Range	IP address range within the network and network mask combination. To add multiple IP address range, click +.	You can add up to 64 IP address range.
Exclude Address Range	IP address range to exclude. This field is available only for the Mobility Access Switches. To add multiple excluded address range, click +.	You can add up to 64 IP address range.
Option	The code type, and ASCII or HEX value of the DHCP option to configure. To add multiple options, click +.	You can add up to 8 options. A value within the range of 2-254 with type as hexadecimal and ASCII is valid.

5. Click **Ok**.
6. Click **Save Settings**.
7. To edit the details of a DHCP pool, hover over the row for the DHCP pool and click the edit icon in the **Edit** column.
8. To delete a DHCP pool, hover over the row for the DHCP pool and click the delete icon in the **Delete** column. Click **Yes** in the confirmation window.

Configuring DHCP Snooping on AOS-Switches

DHCP snooping provides network security by filtering untrusted DHCP messages. Filtering is performed by distinguishing trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users.

When you enable DHCP snooping, DHCP packets received at untrusted ports will be dropped, because all ports are configured as untrusted by default. You must configure the ports to be trusted in the **Switches** > **Interface** > **Ports** page.

You must also configure authorized DHCP servers for the network to have a functional DHCP server that serves clients on this switch.

By default, DHCP snooping is disabled for the switch.

Enabling DHCP Snooping on a Switch

To enable DHCP snooping on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Security** > **DHCP Snooping**. The DHCP Snooping page is displayed.
3. To enable DHCP snooping for the switch, move the **DHCP Snooping** toggle switch to the on position.
4. To enable option-82 for the switch, move the **DHCP Snooping Option-82** toggle switch to the on position.
   When you enable both DHCP snooping and option-82, the switch drops the option-82 information from the DHCP packets.
5. Click **Save Settings**.

Adding Authorized DHCP Servers for a Switch

To add the list of IP addresses of authorized DHCP servers for a switch, complete the following steps:

1. In the DHCP Snooping page, click + in the **Authorized DHCP Servers IP** table. The Add Authorized DHCP Server IP window is displayed.
2. Enter the IP address in the **Authorized DHCP Servers IP** field.
3. Click **OK**.
4. Click **Save Settings**.

Deleting Authorized DHCP Servers for a Switch

To delete the authorized DHCP servers IP addresses, in the **Authorized DHCP Servers IP** table, point to IP address, and click the delete icon for the DHCP server IP you want to delete.

Enabling DHCP Snooping for a VLAN

To enable DHCP snooping for a VLAN, complete the following steps:

1. In the **DHCP Snooping Settings** table, select the VLAN row(s) for which you want to configure DHCP snooping, and click **Edit**.
2. Select **Enable** or **Disable** from the **DHCP Snooping** drop-down.
3. Click **OK**.
4. Click **Save Settings**.

Configuring IGMP on AOS-Switches

In a network where IP multicast traffic is transmitted for various multimedia applications, Internet Group Management Protocol (IGMP) helps reduce bandwidth usage on a per-port basis on a switch. Enabling IGMP for a VLAN allows the ports to detect IGMP queries and report packets, and manage IP multicast traffic through the switch.

By default, IGMP is disabled for all VLANs.

To enable IGMP for a VLAN, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **IGMP**. The IGMP page is displayed with the list of existing VLANs.
3. Select the VLAN row(s) for which you want to configure IGMP, and click **Edit**.
4. Select **Enable** or **Disable** from the **IGMP** drop-down.
5. Click **OK**.
6. To configure the switch to filter unknown multicast messages, move the **Filter Unknown Multicast** toggle switch to the on position.
7. Click **Save Settings**.

Configuring Time Synchronization on AOS-Switches

Time synchronization in a switch ensures maintaining a uniform time among all interoperating devices. Aruba Central offers the following time synchronization protocols for switches:

- Network Time Protocol (NTP)
- Simple Network Time Protocol (SNTP)

To configure time synchronization in a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **System** > **Time**. The Time page is displayed.
3. Configure the following parameters.

Table 221: *Configuring Time Synchronization Parameters*

Name	Description	Value
Time Sync Method	The synchronization method or protocol to use for synchronizing the time on the switch.	SNTP and NTP Default: NTP
Mode	The operating mode for connecting to a time server. The following modes are supported: ■ **Broadcast**—The switch acquires time updates from the data that any time server broadcasts to the network. The switch uses the time data from the first server detected and ignores others. If the poll interval expires thrice without the switch acquiring a time update from the first server detected, the switch accepts a time update from the next server broadcast. **Note:** To use the **Broadcast** mode, the switch and the time server must be in the same subnet. Also, the time server must be configured to broadcast time updates to the network broadcast address. ■ **Unicast**—The switch acquires time updates from a specific server for time synchronization. This mode requires at least one server address to be configured in the **Server Address** field. ■ **DHCP**—The switch attempts to acquire a time server IP address from the DHCP server. If the switch receives a server address, it polls the server for time updates according to the poll interval. If the switch does not receive a time server IP address, it cannot perform time synchronization updates. This mode is applicable only for SNTP. ■ **Disabled**—Time synchronization is disabled. You cannot disable synchronization if NTP is selected.	**SNTP** Supported modes: Broadcast, Unicast, DHCP, and Disabled Default mode: DHCP **NTP** Supported modes: Broadcast, Unicast Default mode: Broadcast Default: DHCP
Server Address	IP address of the time server that the switch accesses for obtaining time synchronization updates. This field is applicable only when you select the **Unicast** mode for synchronization.	IPv4 address

Name	Description	Value
	You can configure a maximum of three time server IP addresses. When you add more than one IP address, the priority that the switch considers in selecting the IP address is the order in which you add the IP address. Therefore, the first IP address that you add will be priority 1, second IP address will be priority 2, and so on. There is no priority assigned when NTP mode is selected. You can delete the IP addresses by clicking the delete icon corresponding to the address. For STP, when more than one IP addresses are added, you must first delete the IP address you added last. In the case of NTP, you can delete the IP addresses in any order.	
Timezone	The time zone corresponding to the location of the switch.	Time zone selected from the drop-down.
Daylight Time Rule	The rule that the switch uses to adjust the time for Daylight Saving Time (DST). For information about the predefined and user-defined times, see Predefined DST Rules. When you select the **User-defined** option, you must configure the beginning and ending months and dates for DST changes in the **Begin Month and Day** and **End Month and Day** fields. All DST rules begin and end at 2 a.m. on the configured dates.	Alaska, Canada and Continental US, Middle Europe and Portugal, Southern Hemisphere, Western Europe, and User-defined.
Begin Month and Day	The beginning month and date for the user-defined DST changes. This field appears only when you select **User-defined** in the **Daylight Time Rule** field.	Month and date selected from the drop-down.
End Month and Day	The ending month and date for the user-defined DST changes. This field appears only when you select **User-defined** in the **Daylight Time Rule** field.	Month and date selected from the drop-down.

4. Click **Save Settings**.

Predefined DST Rules

Following are the details of the beginning and ending days for the predefined DST rules:

Predefined DST Rule Name	Description
Alaska	■ Begin DST at 2 a.m. on March 8. ■ End DST at 2 a.m. on November 1.
Canada and Continental US	
Middle Europe and Portugal	■ Begin DST at 2 a.m. on March 25. ■ End DST at 2 a.m. on September 24.
Southern Hemisphere	■ Begin DST at 2 a.m. on October 25. ■ End DST at 2 a.m. on March 1.
Western Europe	■ Begin DST at 2 a.m. on March 25. ■ End DST at 2 a.m. on October 25.

Configuring Routing on AOS-Switches

- Aruba Central does not support routing on Aruba Mobility Access Switches.
- In Aruba Central 2.5.3, **Routing** configuration is moved from the **IP Settings** tab to the **Routing** tab.

Static routes provide a means for restricting and troubleshooting routed traffic flows and in small networks can provide the simplest and most reliable configuration for routing. Static routes are manually configured in the routing table.

To enable routing and to add routes on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Routing**. The Routing page is displayed.
3. To enable routing, move the **Routing** toggle switch to the on position.

   Before enabling routing, you must already have configured a path to the gateway.
4. In the **Routes** table, click + to add a VLAN and configure the following parameters:

Table 222: *Routing Path Parameters*

Name	Description	Value
Network	A valid network IP address for the destination network or host.	IPv4 address.
Netmask	Netmask of the IP address.	Netmask address.
Gateway	Default gateway IP address.	IPv4 address.
Metric	A parameter used by the routers to determine the best optimal path for routing traffic.	This is a fixed metric for static IP routes, and is set to “1”.
Distance	The administrative distance helps routers determine the best route when there are multiple routes to the destination. A lower value is recommended.	The default administrative distance for static IP routes is 1, but can be configured to any value in the range of 1 - 255.

If the routing metric and administrative distance are set to a lower value for static routes, switches use the static IP routes as the best route for routing traffic.

5. Click **Save**.
6. To delete a route, hover over the row for the route in the **Routes** table and click the delete icon in the **Distance** column. Click **Yes** in the confirmation window.

Configuring QoS Settings on AOS-Switches

QoS is used to classify and prioritize traffic throughout a network. QoS enables you to establish an end-to end traffic-priority policy to improve the control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first.

Aruba Central allows you to configure QoS settings on individual or group of switches through the UI. The settings that you apply at the group level are applied to all switches in the group, except in the following conditions:

- A switch has a configuration override—That is, a QoS setting is changed at the device level. Once you update or apply a setting at the device level, any further changes that you make at the group level are not applied to the switch. A notification for the configuration override is added to the Audit Trail. If you remove local overrides on a switch, then all QoS configurations that were applied to the switch are removed, and the configurations available at the group level are applied to the switch.

  For example, when a switch does not have any policies, if you add a policy for port 2 and 3 at the group level, then the policy is applied to the switch. If you add a policy for port 4 at the device level, and then add a policy for port 5 at the group level, then the policy for port 5 is not applied to the switch. You must add the same policy again at the device level to apply the policy. If you remove the local overrides on the switch, then any policies that were updated or added to the switch and the associated QoS class are replaced by the policies at the group level.
- A switch has invalid port number or VLAN ID—The port or VLAN to which the setting was applied at the group level is not available or is invalid on the switch. For example, if you apply a setting to port 15 and 16 at the group level, and a switch has only ports 1 to 10, then the settings will not be applied to that switch.

The setting that can be configured using the UI are:

- Creating QoS traffic policies on switches in your network to enable traffic-handling rules across the network.
- Defining QoS classes for a QoS Policy.
- Changing the priorities of traffic from various segments of your network as your business needs change.

Creating a QoS Traffic Policy

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.

        The tabs to configure the switch is displayed.
2. Click **QoS**. The QoS page is displayed.
3. In the **QoS Traffic Policy** accordion, click **+** to add a new QoS traffic policy.

4. Configure the following parameters.

Table 223: *Configuring QoS policy*

Name	Description	Value
Policy Name	The name of the QoS policy.	A string
Target	The target where the policy is applied.	**Port** or **VLAN**
ID	Select one or more ports or VLAN ID to be mapped to a traffic policy.	Numeric value

5. Click **Save**.

Editing a QoS Policy

To edit a QoS policy, point to the row for the Qos policy, and click the edit icon.

Deleting a QoS Policy

To delete a QoS policy, point to the row for the Qos policy, and click the delete icon.

Adding a QoS Class for the Policy

To define a QoS class for the a policy, complete the following steps:

1. Select a QoS policy from the New QoS Policy table. The QoS Class table is displayed below the New QoS Policy table with the configured QoS classes.
2. Click **+** to add a QoS classifier for the selected policy. The Add QoS classifier window is displayed.
3. Configure the following parameters.

Table 224: *Configuring QoS class*

Name	Description	Value
Class Name	The class name of the QoS policy.	A string
Packet Matching Criteria		
Source	The type of source for which you want to apply a policy.	**Any**, **Network**, or **Host**. If you select Network, enter the IP address and wildcard mask . If you select Host, enter the IP address.
Destination	The type of destination for which you want to apply a policy.	**Any**, **Network**, or **Host**. If you select **Network**, enter the IP address and wildcard mask . If you select **Host**, enter the IP address.

Name	Description	Value
Protocol	Select the type of data transfer protocol from the drop-down. If you select SCTP, TCP, or UDP, the source ports and destination ports fields are displayed.	Protocol types: GRE, ESP, AH, OSPF, PIM, VRRP, ICMP, IGMP, IP, SCTP, TCP, UDP, IP_IN_IP and IPv6_IN_IP.
Source Port (s)	The port numbers of source. You can specify a comma separated list of ports or range of ports. For example: 10-12 or 10,12.	Numeric value
Dest Port(s)	The port numbers of destination. You can specify a comma separated list of ports or range of ports. For example: 10-12 or 10,12.	Numeric value
Actions		
DSCP	Select a Differentiated Service Code Point (DSCP) from the drop-down.	DSCP value range from 0 to 63. Default value is No Change.
Priority	Select a priority value for the selected DSCP.	The priority range from 0 to 7. 0 – Normal Priority 1 – Low Priority 7 – High Priority Default value is No Change.

Editing a QOS Class

To edit a QoS Class, point to the row for the Qos policy class, and click the edit icon.

Deleting a QOS Class

To delete a QoS Class, point to the row for the Qos policy class, and click the delete icon.

Configuring DSCP Map

DSCP map table displays mappings between Incoming DSCP and priority.

To change priority value associated with a DSCP code point, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
2. Click **QoS**. The QoS page is displayed.
3. Expand the **DSCP Map** accordion.
4. Select the Incoming DSCP row for which you want to change the priority and click the edit icon. The Edit DSCP window is displayed.
5. Select the priority value from the drop-down.
6. Click **OK**.

Configuring Device Profile

Device profile configuration allows you to dynamically detect an Aruba AP, which is directly connected to the switch, and apply predefined configurations to ports on which the Aruba AP is detected.

Configuration changes made on the **Device Profile** page will always take precedence over changes made on other configuration pages.

To configure device profile, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Device Profile**. The Device Profile page is displayed.
3. Slide the **Status** toggle switch to on to enable the device profile support for a device type. By default, the device profile is disabled.
4. Configure the following parameters.

Name	Description	Value
Profile Name	The name of the profile configured. You cannot modify this field. If no other device profile is mapped to the device type, the default device profile `default-ap-profile` is associated with the device type.	Inherited from switch.
Device Type	Type of the device supported.	The only device type supported is Aruba AP.
Tagged VLAN	The tagged member of the VLAN.	
UnTagged VLAN	The untagged member of the VLAN.	Select from drop-down list. The default value is 1.
PoE Priority	The PoE priority for the device port.	**Low**, **High** or **Critical**.

Name	Description	Value
Jumbo	Indicates whether jumbo packet handling is enabled for the VLAN interface.	Toggle switch to the on or off position

5. Click **Save Settings**.

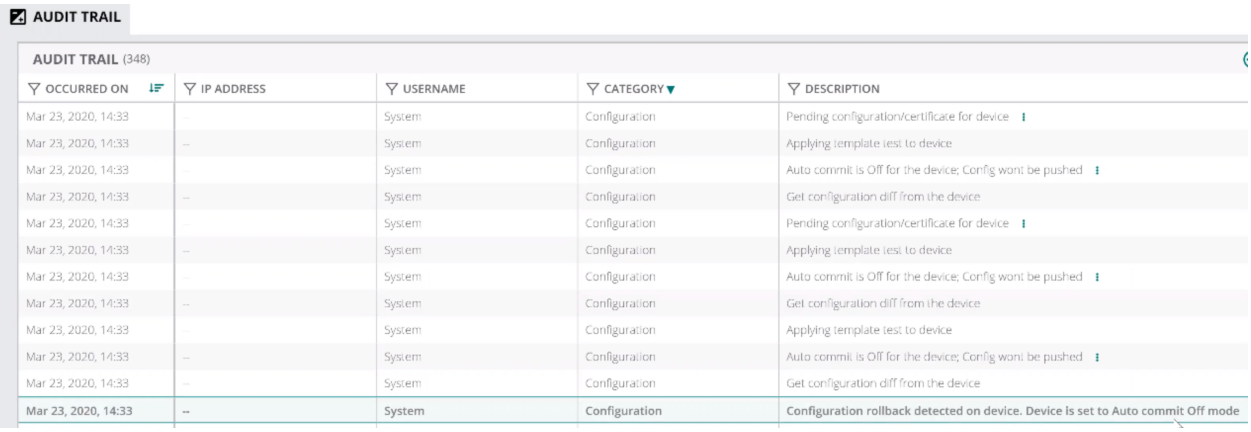
NOTE

You can validate device profile using `show device-profile status` and `show vlan <id>` commands.

Automatic Rollback Configuration

Aruba Central supports an auto-rollback mechanism for switches running software version 16.10.0009 or later. The rollback mechanism is triggered when the switch loses connectivity to Aruba Central after configuration push. A period of about 10 minutes is taken by switch to complete the rollback with last known stable configuration and connect back to Aruba Central. After recovery, the **Auto Commit State** in the **Configuration Audit** page is set to **Off** to stop subsequent configuration push from Aruba Central. Before changing the **Auto Commit** State to **ON**, user needs to review the configuration change that resulted in network disconnect.

If there is a switch rollback, an event will be logged in the **Audit Trail** page as shown in the following figure:



Configuring System Parameters for AOS-Switches

The **System** menu under **Switches-MAS** and **Switches** allows you to configure administrator credentials and enable mode for the switch users.

Configuring Administrator Credentials for Mobility Access Switch

To configure administrator credentials for a Mobility Access Switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.

- To select a switch in the filter:
    a. Set the filter to **Global** or a group containing at least one switch.
    b. Under **Manage**, click **Devices** > **Switches**.
    A list of switches is displayed in the **List** view.
    c. Click a switch under **Device Name**.
    The dashboard context for the switch is displayed.
    d. Under **Manage**, click **Device**.
    The tabs to configure the switch is displayed.

2. Click **System** > **Access/DNS**. The **Access/DNS** page is displayed.
3. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
4. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
5. Click **Save Settings**.

Configuring Administrator and Operator Credentials for Other AOS-Switches

To configure administrator credentials for other AOS-Switches, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
    - To select a switch group in the filter:
        a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
        b. Under **Manage**, click **Devices** > **Switches**.
        c. Click the **Config** icon to view the switch configuration dashboard.
    - To select a switch in the filter:
        a. Set the filter to **Global** or a group containing at least one switch.
        b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
        c. Click a switch under **Device Name**.
        The dashboard context for the switch is displayed.
        d. Under **Manage**, click **Device**.
        The tabs to configure the switch is displayed.
2. Click **System** > **Access/DNS**. The **Access/DNS** page is displayed.
3. Enter the username for the administrator user in the **Admin Username** text box.
4. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
5. To configure the operator user credentials, complete the following steps:
    - Select the **Set Operator Username** check box.
    - Enter a username and password for the operator user.
    - Confirm the password.
6. Click **Save Settings**.

Configuring a Name Server

To set a static IP switches, you must configure a name server. To configure a name server, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.
        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
        The tabs to configure the switch is displayed.
2. Click **System** > **Access/DNS**. The **Access/DNS** page is displayed.
3. Select **DHCP** or **Static** from the **Name Server** drop-down.
4. If you selected **Static** in the drop-down, enter the IP address of the name server obtained from the DNS server in the text box.
5. Click **Save Settings**.

AOS-Switch Stack

A switch stack is a set of switches that are interconnected through stacking ports. The switches in a stack elect a primary switch called Conductor and a backup switch as Standby. The remaining switches become Members of the stack. The following table lists the switches that support stacking:

Table 225: *Switch Stacking Support*

AOS-Switch Platform	Maximum Number of Stack Members	Minimum Supported Version for Template Group	Minimum Supported Version for UI Group	Supported Stack Type (Frontplane (VSF) / Backplane (BPS))	Supported Configuration Group Type for Stacking (UI / Template)
Aruba 2920 Switch Series	4	WB.16.04.0008	WB.16.08.0001	BPS	UI and Template
Aruba 2930M Switch Series	10	WC.16.06.0006	WC.16.08.0001	BPS	UI and Template
Aruba 2930F Switch Series	8	WC.16.07.0002	WC.16.08.0001	VSF	UI and Template
Aruba 5400R Switch Series	2	KB.16.06.0008	N/A	VSF	Template only
Aruba 3810 Switch Series	10	KB.16.07.0002	KB.16.08.0001	BPS	UI and Template

Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central.

For more information on topology and configuration of switch stacks, see the *HPE ArubaOS-Switch Management and configuration Guide* for the respective switch series.

Provisioning AOS-Switch Stacks in Aruba Central

The switch elected as the conductor establishes a WebSocket connection to Aruba Central. The following criteria apply to provisioning and management of switch stacks in Aruba Central:

- Switch stacks can be added only to a template group and cannot be moved to a UI group.
- If the standalone switches in a group join to form a switch stack, the switch is moved to the Unprovisioned state.
- If a switch stack in the template group joins Aruba Central as a stand-alone Switch, it is blocked unless it is deleted from the stack. After it is removed from the stack, the stand-alone switch is moved to the pre-provisioned group.
- If a switch stack is moved from a pre-provisioned group to an existing group in the UI, it will be moved to Unprovisioned state.
- After forming a switch stack, you can remove a member and erase its stacking configuration. However, the member can join Aruba Central as a standalone switch only after it is deleted from the switch stack.

- When a stack is removed, the stack members cannot join Aruba Central until the stack entry is deleted. For more information on deleting the stack, see Configuring AOS-Switch Stacks Using UI Groups. When a stack entry is not deleted and the member tries to rejoin Aruba Central, an event is triggered in the Audit Trail page stating that the stack association is detected.

Assigning Labels and Sites

Aruba Central supports organizing your devices into sites for ease of monitoring. Sites refer to physical locations in which the devices are installed. Administrators can assign switch stacks to a single site for ease of managing installations and monitoring the overall site health. For more information on assigning devices to sites, see Managing Sites.

Similarly, switch stacks can also be tagged using labels. Labels allow you to identify or tag devices installed in a specific site for ease of monitoring. For more information on assigning labels, see Managing Labels.

If any one member of the switch stack is assigned to a site, Aruba Central automatically assigns all other members in a switch stack to the same site. Similarly, if a label is assigned to an individual member in a stack, the same label is applied to all other members of the stack.

Because all members of a switch stack must be assigned to the same site and label, Aruba Central automatically corrects the site and label assignment for switch stacks that were earlier assigned to different labels or sites. If you have such switch stacks in your account, you will notice that all stack members are migrated to the same site or label to which the conductor was assigned. Aruba recommends that you review the sites and labels assigned by Aruba Central to verify that the switch stacks in your account are assigned to sites and labels that you intended to use, and if required, assign all members of stack to a common site or label of your choice.

Configuring AOS-Switch Stacks

For information on configuring switch stacks using template groups, see Configuring AOS-Switch Stacks using Template Groups.

For information on configuring switch stacks using UI groups, see Configuring AOS-Switch Stacks Using UI Groups.

Monitoring AOS-Switch Stacks

See Monitoring Switches in List View.

Viewing AOS-Switch Stacks in Site Topology

See Monitoring Sites in the Topology Tab.

Configuring AOS-Switch Stacks using Template Groups

The switch stacks are provisioned under template groups in Aruba Central. The template groups allow you to configure and modify the settings of a switch stack using configuration templates.

When uploading a configuring template, ensure that the variables are uploaded for all the members of the stack. The template is applied with the variables of the member that is elected as the conductor.

To create a configuration template for switch stack, complete the following steps:

1. In the **Network Operations** app, set the filter to a template group.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

3. Click the **Config** icon.
   The tabs to configure switches using templates is displayed.
4. Click **+** to create a template for the AOS-Switch stack.
5. Specify a name for the template.
6. Select Aruba Switch from the **Device** drop-down list.
7. Select the AOS-Switch model in the **Model** drop-down list.
8. Select the AOS-Switch software version in the **Version** drop-down list.
9. Enter the template text in the **Template** box.

All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command.

10. Click **Save**.

Aruba Central does not support the use of part number (J-number) in place of Switch model number in configuration templates for the AOS-Switch stack.

The following pre-defined variables are refreshed and re-imported from a switch stack when a new stack member is added or removed, or when a failover occurs.

- _sys_template_header
- _sys_module_command
- _sys_stack_command
- _sys_oobm_command
- _sys_vlan_1_untag_command
- _sys_vlan_1_tag_command

For information about deploying VSF stacks of ArubaOS Switches using Zero Touch Provisioning (ZTP) in Aruba Central, see the *VSF Stacking Guide*.

For information about switch stacks using UI groups, see Configuring AOS-Switch Stacks Using UI Groups.

Configuring AOS-Switch Stacks Using UI Groups

Aruba Central supports both Backplane stacking (BPS) and Virtual Switching Framework (VSF) switch stacking. You can create switch stacks and add stack members through the UI. The stack configuration is possible only when the switches are online.

Stacks created using UI groups can only be managed in a UI group. If a device is moved to a template group, then the device cannot be managed in a UI group without rebuilding the stack.
Fiber modules / SFP ports are manageable in a UI group when the stack is created. These modules are available for configuration at the device level context.

See the following topics for more information on managing switch stacks using UI groups:

- Onboarding Conductor and Members for VSF stacking
- Onboarding Conductor and Members for BPS stacking

- Creating an AOS-Switch Stack
- Adding a Stack Member

Onboarding Conductor and Members for VSF stacking

The following is a high-level process flow for configuring VSF switch stacks:

1. Add all the switches that are intended to act as a conductor, standby, and members in the VSF switch stack to the device inventory and assign a valid subscription. All the switch members must be set to factory default and powered off.
2. Power on the switch you intend to add as a conductor. The switch comes up online in Central as a standalone switch.
3. Create a stack with the standalone switch. After stack creation, the switch will reboot and comes up as a stack conductor. For more information, see the section Creating an AOS-Switch Stack.
4. Add other members to the stack when the status of the conductor switch is active. For more information, see Adding a Stack Member.
5. After adding members, connect the Ethernet cables between the switches to form the desired topology.
6. Power on the switches one at a time. The second switch that is powered on will be elected as standby. The subsequent switches that get powered on will be designated as the members of the stack.

For more information on deploying a VSF stack, see Recommended Deployment Workflow section.

For more information on topology and configuration of switch stacks, see the *ArubaOS-Switch Installation and Getting Started Guide* and *ArubaOS-Switch Advanced Traffic Management Guide* for the respective switch series.

If the stack members are connected and powered on before adding to a stack, then the members might not join the stack and status of the stack members are displayed as **Inactive** in the UI. In this scenario, stack cannot be managed through the UI.

Recommended Deployment Workflow

The following procedure provides the recommended workflow for deploying three-member VSF stack (Conductor, Standby, and a Member switch).

1. Connect a staging port on the first switch in the VSF stack to a DHCP enabled network or a device that has access to the internet. After rebooting and initialization, the switch assumes its role as conductor and the LED on the VSF stack ports of the switch will turn amber.
2. Connect a VSF port of the next switch to the VSF port of the conductor switch. During initialization, the switch will act as standby and the LED on the VSF port will turn amber.
3. Connect a VSF port of the next switch to the VSF port of the standby switch. During initialization, the new switch acts as a member and the LED on the VSF port of the switch will turn amber.
4. Connect the VSF port of the conductor switch to the VSF port of the member to complete the loop.

If the stack members are connected and powered on before adding to a stack, then the members might not join the stack in Aruba Central. In such scenarios, the status of the stack members is displayed as **Inactive** in the UI. Also, the stack cannot be managed using UI groups in Aruba Central.

Onboarding Conductor and Members for BPS stacking

The following is a high-level process flow for configuring BPS switch stacks:

1. Add all the switches that are intended to act as a conductor, standby, and members in the BPS switch stack to the device inventory and assign a valid subscription. All the switch members must be set to factory default and powered off.
2. Insert the stacking module to the switch you intend to add as a conductor.
3. Power on the conductor switch. The switch comes up online in Central as one-member BPS switch stack. A one-member BPS switch stack is a single BPS switch with stacking enabled.
4. Move the one-member switch stack from the **Unassigned Devices** group to a UI group. The stacking information is displayed in the **Stacks** configuration page with switch member added as the conductor.
5. Add other members to the stack when the status of the conductor switch is active in the Members table. For more information, see Adding a Stack Member.
6. After adding members, connect the stacking modules and stacking cables between the switches to form the desired topology.
7. Power on the switches one at a time. The second switch that is powered on will be elected as standby. The subsequent switches that get powered on will be designated as the members of the stack.

If the stack members are connected and powered on before adding to a stack, then the members might not join the stack in Aruba Central. In such scenarios, the status of the stack members is displayed as **Inactive** in the UI. Also, the stack cannot be managed using UI groups in Aruba Central.

For more information on topology and configuration of switch stacks, see the *ArubaOS-Switch Installation and Getting Started Guide* and *ArubaOS-Switch Advanced Traffic Management Guide* for the respective switch series.

Creating an AOS-Switch Stack

To create an AOS-Switch stack, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**.
        The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**.
        The tabs to configure the switch is displayed.
2. Click **Stacks**. The Stacks page is displayed.
   The Stacks table displays the following information:

Table 226: *Stacks table*

Name	Description	Value
Name	The name of the switch stack.	A string
Type	The type of switch stacking.	BPS or VFS
Stack ID	The ID of the switch stack. The stack ID is auto-generated and cannot be changed in the settings.	Auto-generated String
Members	The number of members on the switch stack.	Integer
MAC Address	The MAC address of the switch stack.	Alphanumeric MAC address
Topology	The type of switch stack topology.	Chain, Ring, or unknown
Status	The status of the stack formation.	Pending, In-progress, Active, or Failed
VSF Port Speed	The port speed in the case of VSF stacking. This column is hidden by default. You must select the column from the columns list.	1G or 10G

3. In the **Stacks** table, click **+** to add a stack.
   The **Create New Stack** window is displayed.
4. Select a conductor switch from the **Select Conductor Switch** drop-down list. The model number and serial number of switches are displayed in the drop-down list.

- The conductor switch must be installed with the minimum supported firmware version of 16.06 or later.

   If the selected switch supports VSF Stacking, configure the following parameters:
   - **Link 1 Name and Port(s)**—The name of the link 1 and its corresponding ports.
   - **Link 2 Name and Port(s)**— The name of the link 2 and its corresponding ports.
   - **Domain ID**—The domain ID of the switch stack.
   - **Port Speed**—The VSF port speed from the drop-down.

   If the selected switch supports BPS stacking, insert the stacking module in switch and continue to step 5.
5. Click **Save & Reboot Stack**. When the stack reboots, the status of the stack formation is displayed in the **Stacks** table. Do not make any changes to the stack until the status changes from In Progress to Active or Failed. If stack creation fails due to some issues, delete the stack entry and retry.

Editing a Stack

To edit a stack, select the stack row you want to edit and click the edit icon.

You can edit a stack only when its status is **Active**.

Removing a Stack

To remove a stack, select the stack row that you want to remove and click the delete icon.

NOTE

You can remove a stack only when its status is **Failed**.

Adding a Stack Member

Stacking allows you to add switches to the stack only when the conductor is active.

To add a switch to stack as a new member, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. Click the **Config** icon to view the switch configuration dashboard.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.

     c. Click a switch under **Device Name**.

        The dashboard context for the switch is displayed.

     d. Under **Manage**, click **Device**.

        The tabs to configure the switch is displayed.
2. Click **Stacks**. The Stacks page is displayed.
3. In the **Stacks** table, select the stack row for which you want to add a member. The Members table displays the list of members for that particular stack. The **Members** table displays the following information:

Table 227: *Members table*

Name	Description	Value
Name	The name of the switch stack member.	A string
MAC Address	The MAC address of the stack member.	Alphanumeric MAC address
Model	The hardware model of the switch.	A String
Priority	The priority level of the stack member.	1 to 255
Role	The role of a stack member.	Conductor, member, or standby
Status	The status of the switch stack member.	Active, Inactive, or Not Joined
Link1 | Port	The name of the link and its corresponding port of the stack member.	A String
Link2 | Port		

4. In the **Members** table, click **+** to add a stack member.
   The **Add Stack Member For <stack name>** window is displayed. The following information is auto-generated:
   - **Member ID**—Identification number of the member.
   - **Priority**—Priority of the member.
5. Select the member using one of the following options:
   - **Same as Conductor**—Use this option when your conductor and member have the same model number.
   - **Select Model** —Use this option when your conductor and member have different model numbers. Select the switch model from the model drop-down list.
6. If the selected switch supports VSF Stacking, configure the following parameters:
   - **Link1 Name and Port(s)**—Specify the name of the link 1 and its corresponding port.
   - **Link2 Name and Port(s)**—Specify the name of the link 2 and its corresponding port.
7. To add another stack member, click **Save & Add Another**.

A message is displayed above the **Members** table when the maximum number of switches in a stack has been added.

8. Click **Save**. After the stack members appear in **Members** table, connect the stacking modules and stacking cables to all switches and power on the switches.

Editing a stack member

To edit a stack member, select the member row you want to edit and click the edit icon.

Removing a stack member

To delete a stack member, select the member row that you want to delete and click the delete icon.

After removing a member, disconnect the switch from the stack. To disconnect the switch from the stack, do one of the followings:

- Turn off the power from the switch.
- Restart the switch using switch reset button.

You can remove only the stack member that has the lowest priority. For example, if there are three stack members with priority 254, 253 and 252 respectively and if you want to remove a stack member with priority 253, then first you need to remove the member with priority 252.
Priority cannot be assigned manually. Conductor switch is always assigned with priority 255. The priority of other subsequent members is decremented by 1.

The switch dashboard enables you to manage, configure, monitor and troubleshoot AOS-Switch, AOS-CX switches, and switch stacks provisioned and managed through Aruba Central.

To view AOS-CX switches in the monitoring and topology pages, you must create a template configuration for the switch with the password in plaintext. See Using Configuration Templates for AOS-CX Switch Management.

If you are unable to view all details of the AOS-CX switch, then maybe the template configuration was not applied correctly, the password was missing in the template configuration, or the password was not in plaintext. See the audit trail to check the status of the switch. The audit trail should show the device onboarded message for the switch serial number followed by the configuration push and login successful messages. For more information on troubleshooting AOS-CX switch onboarding issues, see Troubleshooting AOS-CX Switch Onboarding Issues.

Monitoring Switches in List View

The switch monitoring details are displayed on the switch dashboard and the switch details page. The switch dashboard and the switch details page are accessed from the **Network Operations** app.

The switch dashboard displays details about the health and status of switches and switch stacks. The switch details are provisioned and managed through Aruba Central. The switch dashboard displays the details in a summary and list view.

The Switches List page provides information associated with the switches provisioned and managed in Aruba Central. The Switches List page displays the following sections:

Viewing the Switches List Page

To navigate to the Switches List page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.

   A list of switches is displayed in the **List** view.

   The Switches List page displays the following information:
   - **Switches**—Displays the total number of switches, both online and offline. When you click the **Switches** tab, it provides information about all switches in the **Switches** table.
   - **Online**—Displays the number of online switches. When you click the **Online** tab, it provides information about all switches that are currently online and connected to Aruba Central in the **Switches** table.
   - **Offline**—Displays the number of offline switches. When you click the **Offline** tab, it provides information about all switches that are currently offline or not connected to Aruba Central in the **Switches** table.

The online switches are displayed with a green dot and offline switches are displayed with a red dot.

Even when the AOS-CX switches are displayed as online, there might be instances when the details of the switches are not displayed completely. This may be because of the following reasons:

- Template configuration is not applied correctly on the switch
- Password is not configured in the template configuration
- Password is not in plaintext format

See the audit trail to check the status of the AOS-CX switches. The audit trail should show the device onboarded message for the switch serial number followed by the configuration push and login successful messages. For more information on troubleshooting Aruba CX switch onboarding issues, see Troubleshooting AOS-CX Switch Onboarding Issues.

Switches Table

The **Switches** table displays the following information:

- **Device Name**—Name of the switch or switch stack. For a switch stack, a stack icon is displayed next to the device name.
- **Type**—Type of switch. Following are the supported values:
  - **AOS-S**
  - **AOS-CX**
  - **AOS-S Stack**
- **Clients**—Number of clients connected.
- **Alerts**—Number of alerts from the switch or switch stack.
- **Model**—Model number of the switch. For a switch stack, the term **Stack** is displayed.
- **Config Status**—Configuration status of the switch or switch stack. Following are the supported values:
  - **In sync**
  - **Not in sync**
- **Last Seen**—Date and time when the switch or switch stack was last connected.
- **Usage**—Data usage on the switches.
- **IP Address**—IP address of the switch or switch stack.
- **MAC**—MAC address of the switch or switch stack.
- **Firmware Version**—Firmware version of the switch or switch stack.
- **NAE Status**—Consolidated status of the NAE agents running on the AOS-CX switch. Following are the supported values:
  - **Critical**
  - **Major**
  - **Minor**
  - **Normal**
  - **Disabled**

The NAE Status is applicable only for AOS-CX switches.

- **Group**—Name of the group to which the switch or switch stack is assigned.

- **Labels**—Name of the label associated with the switch or switch stack.
- **Site**—Site in which the switch or switch stack is provisioned.
- **Uptime**—Duration for which the switch is operational.
- **Serial/Stack ID**—Serial number of the switch or switch stack.
- **Uplink Ports**—Uplink ports configured on the switch or switch stack.
- **Port Utilization**—Utilization percentage of the port.

NOTE

A search filter is provided only for the **Device Name** and **Model** columns.

To download the switch details as a **.csv** file, click the **Download CSV** icon. If the table contains unicode value, you must use a UTF-8 enabled software to view the contents. To view the file, open the file in a Microsoft Excel spreadsheet software.

Assigning Uplink Ports

To assign uplink port(s):

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.

   A list of switches is displayed in the **List** view.
3. In the **Switches** table, hover over the switch for which you want to assign uplink port(s).
4. Click **Uplinks**.
5. In the **Assign Uplink Ports/Trunks** dialog box, select the ports in the **Assigned Uplink Ports/Trunks** drop-down. On selecting the ports, the uplink rates for the selected ports are displayed in the uplink trend chart. For more information, see Uplink.
6. Click **Assign**.

Deleting an Offline Switch

To delete an offline switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selection contains at least one switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.

   A list of switches is displayed in the **List** view.
3. Click **Offline** to display a table with the list of offline switches.
4. In the **Switches** table, hover over the offline switch that you want to delete.
5. Click the delete icon.

NOTE

To delete multiple offline switches, select the offline switches that you want to delete, and click the

NOTE

delete icon at the bottom of the page.

6. Click **Yes** in the confirmation dialog box.

Downloading Switch Details

You can download the switch details as a .csv file.

To download the switch details, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. In the **Switches** table, click the download icon to download the switches details as a .csv file.

   A .csv file is downloaded.

Monitoring Switches in Summary View

The Switches Summary page provides a graphical view of all metrics about the usage and clients information associated with the switch provisioned and managed in Aruba Central.

Viewing the Switches Summary Page

To navigate to the Switches Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices > Switches**.

   A list of switches is displayed in the **List** view.
3. Click the **Summary** icon.

   The Switches Summary page is displayed with the following information:
   - **Usage**—Displays aggregate client data traffic detected on the switches.
   - **Clients**—Displays the number of clients connected to a switch.

   You can change the time range by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

Switch > Overview > Summary

In the switch dashboard, the **Summary** tab displays the switch device details, network details, ports, hardware, uplink graph, usage graph, and details about the stack members.

The **Summary** tab displays the following sections:

- Switch
- Network
- Ports

- Hardware
- Uplink
- Usage
- Stack Members
- Actions

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Overview** > **Summary** .

   The **Summary** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

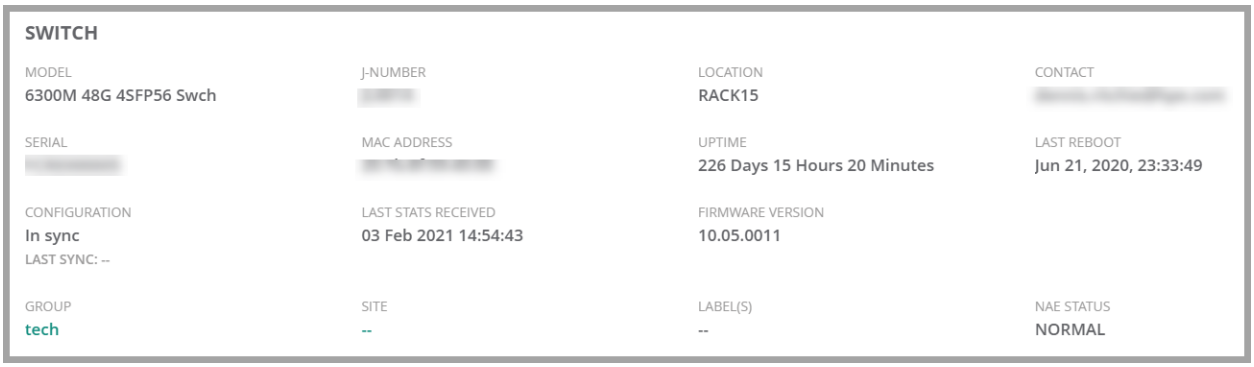
Switch

The **Switch** section displays the following details:

- **Model**—Hardware model of the switch.
- **J-Number**—Part number of the switch. This field is displayed only for standalone switches that are not part of switch stacks.
- **Location**—Current location of the switch.
- **Contact**—E-mail address of the contact person.
- **Conductor**—Serial number of the conductor switch in a switch stack. This field is displayed only for switch stacks.
- **Serial**—Serial number of the switch. This field is displayed only for standalone switches that are not part of switch stacks.
- **MAC Address**—MAC address of the switch. This field is displayed only for standalone switches that are not part of switch stacks.
- **Uptime**—Time duration for which the switches are operational.
- **Last Reboot**—Timestamp of when the switch was last rebooted.
- **Configuration**—Configuration status of the switch.
- **Last Sync:**—Timestamp when the configuration was last synched between the peer switches in the stack.
- **Last Stats Received**—Timestamp of when the last statistics were received.

- **Firmware Version**—Firmware version of the switch. If an updated version is available, the version number is displayed and you can click the link to navigate to the firmware management page and upgrade the firmware.
- **Last Updated**—Timestamp of when the switch firmware was last changed.
- **Firmware Status**—Displays whether a new firmware version is available.
- **Group**—Name of the group to which the switch belongs. Click the group name to view the dashboard context for the group.
- **Site**—Name of the site to which the switch belongs. Click the site name to view the dashboard context for the site.
- **Label(s)**—Name of the label to which the switch belongs.
- **NAE Status**—Consolidated status of the NAE agents running on the AOS-CX switch.

Figure 153 *Switch Overview*

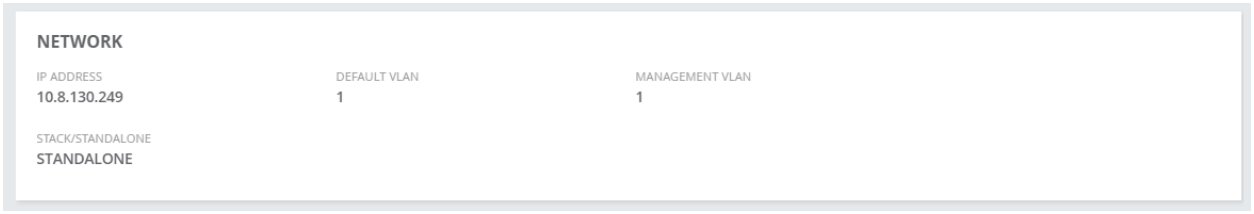


Network

The **Network** section displays the following details:

- **IP Address**—IP address of the switch. For AOS-CX switches, a value is displayed only if the IP address is configured for the management interface of the switch. If IP address is obtained from the DHCP server, this field will appear blank for AOS-CX switches.
- **Default VLAN**—Default VLAN ID of the switch.
- **Management VLAN**—Management VLAN ID of the switch. This field is displayed only for AOS-Switches.
- **Stack/Standalone**— Indicates whether the switch is part of a stack or if it is a standalone switch.
- **Stack Members**—Total number of members in the stack. This field is displayed only for switch stacks.
- **Stack Topology**—Topology of the stack.
- **Stack ID**—Stack ID used to identify the stack. This field is displayed only for switch stacks.

Figure 154 *Network Details*

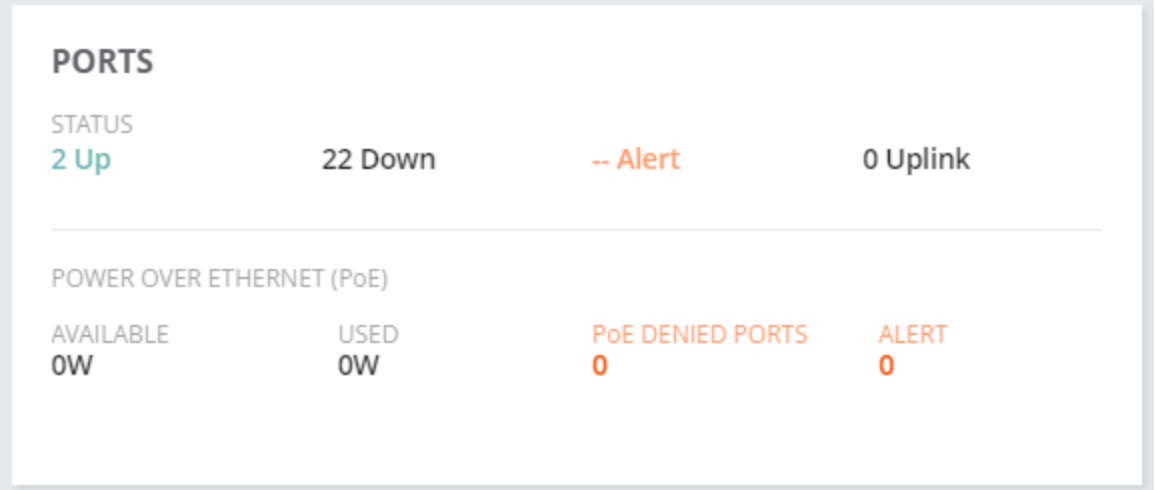


Ports

The **Ports** section displays the following details:

- **Status**—Number of ports in Up and Down state, and number of alerts.
- **Power Over Ethernet (PoE)**—Number of PoE ports enabled and disabled, and number of alerts.

Figure 155 *Port Summary*

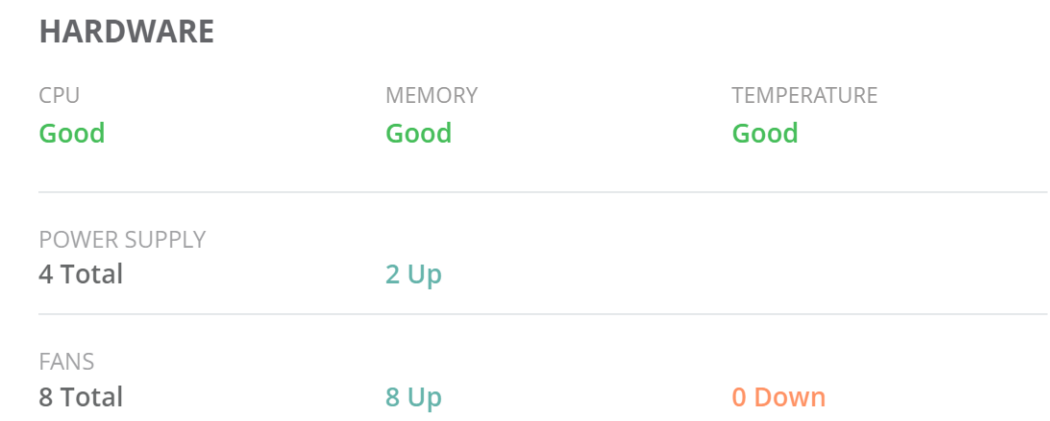


Hardware

The **Hardware** section displays the following details:

- **Power Supply**—Total number of power supplies and number of power supplies in Up state.
- **Fans**—Total number of fans and the number of fans in the Up and Down states.
- **CPU**—CPU utilization status.
- **Memory**—Memory utilization status.
- **Temperature**—Temperature status. Hover your mouse over the status to view the temperature data.

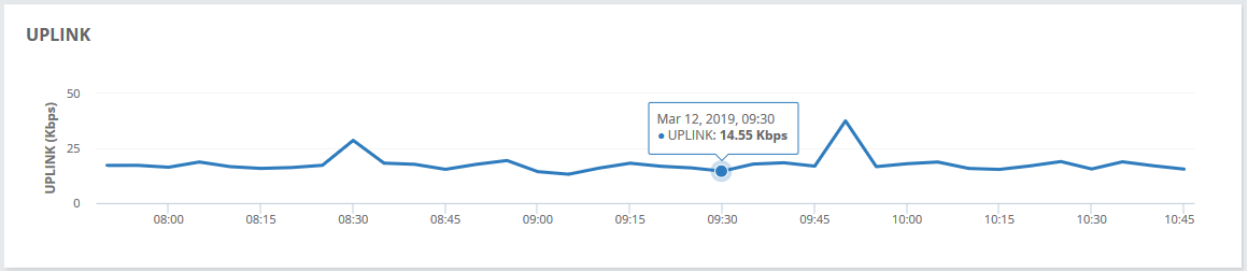
Figure 156 *Hardware Details*



Uplink

The **Uplink** section displays the uplink rate (bps) trend chart for the duration specified in the time range filter. Hover the mouse over the trend chart to view the uplink rate at a particular time.

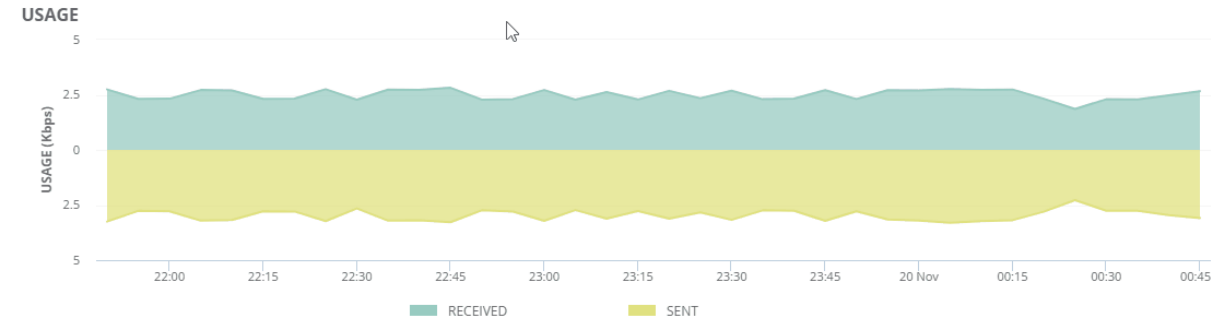
Figure 157 *Uplink Trend Chart*



Usage

The **Usage** section displays the trend chart for client data traffic detected on the switch. Hover your mouse over the trend chart to view data transmitted and received at a particular time.

Figure 158 *Usage Graph*



Stack Members

The **Stack Members** table displays the following details:

- **Name**—Name of the switch stack member.
- **Member ID**—Identification number of the member.
- **Model**—The hardware model of the switch.
- **MAC Address**— The MAC address of the stack member.
- **Serial**— The serial number of the switch.
- **Role** —The role of a stack member.
- **Status**—The status of the switch stack member.
- **Priority**—Priority of the member. This column is not displayed for AOS-CX switches.

Figure 159 *Stack Members Table*

STACK MEMBERS

Name	Member ID	Model	MAC Address	Serial	Role	STATUS	Priority
GSK-2930M-2	1	Aruba2930M-24G-PoE+ Swi	[redacted]	[redacted]	Conductor	Up	128

Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > Overview > Hardware

In the switch dashboard, the **Hardware** tab displays information related to power supplies, fans, utilization, and temperature. The **Hardware** tab displays the following sections:

- Hardware
- Power Supplies
- Fans
- CPU
- Memory
- Temperature
- Thermals
- Actions

Viewing the Overview > Hardware Tab

To navigate to the **Hardware** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Overview** > **Hardware** .

   The **Hardware** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

Hardware

The **Hardware** table displays the overall hardware summary:

- **ID**—Identity of the hardware.
- **Name**—Name of the device.
- **Power Supplies**
  - **Total**—Total number of power supplies.
  - **Up**—Number of power supplies in Up state.
  - **Down**—Number of power supplies in Down state.
- **Fans**
  - **Total**—Total number of fans.
  - **Up**—Number of fans in Up state.
  - **Down**—Number of fans in Down state.
- **Utilization**
  - **CPU**—Current CPU utilization percentage.
  - **Memory**—Current memory utilization percentage.
- **Temperature**
  - **Current**—Current temperature. This column is available only for AOS-Switches.
  - **Min**—Minimum temperature. This column is available only for AOS-Switches.
  - **Max**—Maximum temperature. This column is available only for AOS-Switches.
  - **Sensors**—Number of sensors present in the switch. The number inside the brackets show the number of sensors whose status is high. This column is available only for AOS-CX switches.

Figure 160 *Hardware table details for AOS-Switch*

HARDWARE

	POWER SUPPLIES			FANS			UTILIZATION		TEMPERATURE		
NAME	TOTAL	UP	DOWN	TOTAL	UP	DOWN	CPU	MEMORY	CURRENT	MIN	MAX
HP-Switch...	2	1	0	6	5	0	0%	27%	24 °C	24 °C	25 °C

Figure 161 *Hardware table details for AOS-CX switch*

HARDWARE

	POWER SUPPLIES			FANS			UTILIZATION		TEMPERATURE
NAME	TOTAL	UP	DOWN	TOTAL	UP	DOWN	CPU	MEMORY	SENSORS
6400-VSX-Primary	4	2	0	8	8	0	11%	10%	30 (0 HIGH)

Power Supplies

The **Power Supplies** table displays the following details:

- **Name**—Name of the power supply.
- **Status**—Current status of the power supply.

Fans

The **Fans** table displays the following details:

- **Name** —Name of the fan.
- **Status**—Current status of the fan.

CPU

The **CPU** section displays the current CPU utilization percentage and trend chart. Hover over the trend chart to view the CPU utilization at a particular time.

Memory

The **Memory** section displays the current memory utilization percentage and trend chart. Hover over the trend chart to view the memory utilization at a particular time.

Temperature

NOTE

This section is available only for AOS-Switches.

The **Temperature** section displays the current, minimum, and maximum temperature and trend chart. Hover over the trend chart to view the temperature at a particular time.

Figure 162 *Temperature*

Thermals

NOTE

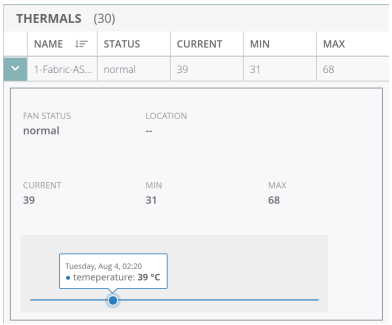
This section is available only for AOS-CX switches.

The **Thermals** table displays the following details of each of the sensors that are present in the AOS-CX switches:

- **Name**—Name of the component where the sensor is present.
- **Status**—Current status of the fan.
- **Current**—Current temperature of the component.
- **Min**—Minimum temperature of the component.
- **Max**—Maximum temperature of the component.

Expand each of the rows to display the fan status, location of the fan, current, minimum, and maximum temperatures, and a temperature trend chart. Hover over the trend chart to view the temperature at a particular time.

Figure 163 *Thermals*



Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

NOTE

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > Overview > Routing

NOTE

The **Routing** tab is displayed only for AOS-Switches that run the firmware version 16.09 or later.

In the switch dashboard, the **Routing** tab displays the following sections:

- Overview of Routing Information
- Routing
- Actions

Viewing the Overview > Routing Tab

To navigate to the **Routing** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.

3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.

4. Under **Manage**, click **Overview** > **Routing** .

   The **Routing** tab is displayed.

5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

Overview of Routing Information

- This section displays the following routing information:
  - **Total**—Displays the total number of routes on the switch.
  - **Static**—Displays the total number of static routes on the switch.
  - **Connected**—Displays the total number of connected routes on the switch.
  - **Dynamic**—Displays the total number of dynamic routes on the switch.

Routing

The **Routing** table displays the following details:

- **Destination**—Displays the network address of the destination route.
- **Gateway**—Displays the IP address of the gateway.
- **VLAN**—Displays the VLAN ID of the route destination.
- **Type**—Displays the following types of routes:
  - **Static**—The routes that are manually added to the routing table in the switch.
  - **Connected**—The routes that are directly connected to the interface.
- **Sub Type**—Displays the subtype of the route as Internal or External.
- **Metric**—Displays the measure used to calculate the best path to reach the destination. A value of 1 indicates the best path, 15 indicates the worst path, and 16 indicates that the destination is unreachable on the route.
- **Distance**—Displays the administrative distance of the route. The administrative distance helps routers determine the best route when there are multiple routes to the destination.

The routing information is displayed from the Aruba 3810 Switch Series and Aruba 5400R Switch Series in the network. The details displayed on the **Routing** tab are refreshed every five minutes.

Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > Overview > AI Insights

In the switch dashboard, the **AI Insights** tab displays information on switch performance issues such as PoE issues, port errors, port flaps, airtime utilization, and memory utilization.

Viewing Switches > AI Insights

To navigate to the **AI Insights** tab in the switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the switch is displayed.
4. In the switch dashboard context, click the **AI Insights** tab.

   The **Insights** page is displayed.

   To exit the switch dashboard, click the back arrow on the filter.

   You can change the time range for the **AI Insights** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** ( ) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

- Red—High priority
- Orange—Medium priority
- Yellow—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. Each insight report provides specific details on the occurrences of these events for ease in debugging. For more information, see The AI Insights Dashboard.

The switch **AI Insights** page displays the following insights:

- AOS-Switches with High CPU Utilization
- AOS-Switches with High Memory Usage
- AOS-Switch Ports with High Power-over-Ethernet Problems
- AOS-Switches with High Port Errors
- AOS-Switches with High Port Flaps
- AOS-CX Switches with High CPU Utilization
- AOS-CX Switches with High Memory Usage
- AOS-CX Switch Ports with High Power-over-Ethernet Problems
- AOS-CX Switches with High Port Errors
- AOS-CX Switches with High Port Flaps

Switch > Clients > Clients

In the switch dashboard, the **Clients** tab displays details about the wired clients that are connected to the switch. This tab also displays a visual representation of the switch faceplate with port details.

The **Clients** tab displays the following details:

- Overview of Connected Devices
- Faceplate
- Client Devices
- Actions

Viewing the Clients > Clients Tab

To navigate to the **Clients** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Clients** > **Clients**.

   The **Clients** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **Clients** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Overview of Connected Devices

This section displays the following details:

- **Total**—Total number of clients connected to the switch.
- **Non-Tunneled**—Number of clients, that are not tunneled connected, to the switch.
- **User Based Tunneled (UBT)**—Number of UBT clients connected to the switch.

- **Port Based Tunneled (PBT)**—Number of PBT clients connected to the switch.

NOTE

To view the details about dynamic segmentation, a gateway must be licensed in and connected to the switch.

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on a port to view port-level information. On the switch faceplate, hover over a port to view the following details:

- Port Number
- Port Name
- Speed
- Type
- Tunneled

Client Devices

The **Client Devices** tab displays the following details:

NOTE

The VLAN Type, Primary VLAN ID, and Primary VLAN Name columns are not displayed for AOS-CX switches.

- **Name**—Displays the name of the client device.
- **Status**—Displays the status of the client as Connected, Disconnected, Failed, Connecting, or Blacklisted.
- **Port**—Displays the port number of the switch the client device is connected to. If the port is part of a LAG, the LAG name is displayed.
- **MAC Address**—Displays the MAC address of the client device.
- **IP Address**—Displays the IP address of the client device. The IP address is displayed only if the client is directly connected to the switch or if the IP tracker is enabled on the switch.
- **VLAN ID**—Displays the VLAN ID of the client device.
- **VLAN Name**—Displays the VLAN name of the client device.
- **VLAN Type**—Displays the following VLAN types of the client device
  - Normal—The subnetwork which can group devices on separate physical LANs.
  - Primary—The standard VLAN that is partitioned to create a private VLAN.
  - Isolated—Secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports.
  - Community— Secondary VLAN that forwards traffic between ports which belong to the same community and to the promiscuous ports.
- **Primary VLAN ID**—Displays the primary VLAN ID of the client device.
- **Primary VLAN Name**—Displays the primary VLAN name of the client device.
- **Authentication**—Displays the authentication type of the client device.
- **Usage**—Displays the total data usage by the client device for the selected time period.
- **Tunneled**—Indicates whether the client is a tunneled client or not. **Yes** or **No**.
- **Segmentation**—Displays the type of dynamic segmentation configured for the client. Supported values are **UBT**, **PBT**, **Underlay**, **Overlay**, or **None**.

- **Switch Role**—Name of the role that the switch assigns to the client.
- **Gateway Role**—Name of the role that the gateway assigns to the client.
- **Gateway Name**—Name of the gateway.

NOTE

The wired client will show up in the **Client Devices** table only if the client is connected to an Aruba 2540 Switch Series, Aruba 2920 Switch Series, Aruba 2930F Switch Series, Aruba 2930M Switch Series, Aruba 3810 Switch Series, Aruba 5400R Switch Series, or any of the AOS-CX switches.

Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

NOTE

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > Clients > Neighbours

In the switch dashboard, the **Neighbours** tab displays details about the devices neighboring the switch.

The **Neighbours** tab displays the following details:

- Neighbour Devices
- Actions

Viewing the Clients > Neighbours Tab

To navigate to the **Clients** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **Clients** > **Neighbours**.

   The **Neighbours** tab is displayed.

5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **Neighbours** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

Neighbour Devices

The **Neighbours** tab displays the following details:

- **MAC Address**—Displays the MAC address of the neighboring device.
- **Hostname**—Displays the hostname of the neighboring device.
- **IP Address**—Displays the IP address of the neighboring device.
- **Description**—Displays the description of the neighboring device.
- **Local Port**—Displays the local port number of the neighboring device.
- **Remote Port**—Displays the remote port number of the neighboring device.
- **Capabilities**—Displays the capabilities of the neighboring device.
- **VLAN ID(s)**—Displays the VLAN IDs of the neighboring device.

Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > LAN > Ports

In the switch dashboard, the **Ports** tab displays details about ports and the LAGs configured in the switch.

The **Ports** tab displays the following details:

- Port Status
- Faceplate
- Ports
- LAGS
- Viewing Port-Level Information
- Actions

Viewing the LAN > Ports Tab

To navigate to the **Ports** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **LAN** > **Ports**.

   The **Ports** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **Ports** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

Port Status

The **Port Status** section displays the total number of ports for the following:

- **Up**—Ports in up state
- **Down**—Ports in down state
- **Alert**—Alerts generated
- **Uplink**—Number of uplink ports

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover over a port to view the following details:

- Port
- Name
- Type
- Speed
- LAG
- Reason (Applicable only to AOS-CX switches)

Ports

The **Ports** table displays the following details:

- **Port**—Port number. Use the column filter to search for a particular port and use the sort option to sort the ports in ascending or descending order.
- **Name**—Name of the switch.
- **Status**—Status of the switch. Use the column filter to filter by status.
- **Type**—Type of switch port. Use the column filter to filter by type.
- **MTU (Bytes)**—MTU size of the switch.
- **Speed (Mbps)**—Port speed of the switch.
- **LAG**—If the port is part of a trunk group or LAG, the name of the trunk group or LAG is displayed.

- **Admin**—Admin status of the switch.
- **MAC Address**—MAC address of the switch.
- **VLAN**—VLAN ID of the port.
- **VLAN Mode**—VLAN mode of the port. Supported values are **Access** or **Trunk**.
- **Native VLAN**—Native VLAN ID of the port.
- **Reason**—Indicates the reason when the switch is down. This field is displayed only for AOS-CX switches.

LAGS

The LAGs table displays the list of LAGs with the following details:

- **Name**—Name of the LAG. Use the sort option to sort the LAGs in ascending or descending order.
- **Up Ports**—Number of uplink ports in the LAG and their port numbers.
- **Down Ports**—Number of downlink ports in the LAG and their port numbers.
- **VSX**—Indicates whether VSX is enabled or disabled in the LAG. This column is displayed only for AOS-CX switches.

Viewing Port-Level Information

Use one of the following options to navigate to the port and view port-level information:

- In the switch faceplate, click on the port number.
- In the Ports table, click the port number.

  The port-level information page consists of the following sections:
- **Status**—The **Status** section displays the following details:
  - Operational status
  - Admin status
  - Type of port
  - Description
  - MAC Address
  - Name
  - Untagged VLAN
  - Tagged VLAN
  - Trunk group
  - Usage In
  - Usage Out
- **Port Usage**—The **Port Usage** section provides a graphical representation of data received and transmitted by the port. Each line in the graph is a sum of the received and sent traffic for a given uplink port. Hover over the graph to view data for a particular time of the day.
- **Frame Counters**—The **Frame Counters** section provides a graphical representation of the interface frame counters. From the drop-down, select one of the following options:
  - **Unicast**
  - **Broadcast**
  - **Multicast**

- **Discards**
- **Error**

Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > LAN > PoE

In the switch dashboard, the **PoE** tab displays details, such as, PoE status summary, PoE ports, and PoE consumption.

The **PoE** tab displays the following details:

- PoE Status
- Faceplate
- Ports PoE
- PoE Consumption
- Viewing PoE Port-Level Information
- Actions

Viewing the LAN > PoE Tab

To navigate to the **PoE** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **LAN** > **PoE**.

   The **PoE** tab is displayed.

5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **PoE** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

The **PoE** tab is displayed only if the AOS-Switch or the AOS-CX switch supports PoE.

The **PoE** tab displays monitoring data only if the AOS-Switch firmware version is 16.08.0001 or later.

PoE Status

The **PoE Status** section displays the following details:

- **Available**—Power available for consumption for the switch or stack.
- **Used**—Power used by various devices.
- **Remaining**—Power remaining to be utilized in the stack or device.
- **PoE Denied Ports**—Number of ports for which power is denied.
- **Alerts**—Number of alerts generated.

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover over a PoE port to view the following details:

- Port
- Name
- Type
- Class
- Priority

From the **Context** drop-down, select the context:

- **POE-STATUS**—Displays the sate of each port. The state can be: Uplink, Drawing, Enabled, Disabled, or Alert.
- **POE-CLASS**—Power class of the PoE port. The class can be: Class0, Class1, Class2, Class3, Class4, or Disabled.
- **POE PRIORITY**—PoE priority configured on the port. The priority can be: Critical, High, or Low.

Ports PoE

The **Ports PoE** table displays the following details:

- **Port**—Port number.
- **Name**—Name of the port.
- **PoE**—PoE state: Enabled or Disabled.
- **Priority**—PoE priority: Critical, High, or Low.
- **Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.
- **Pre-STD Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off.
- **Alloc Actual**—Power actually being used on the port.

- **Alloc Configured**—The maximum amount of power allocated for the port.
- **PLC Class**—Power class of the PoE port.
- **PLC Type**—Physical layer classification type.

PoE Consumption

The **PoE Consumption** section displays a trend chart for the PoE power drawn from the switch in watts. Hover over the trend chart to view the PoE power drawn at a particular time. For a stack, select the switch from the drop-down to view the PoE consumption for the specific device (conductor, standby, or member.)

Viewing PoE Port-Level Information

Use one of the following options to navigate to the PoE port and view port-level information:

- In the switch faceplate, click on the port number.
- In the **Ports PoE** table, click the port number.

The port-level information pane displays the following details:

- Summary
- Slot Info & PoE Configuration
- LLDP Information

Summary

The **Summary** tab displays the following sections:

- **Summary**—Displays the following details:
  - **PSE Reserved Power**—Power reserved for the port in the Power Sourcing Equipment (PSE).
  - **PSE Voltage**—Total voltage, in volts (V), currently being delivered to the powered device connected to the port
  - **PD Power Draw**—Power drawn by the powered device.
  - **PD Amperage Draw**—Amperage drawn by the powered device.
  - **Over Current Count**—Number of times a powered device connected to the port attempted to draw more power than was allocated to the port.
  - **MPS Absent Count**—Number of times the powered device has no longer requested power from the port MPS is Maintenance Power Signature.
  - **Power Denied Count**—Number of power requests from the port that were denied because sufficient power was unavailable.
  - **Short Count**—Number of times the switch provided insufficient current to the powered device connected to the port.
- **PoE Consumption**—Displays the trend chart for PoE consumption and power available for the duration specified in the time range filter

Slot Info & PoE Configuration

The **Slot Info & PoE Configuration** tab displays the following sections:

- **PoE Slot Information**—Displays the following details:
  - **Slot**—Slot where the port is located.
  - **Operation Status**—Operational status of the PoE slot: On, Off, or Faulty.

- **Maximum Power**—Maximum PoE wattage available to provision active PoE ports in the slot.
- **Power In Use**—PoE power currently being used by the slot.
- **Usage Threshold**—Configured percentage of available PoE power provisioning the switch must exceed to generate a usage notice.

- **PoE Configuration**—Displays the following details:
  - **PoE Power**—Displays whether PoE power is enabled on the port.
  - **Pre STD Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off. This field is not displayed for AOS-CX switches.
  - **PoE Port Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.
  - **Power Priority**—Power priority configured on ports enabled for PoE: Low, High, or Critical.
  - **Allocate by Configuration**—Maximum amount of power allocated for the port.
  - **Allocate by Actual**—Power actually being used on the port.
  - **PLC Class Type**—Physical layer classification type.
  - **DLC Class Type**—Data link layer classification type.
  - **Configured Type**—If configured, shows the user-specified identifier for the port. If not configured, this field is empty.
  - **PoE Value configuration**—PoE power value configured for the port. This field is not displayed for AOS-CX switches.

LLDP Information

The **LLDP Information** tab displays the following details:

- **UPSE Allocated Power**—Power allocated for the port in the PSE.
- **PD Requested Power**—Power requested by the powered device.
- **PD TLV Sent Type**—TLV that is actually sent from the powered device.
- **PSE TLV Configured**—TLV that is configured for the switch port to send to the powered device.
- **PSE TLV Sent Type**—TLV that is actually sent from the PSE.
- **MED LLDP Detect**—Status of the PoE LLDP detection. This field is not displayed for AOS-CX switches.

Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > LAN > VLAN

In the switch dashboard, the **VLAN** tab displays VLAN information configured on the switch and details about tagged and untagged ports.

The **VLAN** tab displays the following details:

- VLANs
- Faceplate
- Actions

Viewing the LAN > VLAN Tab

To navigate to the **VLAN** tab in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active switch.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**.

   The dashboard context for the specific switch is displayed.
4. Under **Manage**, click **LAN** > **VLAN**.

   The **VLAN** tab is displayed.
5. To exit the Switch dashboard, click the back arrow on the filter.

   You can change the time range for the **VLAN** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, or **3 months**.

VLANs

The **VLANs** table displays the following details:

The **Type**, **Primary VLAN**, **Promiscuous**, **ISL**, and **Jumbo** columns are displayed only for AOS-Switches.

- **Name**—Displays the name of the VLAN. Click the sort icon to sort the VLAN names in the column.
- **ID**—Displays the VLAN ID associated with the VLAN.
- **Status**—Displays the status of the VLAN as Up or Down.
- **Type**—Displays the following types of VLANs:
  - **Regular VLAN**—A regular VLAN is a single broadcast domain.
  - **Private-Primary**—The regular VLAN which partitions one broadcast domain into multiple smaller broadcast sub-domains.
  - **Private-isolated**—Secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports.
  - **Private-Community**—Secondary VLAN that forwards traffic between ports which belong to the same community and to the promiscuous ports.
- **Primary VLAN**—Displays the primary VLAN details.

- **Promiscuous**—Displays the promiscuous port value. A promiscuous port is a switch port that is connected to an uplink router, firewall, or other common gateway device, and can communicate with all ports within a private VLAN, including the ports in the isolated and community VLANs. By default, every primary VLAN port acts as a promiscuous port.
- **ISL**—Displays the Inter-switch Link (ISL) port value (range). ISL port is also called PVLAN member port. ISL port is required in multi-switch PVLAN configurations to span the switches. The ISL port will automatically become a member of all VLANs within the PVLAN and it carries traffic from the primary VLAN and all secondary VLANs
- **Tagged Ports**—Displays the ports that have marked the VLAN as tagged.
- **Untagged Ports**—Displays the ports that have marked the VLAN as untagged.
- **IP address**—Displays the IP address of the VLAN.
- **Voice**—Displays whether the Voice is enabled or disabled for the VLAN.
- **IGMP**—Displays whether the IGMP is enabled or disabled for the VLAN.
- **Jumbo**—Displays whether the Jumbo packets are enabled or disabled for the VLAN.

Faceplate

From the **VLANs** table, select a VLAN to view the tagged and untagged ports, promiscuous port, ISL port, and the VLAN types in the faceplate.

Figure 164 *VLANs Tab Details for AOS-Switch*

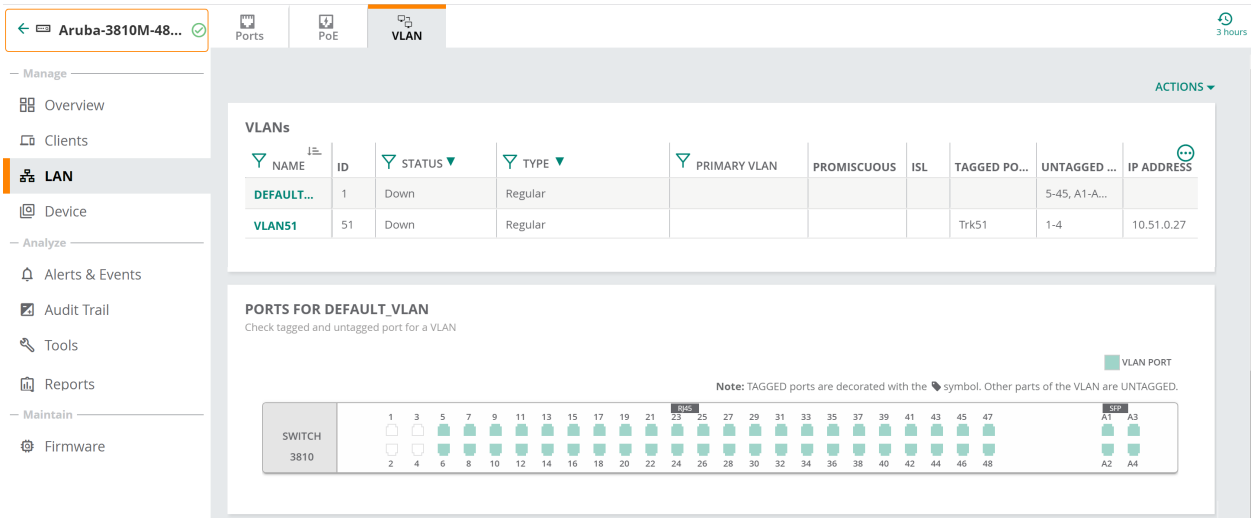
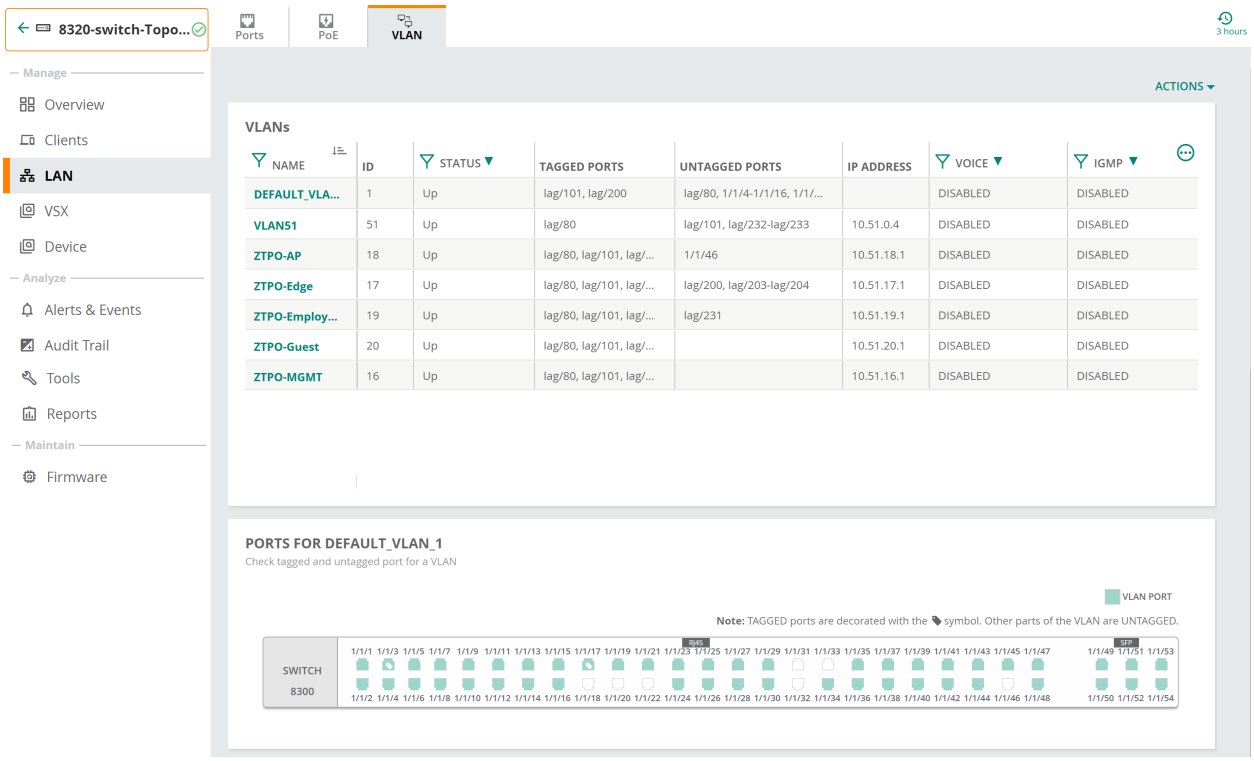


Figure 165 *VLAN Tab Details for AOS-CX Switch*



Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

NOTE

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > VSX

Aruba Virtual Switching Extension (VSX) is virtualization technology for aggregation and core AOS-CX switches. The VSX solution lets the switches present as one virtualized switch in critical areas.

VSX is supported in the AOS-CX 6400 Switch Series, AOS-CX 8320 Switch Series, and AOS-CX 8325 Switch Series.

Aruba Central provides support for VSX by displaying information about the configurations of the switches and the status of the inter-switch link (ISL) between the switches.

Viewing the VSX Page

To navigate to the VSX page in the Switch dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group**, **Label**, or **Site**. Ensure that the filter selection contains at least one AOS-CX switch. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. Click an AOS-CX switch under **Device Name**.

   The dashboard context for the switch is displayed.
4. Under **Manage**, click **VSX**.

   The **VSX** page displays the following details:
   - VSX Summary
   - Info
   - Actions
5. To exit the switch dashboard, click the back arrow on the filter

VSX Summary

Displays state information of the switch, connections to the peer switch, and the role of the switch in the VSX configuration.

Table 228: *VSX Summary Details*

Field	Description
ISL State	State of the ISL connection with the peer AOS-CX switch. Following are the supported values: ■ **WAITING_FOR_PEER**—Waiting for connectivity to the peer. ■ **PEER_ESTABLISHED**—Steady state. VSX LAGs are up when the device is in this state. ■ **SPLIT_SYSTEM_PRIMARY**—Lost ISL connectivity to the peer and the device is operating as primary. ■ **SPLIT_SYSTEM_SECONDARY**—Lost ISL connectivity to the peer and the device is operating as secondary. ■ **SYNC_PRIMARY**—ISL connectivity to the peer restored and the device is syncing states to the peer. ■ **SYNC_SECONDARY**—ISL connectivity to the peer restored and he device is learning states from the peer. VSX LAGs are down when the device is in this state. ■ **SYNC_SECONDARY_LINKUP_DELAY**—Device has learned its states from the peer and monitoring for hardware is to be programmed. VSX LAGs are down when the device is in this state.
ISL Mgmt State	Management state of the ISL. Following are the supported values: ■ **OPERATIONAL**—ISL management is operational. ■ **INTER_SWITCH_LINK_MGMT_INIT**—ISL management is in initialization state. ■ **CONFLICTING_OR_MISSING_DEVICE_ROLES**—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers. ■ **SW_IMAGE_VERSION_MISMATCH_ERROR**—Software version on the primary device does not match with the software version on the secondary device.

Field	Description
	▪ **INTER_SWITCH_LINK_DOWN**—ISL is down. ▪ **INTERNAL_ERROR**—ISL management has internal errors.
Config Sync Status	Status of the configuration synchronization between the VSX switches. Following are the supported values: ▪ **IN-SYNC**—Configuration synchronization is operational and the VSX switches are in sync. ▪ **DISABLED**—Configuration synchronization is disabled. ▪ **SW_IMAGE_VERSION_MISMATCH_ERROR**—Software image version on the primary device does not match with the software image version on the secondary device. ▪ **CONFLICTING_OR_MISSING_DEVICE_ROLES**—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers. ▪ **PEER_DB_CONNECTION_ERROR**—Error in connecting to peer database. It involves errors due to ISL or ISL management. ▪ **CONFIGURATION_SYNC_CONFLICT**—Configuration synchronization is operational but has conflicts synchronizing the configuration. Conflicts can occur if the configuration on the primary device is marked for sync, but the same configuration on the secondary device is not marked for sync. ▪ **CONFIGURATION_SYNC_MISSING_REFERENCE**—Configuration synchronization is operational but has missing references in synchronizing the configuration.
NAE	Status of the NAE connection between the VSX switches.
HTTPS Server	Status of the HTTPS server connection between the VSX switches.
Last Synched	Timestamp of when the configuration was synched between the peer switch. **NOTE:** Last synced data is displayed in the **VSX** page only when VSX synchronization is enabled for the AOS-CX switch. However, enabling VSX synchronization using template configuration in Aruba Central is not recommended. By enabling VSX synchronization, the peer switch may get into an unknown configuration state.
Role	Role of the AOS-CX switch in the VSX configuration. Supported values are **Primary** and **Secondary**

Info

Displays system and configuration information of the switch and its peer. The following details are displayed:

- **System**
  - **Local MAC**—MAC address of the selected switch.
  - **Peer MAC**—MAC address of the peer switch.
  - **Peer Hostname**—Hostname of the peer switch.
  - **Peer IP**—IPv4 address of the peer switch.
- **Configuration**
  - **Config Sync**—Indicates whether the configuration synchronization between the peers are enabled or disabled.
  - **ISL Port**—Inter-switch Link (ISL) port number of the selected AOS-CX switch. If the ISL is a LAG, then this field displays the LAG name.

- **Peer ISL Port**—ISL port number of the peer switch. If the ISL is a LAG, then this field displays the LAG name.
- **MC LAGs**—List of MC LAG names present in the switches.

Actions

The **Actions** down-down lists the following options available for remote administration of the switch:

- **Reboot**—Reboots the switch. See Rebooting Switches.
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device. See Troubleshooting Aruba Switches.
- **Console**—Opens the remote console for a CLI session through SSH. Ensure that you allow SSH over port 443. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening Remote Console for Switch.

If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

You can only troubleshoot Aruba switches using the **Console** option in Aruba Central. You cannot configure the switches.

Switch > Alerts & Events > Events

The events page displays events generated by the AOS-Switch and AOS-CX switches with the following severity:

- Emergency
- Fatal
- Alert
- Critical
- Error
- Warning
- Notice

For more information about the AOS-Switch events, see the *Event Log Message Reference Guide for ArubaOS-Switch*.

For more information about the AOS-CX switch events, see the *AOS-CX Event Log Message Reference Guide*.

Rebooting Switches

You can reboot a switch using the Aruba Central UI.

To reboot a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices** > **Switches**.
   A list of switches is displayed in the **List** view.
3. Click **Online** to display a table with the list of online switches.
4. In the Switches table, click the switch to reboot.
   The Switches Details page corresponding to the switch is displayed.
5. In the **Actions** drop-down, click **Reboot**.
   A **Reboot Switch** dialog box is displayed.
6. Click **Continue** to reboot the switch.
   All clients connected to this switch are disconnected and the switch reboots.

The Switches Details page takes less than a minute to update the interface status after the switch is rebooted and reconnected to Aruba Central.

Opening Remote Console for Switch

In the Aruba Central UI, you can open the remote console for a CLI session through SSH for a switch. Ensure that you allow SSH over port 443.

For AOS-CX 8320 and 8325 switch series, you must enable SSH server on either the default VRF or the management VRF depending on the type of VRF that the switch uses to connect to Aruba Central. You must add one of the following commands in the template:

- If the switch is connecting to Aruba Central using inline default VRF, add `ssh server vrf default` to the template.
- If the switch is connecting to Aruba Central using OOBM management VRF, add `ssh server vrf mgmt` to the template.

You can only troubleshoot switches using the Console option in Aruba Central. You cannot configure the switches.

To open the remote console for a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups, Labels, or Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.
2. The dashboard context for the selected filter is displayed.
3. Under **Manage**, click **Devices** > **Switches**.
   A list of switches is displayed in the **List** view.
4. Click **Online** to display a table with the list of online switches.
5. In the Switches table, click the switch for which you want to open the remote console.
   The Switch Details page corresponding to the switch is displayed.
6. In the **Actions** drop-down, click **Open Remote Console**.
   A CLI session dialog box is displayed. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.

Troubleshooting Aruba Switches

You can troubleshoot a switch using the Aruba Central UI.

To troubleshoot a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed in the **List** view.
3. In the Switches table, click the switch to troubleshoot.

   The Switch Details page corresponding to the switch is displayed.
4. In the **Actions** drop-down, click **Tech Support**.

   The **Commands** page is displayed.
5. Select any command category in the **Categories** pane and the **Commands** pane displays the associated commands.

AOS-CX switches support only the show tech and show running-config commands.

6. Click **Add >** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box. For more information on filtering commands, see Filtering Commands.
8. (Optional) Select command(s) and click **< Remove** to remove selected command(s) or click **< Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
   a. Click the **Repeat** check box.
   b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
   c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**. The output is displayed in the **Device Output** section.

    For information about viewing and downloading the output, see Viewing the Device Output.

Enabling Unsupported Transceivers on AOS-Switches

AOS-Switches running software versions 16.02.0013 or later, support the use of third-party transceivers. Allowing unsupported transceivers enables the AOS-Switch to unblock the port and allow third-party transceivers to connect to the switch.

To enable this feature, complete the following procedure in Aruba Central:

1. Open the console of the switch using the console option in Aruba Central. For more information, see Opening Remote Console for Switch.
2. Login to the switch in the console.

3. Run the following command to enable Aruba Central support mode:

```
aruba-central support-mode enable
```

4. Run the following command to allow third -party transceivers to be connected to the AOS-Switch:

```
allow-unsupported-transceiver
```

5. Run the following command to save the running configuration of the switch to the startup configuration.

```
write memory
```

6. Run the following command to disable Aruba Central support mode:

```
aruba-central support-mode disable
```

7. Reboot the switch. For more information, see Rebooting Switches.
8. Verify the transceiver details by running the following command:

```
show tech transceivers
```

Troubleshooting AOS-CX Switch Onboarding Issues

Though an AOS-CX switch is displayed as online, there might be instances where the complete switch details are not displayed. To troubleshoot such issues, you can see the audit trail page to check the status of the switch.

To see the audit trail for a switch, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one switch. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**.

   A list of switches is displayed.
3. In the **Switches** table, click the switch you wish to troubleshoot.

   The dashboard context for the switch is displayed.
4. Under **Analyze**, click **Audit Trail**.

   The **Audit Trail** page is displayed.

   If a switch is onboarded successfully, the audit trail log displays the following messages:
   a. **Device : *<Device Serial Number>* Onboarded**
   b. **Applying template *<Template Configuration Name>* to device**

c. **Login Successful reading running configuration**

d. **Config push successful**

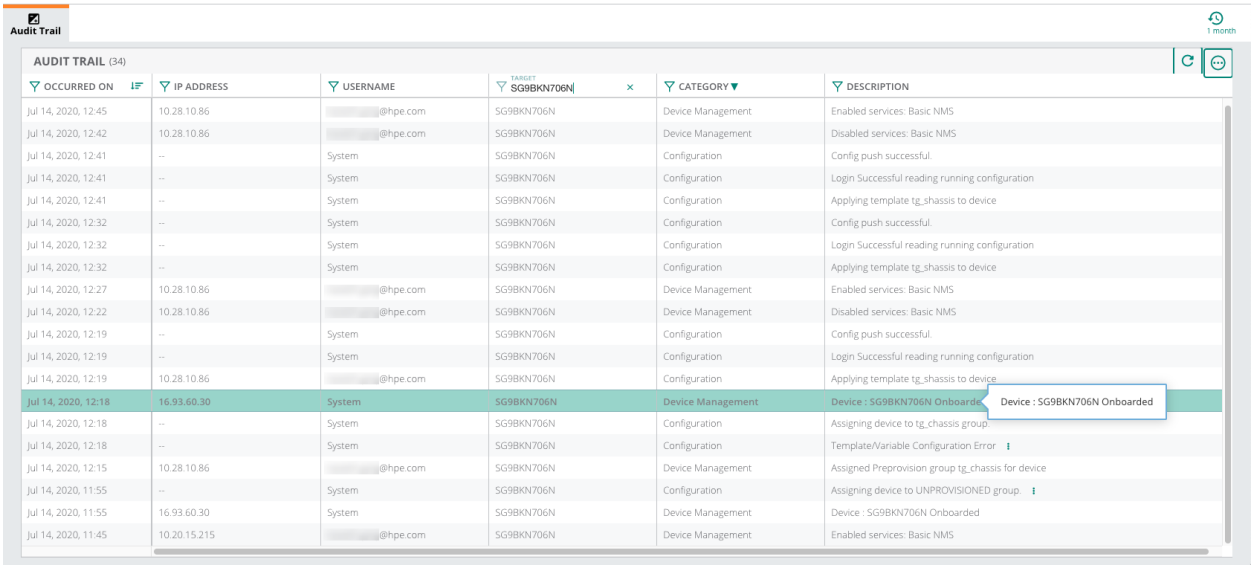
If applying template configuration to the AOS-CX switch fails, the **Template/Variable Configuration Error** error message is displayed:

If any of the messages listed in step 4b, 4c, 4d, or **Template/Variable Configuration Error** is not displayed in the audit trail logs, one of the following might be the reason:

- User has not created a template group with template configuration for the AOS-CX switch.
- User has created a template group with template configuration but has not moved the AOS-CX switch to the template group.

The following image displays the audit trail log of a switch that is successfully onboarded.

Figure 166 *Example Audit Trail Log for Successfully Onboarded AOS-CX Switch*



Chapter 12
Aruba SD-Branch Solution

The Aruba SD Branch solution offers the best-in-class wireless and wired infrastructure and management orchestration features with the SD-WAN capabilities. The SD Branch solution extends the SD-WAN concept to all elements in the branch to deliver a full stack solution that addresses the business challenges of distributed enterprises. Coupled with Aruba Central, the solution provides a cloud-hosted environment for simplified operations and improved agility.

Why SD-WAN?

A traditional branch setup supports client connectivity requirements across different geographical locations for various types of business operations. The sites in remote geographical locations serve as branch offices, while the headquarters or main office serves as a data center that hosts network resources to store, manage, and distribute data. The main office also hosts a centralized Virtual Private Network (VPN) management system to aggregate traffic from the remote branch sites. A Wide Area Network (WAN) —with Multiprotocol Label Switching (MPLS), T1, T3, Broadband, or Cellular links—is used for connecting multiple local area networks to a central corporate network or data centers separated by distance.

Due to an increase in the number of client devices at the remote sites and the new bandwidth requirements, branch office networks are expected rapidly scale to provide uninterrupted user experience. A traditional branch infrastructure with multiple appliances, different operating systems, and management tools only adds to the cost, involves a maintenance overhead, and demands skilled IT personnel.

The Aruba SD-WAN solution simplifies your branch deployments with a single management interface for administering, managing, and monitoring your branch networks. It also provides a unified policy enforcement framework with operational ease.

Key Features and Benefits

The SD-WAN solution comes with the following key capabilities:

- Zero Touch Provisioning of devices—Ability to self-provision without operator's intervention.
- Centralized overlay management and control—A single cloud-based network management interface for managing and monitoring SD Branch devices. Aruba Central, the cloud based network management system, supports unified management of SD branch devices with ZTP and hierarchical configuration.
- IPsec based Automatic VPN Tunnels—Support for high-performance and automatic IPsec VPN for secure overlay networking.
- Unified security policy for wired, wireless, and WAN—Support for a common security policy framework based on user roles for WAN, WLAN, and LAN users.
- Dynamic path selection—Support for dynamically steering traffic or a service request to the best available path. For example, you can configure a policy to dynamically route the real-time voice and video traffic on the link with the lowest latency and jitter, and the bulk file traffic on the link with the maximum bandwidth.
- Deep Packet Inspection and Web Content Classification—Support for monitoring and analyzing application usage by clients.

- Visibility, analytics, and troubleshooting—Dashboards for monitoring branch health, device performance, and client connectivity metrics. Alerts, reports, and audit trails for monitoring and troubleshooting network performance issues.
- Policy-based Routing—In addition to the traditional destination-based routing, the SD Branch devices support routing client traffic based on user role or type of application, For example, traffic generated from the guest devices can be routed directly to the internet, while traffic from the employees can be routed to the MPLS network.

Other Documentation Resources:

- Aruba SD-Branch Fundamentals Guide
- Aruba SD-Branch Security Hardening Guide

For more information about how SD-WAN works, see Understanding SD-WAN.

Understanding SD-WAN

The SD-WAN solution includes a new set of devices called Aruba Gateways that inter-operate with Aruba Switches and Instant APs to provide a full-fledged WAN architecture.

Based on the size of your branch setup, you can choose device combination that best suits your requirement:

- Medium to large branches—For branches that require more than 24 ports, you can use a combination of Branch Gateways and one or more Aruba switches at the branch site, with Aruba Gateways as VPN Concentrator (VPNC) at the data center.
- Small to medium branches—For branches that require less than 24 ports (including all WAN and LAN ports), you can deploy Branch Gateways at the branch sites, with Aruba Gateways as VPNC at the data center.
- Micro branches—For micro branches, you can deploy an Instant AP cluster at the branch site, with Aruba Gateway as the VPNC at the data center.

See Supported SD-Branch Components for information on Aruba Gateways that can be deployed as VPNCs.

Figure 167 shows a typical deployment topology of an SD-Branch with Branch Gateways and a micro branch with Instant APs:

Figure 167 *SD Branch Topology*

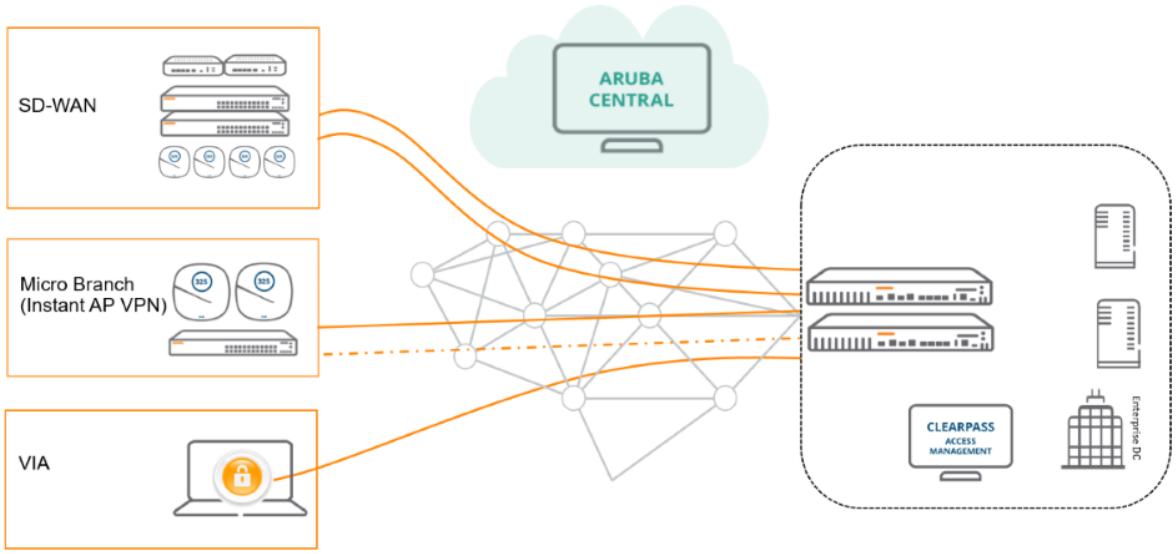


Figure 168 illustrates the communication flow between Aruba Central, branch sites, and data center.

Figure 168 *Aruba Central and Cloud Communication*

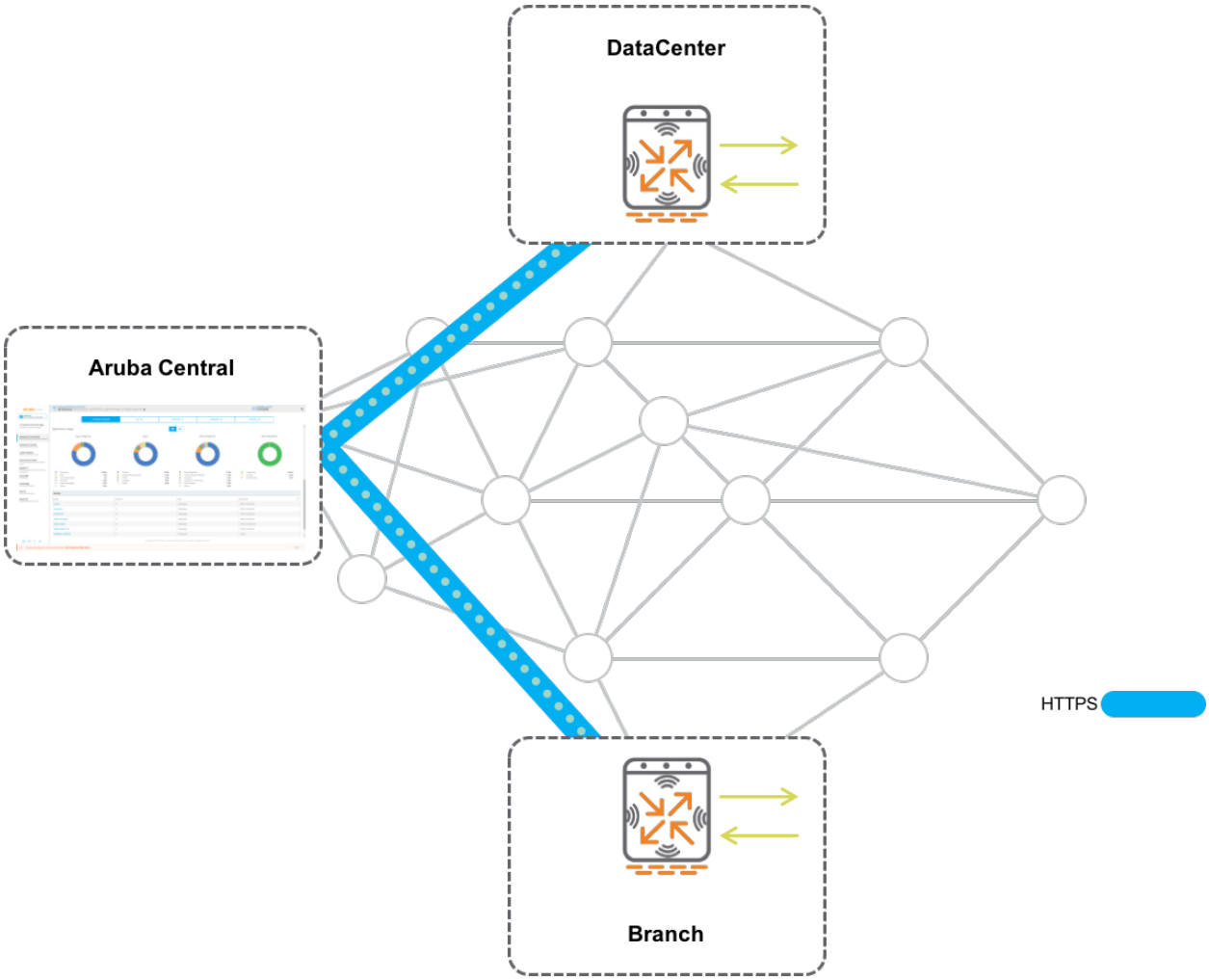
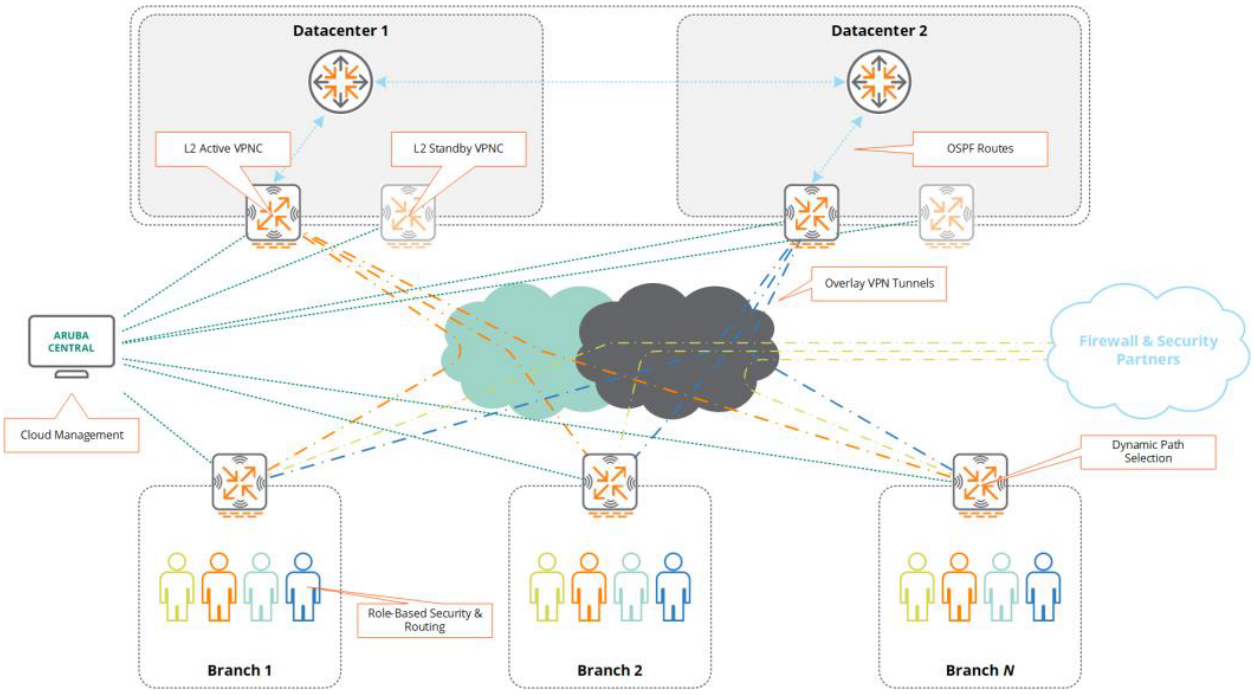


Figure 169 shows all elements in an SD-Branch and the SD-WAN data flow.

Figure 169 *Aruba SD-WAN Data Flow*



What are the Solution Requirements?

The Aruba Gateways are the most important components of the Aruba SD-Branch Solution. The SD-WAN Gateway portfolio includes Aruba Branch Gateways an d VPNCs.

At the Branch Site

The following are the components in a branch:

- **Branch Gateways**—Function at the branch to optimize and control WAN, LAN, and cloud security services.
- **Switches**—Function with Branch Gateways to detect and isolate rogue APs, and denylist rogue devices.
- **Instant APs**—Function as VPN clients at branch sites. The client data traffic from these APs are aggregated by the VPNC located at the data center

At the Data Center

At the data center, you can deploy Aruba Gateways as VPNC. For data center redundancy, you can deploy two VPNCs in the active-standby or active-active mode.

The following are the components operational at the Data Center:

- **VPNC**—A VPNC functions as a VPN management system that aggregates data traffic from the branches and terminates IPsec VPN tunnels.
- **Virtual Gateway**—The headend gateway at the enterprise data center can be hosted as a virtual appliance. The virtualised instance enterprise data center gateway in public or private cloud is referred to as Virtual Gateway. Aruba Virtual Gateways function as VPNCs.

NOTE

For a list of supported Gateways, Switches, and APs, see Supported SD-Branch Components.

In the Cloud

A valid Aruba Central subscription is required to avail cloud-based administration, management, configuration, and monitoring of SD branch components such as Branch Gateways, VPNCs, Instant APs, and Aruba Switches.

Supported SD-Branch Components

The Aruba SD-WAN Gateway portfolio includes Aruba Gateways that function as Branch Gateways and VPNCs.

The following table lists the Aruba Gateway platforms and ArubaOS software versions that function as Branch Gateways:

Table 229: *Supported Aruba Gateways*

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 9004-LTE	ArubaOS 8.5.0.0-2.1.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.1.0.0
Aruba 9012	ArubaOS 8.5.0.0-2.0.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.0.0.4
Aruba 9004	ArubaOS 8.5.0.0-1.0.7.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.0.0.4
Aruba 7210, 7220, and 7240XM	ArubaOS 8.5.0.0-2.0.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.5.0.0-2.0.0.4
Aruba 7030	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7024	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7010	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7008	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7005	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4

The following table lists the Aruba Gateway platforms and ArubaOS software versions that function as VPNCs:

Table 230: *Supported Aruba VPNCs*

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 9004	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0

Table 230: *Supported Aruba VPNCs*

Platform	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 9012	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0
Aruba 7280	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7240XM	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7220	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7210	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
vGW-4G	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
vGW-2G	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
vGW-500M	ArubaOS 8.4.0.0-1.0.6.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7030	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7024	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4
Aruba 7010	ArubaOS 8.1.0.0-1.0.4.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.4.0.0-2.0.0.4

Aruba Virtual Gateways also function as VPNCs. The minimum supported software version for Virtual Gateways is ArubaOS 8.1.0.0-1.0.4.1.

Aruba 9012 Gateway supports traffic inspection while deployed as a VPNC.

Data sheets and technical specifications for the supported Gateways are available at:
https://www.arubanetworks.com/products/networking/gateways-and-controllers/

Supported 4G Modems for Aruba SD-Branch

The following table lists the 4G modems that are supported on the Aruba Branch Gateways:

Table 231: *Supported 4G Modems for Aruba SD-Branch*

USB 4G Modem Model	Carrier Support
Inseego Skyus SC4V	Verizon

USB 4G Modem Model	Carrier Support
Inseego Skyus SC4A	AT&T
Digisol DG-BA4305	ROW
ZTE MF861	AT&T
Franklin Wireless U772	Sprint
Huawei E3372h-320	ROW
Huawei E3372s-153/ E3372h-153	ROW
Huawei E3372h-607	ROW
Huawei E8372h-153	ROW
Huawei E8372h-608	ROW
Huawei E8372h-511	T-Mobile
Huawei E8372h-517	T-Mobile
Huawei E3276-500	ROW
Huawei K5160	ROW
ZTE MF79S	ROW
ZTE MF825C	ROW
ZTE MF831	ROW
ZTE MF832S	ROW
ZTE MF832U	ROW
ZTE MF823	ROW
Huawei E3276-150	ROW
Novatel (Inseego) U620L	Verizon

ROW (Rest of the World) indicates that the modem can be used outside of the United States region. However, the list of supported carriers and supported countries for the modem may vary. To select a modem for a specific country and carrier, refer to the modem documentation.

SD-Branch Enhancements

The following features and enhancements are now available for SD-Branch support in Aruba Central:

- New Capabilities
- Routing Enhancements

New Capabilities

The following features are introduced in this SD-Branch release.

Branch Mesh Topology for Aruba SD-Branch

Branch Mesh Topology Configuration

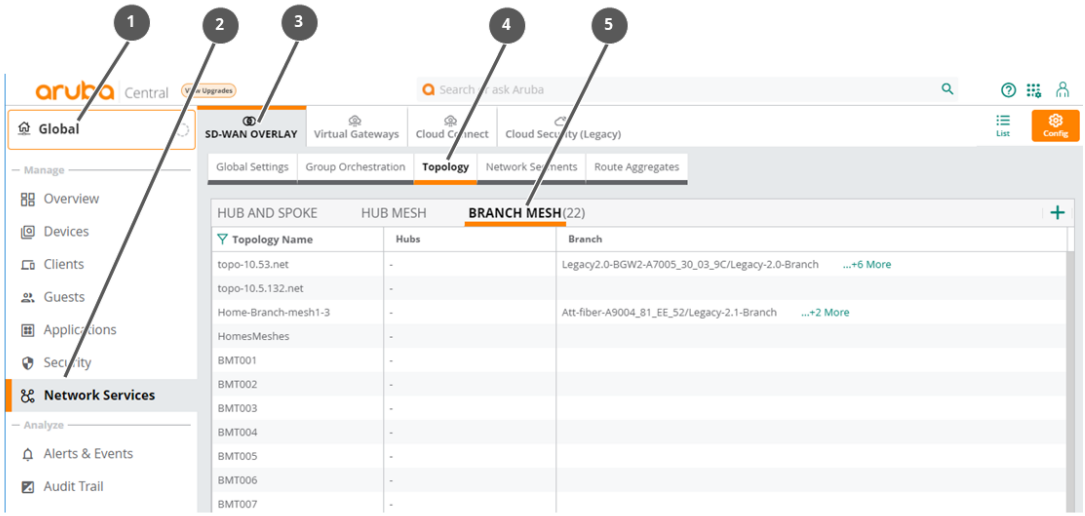
Branch mesh topology configuration is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

This release introduces the Aruba SD-Branch branch mesh topology configuration, which allows Branch Gateways to establish secure overlay tunnels with other Branch Gateways those are part of a same group or different group. When a branch mesh topology is configured between two or more Branch Gateways, a branch mesh link is established to securely transport traffic between the Branch Gateways. The branch mesh link is a point-to-point link that allows traffic to flow from one Branch Gateway to another based on the subnets advertised by the destination Branch Gateway to the cloud orchestrator. Note that a destination Branch Gateway in a branch mesh topology never acts as a transit gateway.

It is not necessary for Branch Gateways to be part of a same group to form a branch mesh tunnel. The Branch Gateways can be part of a same group or different group, and each Branch Gateway establishes point-to-point secure tunnels with the other Branch Gateways which are part of the same branch mesh topology.

To configure a branch mesh topology, in the global dashboard, navigate to **Manage** > **Network Services** > **SD-WAN Overlay**. Click the **Config** icon and then navigate to **Topology** > **Branch Mesh**. The path is displayed in the following figure.

Figure 170 *Configuring a Branch Mesh Topology*



aruba
a Hewlett Packard Enterprise company

1

The following are the important guidelines for configuring a branch mesh topology:

- Every branch group must be connected to a hub or data center (DC).
- You can configure up to 64 Branch Gateways in a branch mesh topology.
- You can configure up to 256 branch mesh topologies.
- The Branch Gateways can belong to different groups.
- The Branch Gateways can be part of more than one branch mesh topology.

For more information, see Branch Mesh Topology in SD-Branch

Branch Mesh Topology Monitoring

Aruba Central provides a separate dashboard to monitor the status of tunnels and routes. In the global dashboard, navigate to **Manage** > **Network Services** > **SD-WAN Overlay**, and click the **Summary** or **List** icon to monitor overlay tunnels and routes. Both graphical and tabular views are available.

Enhancements and changes are introduced in the **SD-WAN Overlay** monitoring pages include support for branch mesh topology. In addition, some changes are also introduced for hub mesh topology.

Hub Mesh Monitoring

The following is the list of changes for this release:

- The **Overlay Tunnel Orchestrator Summary** and **Overlay Route Orchestrator Summary** is removed from the **Tunnel** and **Route** tabs.
- Only VPNC groups support hub mesh topology. The VPNC groups tab is added to the map views of **Tunnel** and **Route** tabs.

Branch Mesh Monitoring

The following is the list of changes for this release:

- Only Branch groups support branch mesh topology.
- The **Branch groups** tab is added to the map views of **Tunnel** and **Route** pages.

Map View Updates for Branch Group

The following is the list of changes for this release, the updates are common to both the **Tunnel** and **Route** tabs:

- The map view for a Branch Group allows to:
- Choose the required site or host from the selected Branch group using the search box
- View the tunnel links on the map
- The **Unallocated sites** collapsible pane enables you to view the unallocated sites and navigate to the device details by clicking the number or name of the site.
- The **Status filter** enables you to view only the pins based on the status of the site. You can display the site name for the pins by selecting the **Name** option.

For more information, see Overlay Tunnel Orchestrator in Map View and Overlay Route Orchestrator in Map View.

Forward Error Correction for SD-Branch Traffic Policies

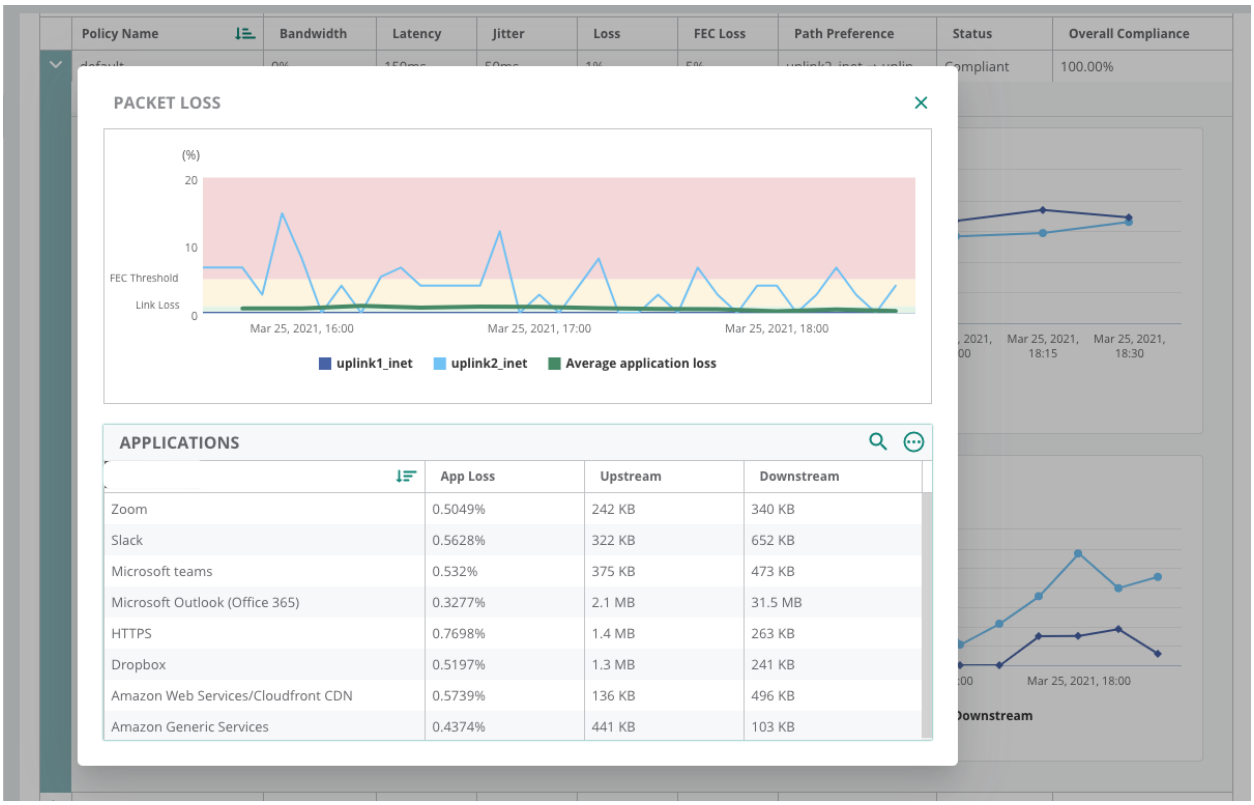
This release introduces the Forward Error Correction (FEC) technology, with the ability to compensate any packet loss during traffic flow. This is achieved by inserting intermittent error recovery or redundant packets in the traffic flow. These redundant packets compensate for the lost packets when the link loss quality goes below the configured SLA limit. The uplink works until the packet loss reaches the FEC threshold beyond which the uplink is non-complaint. This feature is very useful for business-critical applications, since it improves the application's performance across the WAN. This feature is configured as part of the Dynamic Path Steering (DPS) policy. The DPS policy provides WAN performance enhancements, with real-time traffic steering over broadband and MPLS links based on user-defined DPS policies. This feature complements DPS by overcoming the effects of dropped and out-of-order packets on the Internet connections.

As part of this enhancement, a new color coding in purple is introduced in the graph, which indicates that the uplink is compliant and it is FEC protected. The color code is displayed when you hover over the **Compliance Summary** chart in the **Path Steering** monitoring page. The new **Application Performance** tab displays three separate charts to view the performance of the application for QoE, Packet Loss, and Latency. You can further expand the **Packet Loss** chart to drill-down on the details.

The following figure displays an example for the FEC threshold.

For more information, see Gateway > WAN > Path Steering and Configuring Policies for Dynamic Path Steering.

Figure 171 *FEC Threshold*



Tunnel Bandwidth Negotiation

From this release onwards, you can enable bandwidth contract per tunnel on both Branch Gateways and VPN Concentrators to provide equal bandwidth to all branches connected to a head-end.

To ensure that a VPNC is not overloaded with traffic from all the Branch Gateways connected to it, and to allow all branches to have a fair acces to the datacenter, ensure that the amount of traffic transmitted from a Branch Gateway or VPNC is configured with a maximum bandwidth threshold.

You can configure the maximum bandwidth threshold using the new **Tunnel max bandwidth threshold** field to specify the maximum transmit rate in percentage. For more information, see Configuring Uplinks.

Routing Enhancements

Policy Based Routing

From this release onwards, when using IP Next-Hop lists, Aruba SD-Branch gateways allow configuring two options for tracking. When configured with an IP address or a DHCP default-gateway, gateways can either track the immediate next-hop or the IP/FQDN of the remote host defined as WAN Health Check. For more information, see Configuring Policies for PBR.

BGP Routing

The following are the BGP routing enhancements introduced for this release:

- This release introduces a new option for **Route map** configuration. Now, you have one more option called **Community list** added to the **Option** drop-down list. You can choose to **Append** or **Delete** this to the community attribute and define the rule. For more information, see Configuring Route Maps.
- Now, you can enable distribution of default information to the BGP neighbors. A default route is used to forward packets to networks that are not present in the local IP routing table.
- A check box to enable **Default Information** and a drop-down to select the **Route Map** are introduced to configure default route for BGP. For more information, see Enabling BGP.

IAP-VPN Overlay Route Redistribution for OSPF Routing

Route redistribution enables routes learned from one routing protocol, to be advertised to another routing protocol. Route redistribution is very useful for multi-protocol networks. In the Aruba SD-Branch solution, if your corporate network is running on OSPF and you have multiple remote and home offices on IAP-VPN (called Micro Branches), you have the option to use route redistribution between the Micro Branch and the corporate office networks.

You can enable route redistribution from IAP-VPN overlay networks to OSPF networks by accessing the gateway configuration page for either a VPNC or a Branch Gateway.

To know more about configuring the related options for route redistribution and configuring OSPF routing, see Routes Advertisement Using OSPF.

BGP Aggregate Routes

From this release onwards, Aruba SD-Branch gateways advertise an aggregate route only when any of the summarized routes are present in the BGP routing table. For more information, see Advertising Networks to BGP.

Redistributing Route to Null

From this release onwards, Aruba SD-Branch gateways are capable of redistributing a route to null into other protocols such as BGP or the SD-WAN Overlay (OAP). For more information, see Configuring Redistribution Rules for BGP Routes and Advertising Overlay Routes.

Route Filtering

From this release onwards, Aruba SD-Branch gateways can apply route filters with attributes, to the connected routes that are aggregated, when redistributing to the SD-WAN Overlay. The route map applied to redistribution is also applied to aggregated and non-aggregated routes. For more information, see Advertising Overlay Routes.

Users and Roles Enhancements

Role-Based Access Control

The following are the Role-Based Access Control (RBAC) enhancements for this release:

- **Privileged Configuration Option for Network Operations Role**

  For creating or modifying a role for the **Network Operations** app, a new Network Management module is available for a configuration called **Privileged Configuration**. The **Privileged Configuration** option controls access to the **Device(s) > Gateway(s) > System > Admin** tab for

both the gateway group dashboard and the gateway device dashboard. You can create a role to set the access to **View Only, Modify**, or **Block**.

To access the option, perform the following steps:

1. Navigate to **Account Home > Global Settings > Users and Roles > Add Role**.
2. On the **New Role** page, select **Network Operations**.
3. Scroll to **Network Management**.
4. Click **Customize** to see the available modules under **Network Management**.

   The **Privileged Configuration** option is listed here.

   The available permissions for the **Privileged Configuration** option are **View Only**, **Modify,** and **Block**.

- **Roles to Access Users, Roles, and SSO Details for Account Home**

  You can create a role for the **Account Home** page that controls access to the user details, role details, and SSO details available under **Global Settings**. The available permissions are **View Only, Modify,** and **Block**.

  The new roles available include the following:

  - **Users**—Defines a role for accessing the user details in the **Account Home > Global Settings > Users and Roles > Users** page.
  - **Roles**—Defines a role for accessing the role details in the **Account Home > Global Settings > Users and Roles > Roles** page.
  - **SSO**—Defines a role for accessing the Single Sign-On profiles details in the **Account Home > Single Sign On** page.

  To create the role, perform the following steps:

  1. Navigate to **Account Home > Global Settings > Users and Roles > Add Role**.
  2. In the **New Role** page, select **Account Home**.

     The Users, Roles, and SSO options are listed in this page.

Configuration Enhancements

SaaS Express

This release introduces the following enhancements.

SaaS Express offers several new monitoring options for predefined and custom SaaS applications. These options must first be configured.

- **Monitor and Optimize options**—This release introduces a new field called **Mode** to allow users to choose between **Monitor** and **Optimize**. Selecting **Monitor** gathers the uplink performance statistics and displays it in the monitoring dashboard, whereas selecting **Optimize** not only monitors but also optimizes the performance of the SaaS applications. This feature applies to the predefined SaaS applications. The probing frequency for **Monitor** mode is two probes for every 60 seconds, and for **Optimize** mode, it is two probes for every 10 seconds.
  To configure the feature, in the **Network Operations** app, select the Branch Gateway group dashboard, and navigate to **Devices** > **Gateways** > **WAN** > **SaaS Express**.
- **Active Monitoring option**—This release introduces a new column called **Active Monitoring**. Selecting this check box allows the users to only monitor the performance of the SaaS application. Users can view

the performance scores in the monitoring dashboards.
This feature applies to the custom SaaS applications. To configure the feature, in the **Network Operations** app, select the **Global** dashboard, and navigate to **Manage** > **Applications** > **Config icon**.

For more information about how to configure the new monitoring options, see SaaS Application Traffic Management with SaaS Express.

Simplified Configuration

The following enhancements are introduced in the Guided Setup and Basic mode pages:

Configuring SaaS Express using Guided Setup

This release introduces support to configure SaaS Express using the Guided Setup. In the Guided Setup configuration page for a Branch Gateway group, go to **Policies** > **DPS** to configure SaaS policies.

To define custom policies, go to **Global** > **Applications** > **SaaS Express** > **Config** icon.

For more information about how to configure the new monitoring options, see Configuring Policies for a Branch Gateway Group.

Configuring DHCP IP Reservation Using Guided Setup or in Basic Mode

This release introduces support for reserving IP addresses in the DHCP pool to assign the same IP address to a client whenever it requests for a network connection. This feature which is already available in the Advanced mode can now be configured using the Guided Setup or Basic mode. For more information, see Configuring DHCP for LAN Interfaces.

Configuring PBR Policies in Basic Mode

Now, you can configure Policy Based Routing (PBR) policies to allow full-tunnel traffic to the data center or to a cloud service provider for further inspection. For more information, see Configuring Policy-Based Routing (PBR) Policy.

SD-WAN Overlay Configuration

This release introduces the following new tabs under the SD-WAN Overlay tab:

- Global Settings—Allows you to configure the overlay AS number, timers, dynamic data center path computation, and dynamic backup route advertisement (DBRA).
- Group Orchestration—Allows you to enable group orchestration of gateways.
- Topology—Allows you to configure the hub and spoke, hub mesh, and branch mesh topologies.
- Network Segments—Allows you to add a new network segment.
- Route Aggregates—Allows you to aggregate routes for branches or VPNCs in data centers.

For more information, see Configuring Overlay Network Using SD-WAN Orchestrator.

Support for SHA2-256 Authentication for Gateway Tunnels

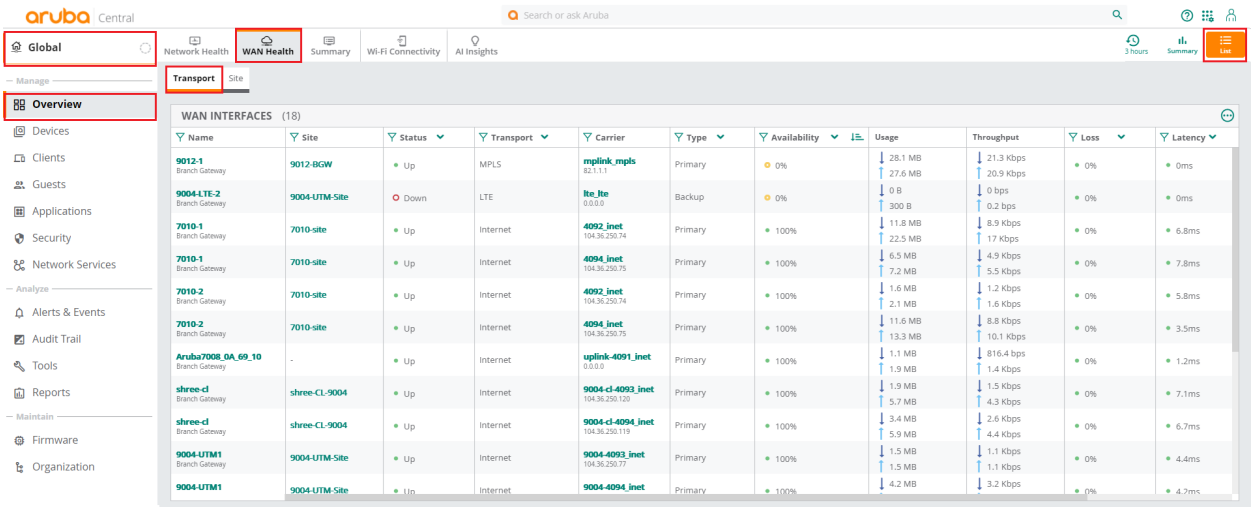
The **Overlay Tunnel Orchestration** service is enhanced to support the SHA2-256 authentication method. This service creates **IPsec** tunnels with the SHA2-256 authentication method when both the tunnel endpoints are running SD-Branch 2.3.0.0 or a later version.

Monitoring Enhancements

WAN Health Dashboard for Gateways

This release introduces the WAN Health—Transport dashboard to display the network health of all the uplinks belonging to an end-user. This dashboard monitors network health of all uplinks based on active monitoring probes, and helps in accessing information of all uplinks in one place to troubleshoot network issues.

For more information, see WAN Health—Transport.



QoS Parameters for Gateway > Overview > Sessions Page

The **Gateway > Overview > Sessions** page for the gateway dashboard now displays the **DSCP** value and the **Priority** value for each application listed under the **Sessions** section.

SaaS Express

This release introduces the following enhancements.

The following new parameters are introduced for the SaaS Express monitoring dashboard.

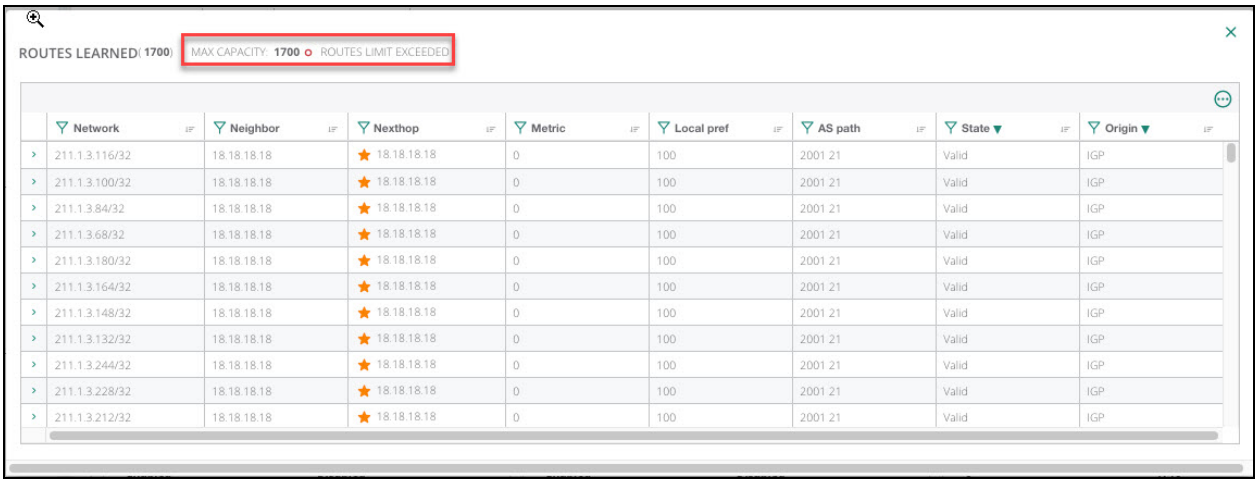
- **Filtering Applications**—In the **Global** dashboard, under **Manage** > **Applications** > **SaaS Express**, you can now filter the applications which you need to monitor. If you do not select any application, the SaaS Express page displays data for all the configured SaaS applications.
- **QoE and MOS Parameters**—In the **Gateway** dashboard, under **Manage** > **Applications** > **SaaS Express**, two new columns are introduced, namely, **Observed LAN QOE** and **Observed WAN QOE**. A new parameter called the **Mean Opinion Score (MOS)** is also introduced in the graph of an application category.

For more information about the application filtering and the new monitoring parameters, see Monitoring SaaS Express .

BGP Routing

The following are the BGP routing enhancements introduced for this release:

This release introduces a small red circle in the BGP monitoring page to indicate that the number of routes received by the BGP neighbor has exceeded the configured limit.



For more information, see Adding BGP Neighbors.

Gateway Firewall Logging

This release introduces the following enhancements to the **Security > Firewall** tab:

- For both the **Global** and **Gateway** dashboards, in the list view and chart view, the time range for historical firewall activity is now, **3 hours**, **1 day**, and **1 week** .
- For the **Gateway** dashboard, in the list view, the **Blocked Sessions** tab now includes a histogram that allows you to select and view the sessions data for a selected time range. This time range can be selected for a minimum of 15 minutes and maximum of 6 hours. Based on the time range selection, the histogram in the list view displays the blocked session data in the following time interval:
  - 3 hours—15 minutes time interval
  - 1 day—1 hours time interval
  - 1 week—6 hours time interval
- For the **Gateway** dashboard, the **Blocked** sessions table now includes the **Blocked reason** column that displays the cause of the blocked session.

Additional Gateway Monitoring Enhancements

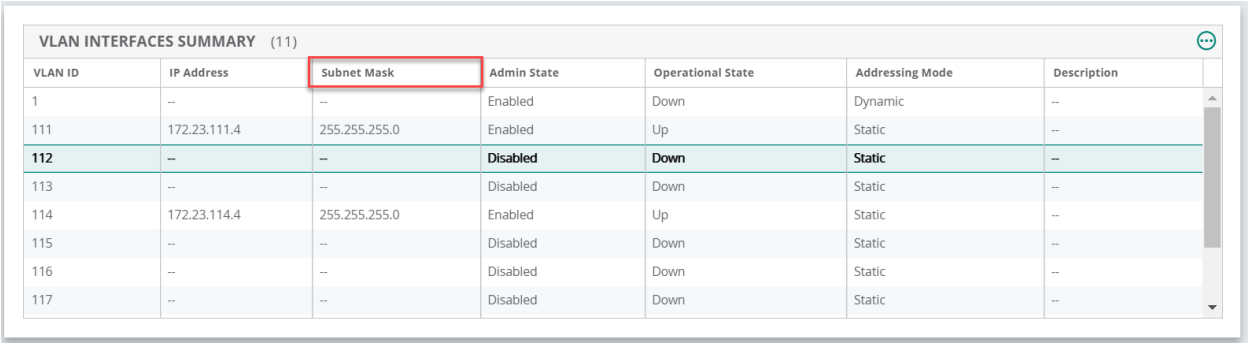
This release introduces the following enhancements for gateway monitoring.

Application Visibility for the WAN Network

The **Summary** page for the gateway dashboard is now enhanced for application visibility related to the WAN network. The **Summary** page displays in-depth details about the usage of different applications per uplink. You can now see the WAN usage for the top 10 applications under the **Usage** section. For more information, see the WAN Interfaces section in the Gateway > WAN > Summary page.

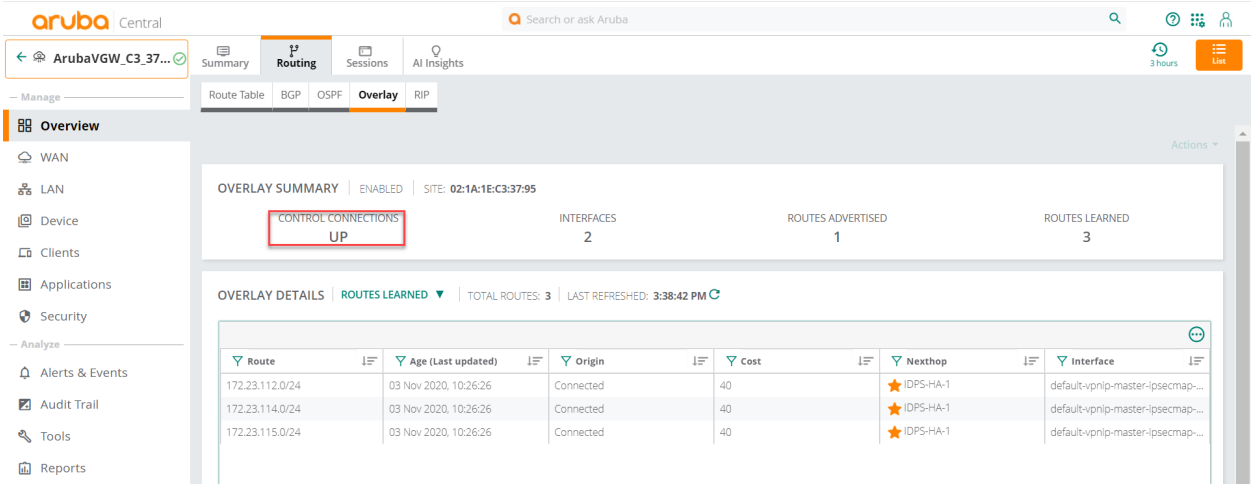
VLAN Subnet Masks for Gateway > LAN > Summary Page

The **Gateway > LAN > Summary** page for the gateway dashboard now displays the subnet mask along with the IP address for the VLANs displayed in the **VLAN Interfaces Summary** table. For more information on the **Summary** page for LAN connections, see the Gateway > LAN > Summary page.



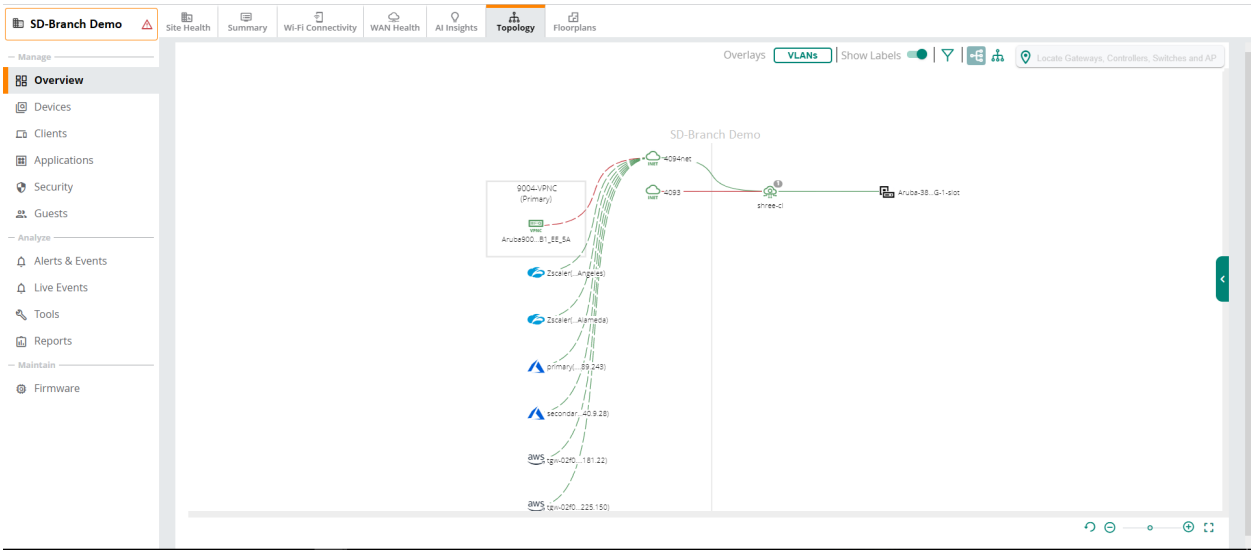
Control Connections Display in Gateway > Overview > Routing > Overlay Page

The **Control Connections** status is now displayed as either **Up** or **Down** in the **Overlay Summary** section of the **Gateway > Overview > Routing > Overlay** page. To know more about the **Overlay** network details, see Gateway > Overview > Routing > Overlay.



AWS VPCs and Azure VPN Gateways in Topology Tab User Interface

The **Overview > Topology** page for a site now displays the AWS VPCs and Microsoft Azure VPN Gateways integrated to SD-Branch through Cloud Connect service. For more information, see Monitoring Sites in the Topology Tab.



Device Enhancements

Changes in Aruba SD-Branch Gateways

The following are the device enhancements in this release:

- Aruba SD-Branch gateways starting from version 8.7.0.0-2.3.0.0, no longer require additional reboot when they receive the controller IP from Aruba Central after the ZTP process. Some services are restarted, resulting in an expected network impact, but the gateways do not reload for the second time. However, the gateways will reboot if there are any subsequent controller IP changes. For more information, see Connecting Aruba Gateways to Aruba Central.
- Aruba SD-Branch gateways with proxy-ARP enabled can now be configured to either respond to ARP requests with their own MAC or the MAC address of any client in the user table. For more information, see Configuring Other Parameters for VLAN.
- Aruba introduces support for 9012 and 9004 gateways to be deployed as VPN Concentrators. For more information, see Supported SD-Branch Components.
- When IDS/IPS is disabled for Aruba 90xx series gateways, the maximum session limit is increased from 64k to 128k sessions.

Security Enhancements

Configuring IDPS in Fail-Open and Fail-Close Modes

From this release onwards, Aruba Central allows configuring the **Gateway IDS/IPS** in SD-Branch gateways, in fail-open mode and in fail-close mode.

New Gateway IDS/IPS Alerts

The following new Aruba Gateway IDS/IPS alerts are introduced in the **Alerts & Events** page:

- **Gateway Threat Count**— Generates an alert when the number of threats exceeds the configured limit in the given duration.
- **Gateway Threat Count Per Signature**— Generates an alert when the number of threats associated with a specific signature exceeds the configured limit in the given duration.

For more information, see Gateway Alerts.

Aruba 9004 - LTE Gateway

The following are the enhancements for the Aruba 9004-LTE gateway:

- This release introduces a new network mode to enable selection of a custom 3G or 4G frequency band. For more information see, Managing 9004-LTE Branch Gateway.
- The following new event types are introduced in the **Events** table in the **Alerts & Events** page:
  - **Cellular Mode Change**—An event is generated when the network mode changes.
  - **Cellular Data Usage**—An event is generated at 75% of configured usage.
  - **Cellular Connectivity**—An event is generated when the WAN uplink interface is disconnected.
- This release introduces a new column in the **Device Inventory** page to display the **IMEI** number of 9004-LTE gateway.

Aruba Virtual Gateway Enhancements

Support for Virtual Gateway in Google Cloud Platform

You can now use the Google Cloud Platform to deploy an Aruba Virtual Gateway in unmanaged mode. In the unmanaged mode, IT administrators bring up and configure the Virtual Gateway instance and monitor the deployed Virtual Gateway from Aruba Central. The Aruba Virtual Gateway requires the use of a supported Google Cloud instance with a minimum of 500 Mbps of throughput and the instance can support up to 1600 IPsec tunnels.

For more information on deploying a Virtual Gateway in Google Cloud Platform, see Deploying Aruba Virtual Gateways in Google Cloud Platform (Unmanaged Mode).

Support for Virtual Gateway in MSP Mode

You can now deploy an Aruba Virtual Gateway in unmanaged mode in the MSP mode of Aruba Central. The MSP mode of Aruba Central enables a service provider to maintain and monitor different Aruba Central accounts belonging to different customers.

For more information on deploying a Virtual Gateway in MSP mode, see Deploying Aruba Virtual Gateways in MSP (Unmanaged Mode).

Orchestrated and Manual tabs for Virtual Gateways

This release now introduces the following summary tabs for Virtual Gateways:

- Orchestrated—lists the automatically orchestrated managed devices.
  To view the Orchestrated tab, in the **Network Operations** app, select the **Global** dashboard, and navigate to **Network Services** > **Virtual Gateways** > **Orchestrated**. For more information, see Creating a Cloud Provider Account in Aruba Central.
- Manual—lists the manually orchestrated unmanaged devices.
  To view the **Manual** tab, in the **Network Operations** app, select the **Global** dashboard, and navigate to **Network Services** > **Virtual Gateways** > **Manual**. For more information, see Verifying the Deployment Status

Cloud Connect Enhancements

SD-Branch Integration with Microsoft Azure Through Cloud Connect Service

This release introduces the SD-Branch integration with Microsoft Azure through the Cloud Connect service. As a result of which, you can set up a secure connection between the Aruba Virtual Gateways and the Microsoft Azure VPN Gateways.

The Cloud Connect service uses SD-WAN Orchestrator as the transport medium to send configurations to Aruba Virtual Gateways and establish direct communication with the Microsoft Azure VPN Gateways.

To integrate SD-Branch with Microsoft Azure through the Cloud Connect service:

1. Configure Microsoft VPN Gateway in Azure Admin Portal.
2. Onboard a Cloud Provider Account in Aruba Central.
3. Discover a Microsoft Azure VPN Gateway in Azure Admin Portal.

4. Orchestrate tunnels to connect Microsoft Azure VPN Gateway with Aruba SD-Branch Group.
5. Verify and monitor the Microsoft Azure VPN Gateway in the SD-WAN Site topology.

For more information on how to integrate SD-Branch with Microsoft Azure through the Cloud Connect service, see Aruba SD-WAN Integration with Microsoft Azure Public Cloud Tech Note and Integration with Microsoft Azure Public Cloud through Cloud Connect Service.

SD-Branch Integration with AWS Through Cloud Connect Service

This release introduces the SD-Branch integration with AWS through the Cloud Connect service. As a result of which, you can set up a secure connection between the Aruba Virtual Gateways and the AWS Virtual Private Cloud (VPC) environments.

The Cloud Connect service uses SD-WAN Orchestrator as the transport medium to send configurations to Aruba Virtual Gateways and establish direct communication with the AWS VPN Concentrators.

To integrate SD-Branch with AWS through the Cloud Connect service:

1. Generate API token in AWS Console.
2. Onboard AWS accounts into Aruba Central through Cloud Connect service.
3. Orchestrate tunnel to the AWS VPC through Cloud Connect.
4. Verify tunnel status.

For more information on the steps to integrate SD-Branch with AWS through the Cloud Connect service, see Aruba SD-WAN Integration with AWS Public Cloud Tech Note and Integration with AWS Public Cloud through Cloud Connect Service.

Troubleshooting Enhancements

Tools

In the **Network Operations** app, use the filter to select a group, label, site, or a device and then, select **Analyze** > **Tools** to use different troubleshooting tools. The **Tools** menu option enables users to troubleshoot AP, gateway, and switch issues in the network through various tests available in the **Network Check**, **Device Check**, and **Commands** tabs. Listed below are the troubleshooting tools enhancements, In this release:

- **New Gateway Connectivity Tests**—Apart from **Ping Test** and **Traceroute**, users can now diagnose gateway network issues with the following tests:
  - **Ping Sweep Test**—Performs an advanced check on the host reachability and network connectivity.
  - **HTTP Test**—Sends packets to the HTTP URL and tries to establish a connection and exchange data.
  - **HTTPS Test**—Sends packets to the HTTPS URL and tries to establish a connection and exchange data.
  - **Speed Test (iPerf)**—Performs a speed test to measure the network speed and bandwidth. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.
- **Additional Tests Parameters**—In the **Network Check** tab, additional parameters are introduced in the **Show Additional Test Settings** section to enhance the troubleshooting procedure for the following tests:

- **Ping Test**—Sends ICMP echo packets to the hostname or IP address of the selected devices to check for latency issues.
- **HTTP Test**—Sends packets to the HTTP URL and tries to establish a connection and exchange data.
- **HTTPS Test**—Sends packets to the HTTPS URL and tries to establish a connection and exchange data.
- **TCP Test**—Sends packets to the host, for example, FTP server, and tries to establish a connection and exchange data.
- **Speed Test (iPerf)**—Performs a speed test to measure the network speed and bandwidth. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

The **Show Additional Test Settings** is not displayed when a **Test** type is not selected. You can now show or hide the **Show Additional Test Settings** section.

- **Device check**—This test is now available for gateways, and you can perform interface bounce and PoE bounce to check the PoE issues for the gateways available in the network.

To start using the SD-WAN solution, ensure that you have a valid Aruba Central subscription and licenses for the SD-Branch devices.

- If you are an existing Aruba Central customer with a valid subscription key and device licenses, access the Aruba Central UI and complete the provisioning tasks.
- If you are an existing Aruba customer with valid device licenses, but not an Aruba Central customer, sign up for Aruba Central. After a successful registration, Aruba sends a verification e-mail with a link to the Aruba Central portal. For more information, see *Aruba Central Help Center*.

Aruba Central offers a 90 day evaluation subscription for customers who want to try the Aruba cloud solution for managing their networks. When you sign up for Aruba Central, an evaluation subscription is automatically assigned, unless you purchased a subscription. To purchase subscriptions, contact the Aruba support team.

Gateway Provisioning Tasks

Complete the following provisioning tasks to bring up your devices in the Aruba Central management interface:

- Onboard Devices
- Assign Subscriptions
- Assign Devices to Sites
- Assign Labels
- Assign Groups
- Assigning a Group Role or Persona
- Provision Gateways
- Open Firewall Ports for Device Communication

Creating an Aruba Central Account

To start using Aruba Central, you need to register and create an Aruba Central account. Both evaluating and paid subscribers require an account to start using Aruba Central.

Zones and Sign-Up URLs

Aruba Central instances are available on multiple regional clusters. These regional clusters are referred to as zones. When you register for an Aruba Central account, Aruba creates an account for you in the zone that is mapped to the country you selected during registration.

To create an Aruba Central account in the zone that is mapped to your country, use the following zone-specific sign-up URLs.

Table 232: *Sign-Up URLs & Apps*

Regional Cluster	Sign-Up URL	Available Apps
US-1	https://portal.central.arubanetworks.com/signup	**Network Operations**
US-2	https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/	▪ **Network Operations** ▪ **ClearPass Device Insight**
Canada-1	https://portal-ca.central.arubanetworks.com/signup	**Network Operations**
China-1	https://portal.central.arubanetworks.com.cn/signup	**Network Operations**
EU-1	https://portal-eu.central.arubanetworks.com/signup	▪ **Network Operations** ▪ **ClearPass Device Insight**
APAC-1	https://portal-apac.central.arubanetworks.com/signup	**Network Operations**
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/signup	**Network Operations**
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com/signup	**Network Operations**

Signing up for an Aruba Central Account

You can choose one of the following ways to start your Aruba Central account trail:

1. Open the following page in a supported browser window:http://www.arubanetworks.com/products/sme/eval/.
   a. Click **Start the Central Demo**. The Aruba Central Demo page is displayed.
   b. Fill the form to start a product demo, and click **Start Demo**.
   c. The Aruba Central Account Home page is displayed.
2. Use the sign-up URL for your region from Sign-Up URLs & Apps and complete the following steps:
   a. Enter your email address. Based on the email address you entered, the **Registration** page guides you to the subsequent steps:

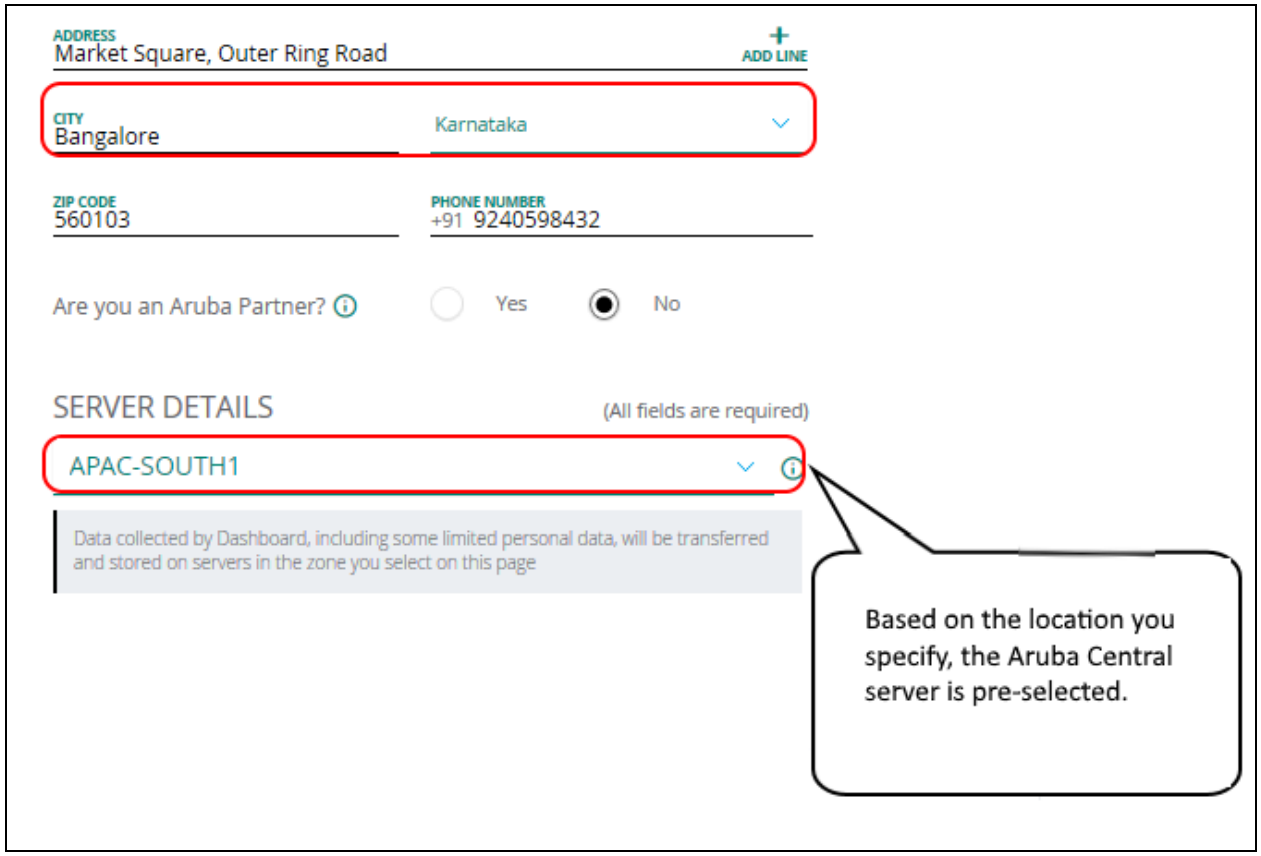
Table 233: *Registration Workflow*

If...	Then...
If you are a new user:	The **Registration** page prompts you to create a password. To continue with the registration, enter a password in the **Password** and **Confirm Password** fields.

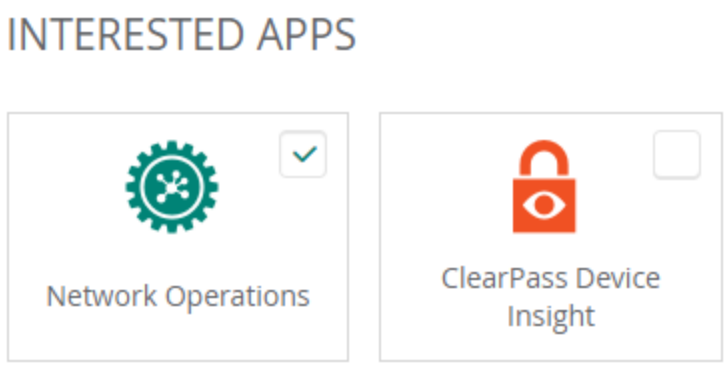
Table 233: *Registration Workflow*

If...	Then...
If you are an existing Aruba customer, but you do not have an Aruba Central account: If your email account is already registered with Aruba, but you do not have an Aruba Central account:	The **Registration** page displays the following message: **Email already exists. Please enter the password below**. To continue with registration, validate your account: 1. Enter the password. 2. Click **Validate Account**. **NOTE:** If you do not remember the password, click **Forgot Password** to reset the password.
If you are invited to join as a user in an existing Aruba Central customer account:	The **Registration** page displays the following message: **An invitation email has already been sent to your email ID. Resend**. To continue with the registration: 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the **Registration** page and click **Resend**. A registration invitation will be sent your account. 3. Click the registration link. The user account is validated. 4. Complete the registration on the **Sign Up** page to sign in to Aruba Central.
If you are a registered user of Aruba Central and have not verified your email yet:	The **Registration** page displays the following message: **You are an existing Aruba Central user. Please verify your account. Resend Verification email**. To continue: 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the **Registration** page and click **Resend Verification email**. A registration invitation will be sent your account. 3. Click the account activation link. 4. After the email verification is completed successfully, click **Log in** to access Aruba Central.
If you are already a registered user of Aruba Central and have verified your email:	The **Registration** page displays the following message: **User has been registered and verified. Sign in to Central**. Click **Sign in to Central** to skip the registration process and access the Aruba Central portal.
If your email address is in the **arubanetworks.com** or **hpe.com** domain:	The **Single Sign-On** option is enabled. You can use your respective Aruba or HP Enterprise credentials to log in to your Aruba Central account after the registration.

b. To continue with registration, enter your first name, last name, company name, address, country, state, ZIP code, and phone details.
c. Specify if you are an Aruba partner.
d. Ensure that you select an appropriate zone. The **Registration** page displays a list of zones in which the Aruba Central servers are available for account creation. Based on the country you select, the Aruba Central server is automatically selected. If you want your account and Aruba Central data to reside on a server from another zone, you can select an Aruba Central server from the list of available servers.



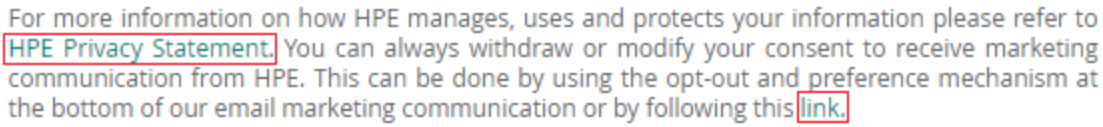
e. From the **Interested Apps** section, select the app(s) that you want to pre-provision. You must select at least one app to continue:
   - **Network Operations**
   - **ClearPass Device Insight**



See Table 232 for the app(s) available in the zone in which you are signing up.

If you are interested in evaluating the Aruba Central MSP solution, select only the **Network Operations** app.

f. Select the **I agree to the Terms and Conditions** check box.
g. Set a preferred mode of communication for receiving notifications about Aruba products and services.
h. Optionally, to read about the privacy statement, click the **HPE Privacy Statement** link. To opt out of marketing communication, you can either click the unsubscribe link available at the bottom of the email or click the link as shown in the following figure:



i. Click **Sign Up**. Your new account is created in the zone you selected and an email invitation is sent to your email address for account activation.
j. Access your email account and click the **Activate Your Account** link. After you verify your email, you can log in to Aruba Central.

Accessing Aruba Central Portal

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central.

If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created.

Login URLs

When you try to access Aruba Central portal, you are redirected to the Aruba Central URL that is mapped to your cluster zone.

Table 234: *Cluster Zone— Portal URLs*

Regional Cluster	Login URL
US-1	https://portal.central.arubanetworks.com/platform/login/user
US-2	https://portal-prod2.central.arubanetworks.com/platform/login/user
Canada-1	https://portal-ca.central.arubanetworks.com/platform/login/user
China-1	https://portal.central.arubanetworks.com.cnath/platform/login/user
EU-1	https://portal-eu.central.arubanetworks.com/platform/login/user
APAC-1	https://portal-apac.central.arubanetworks.com/platform/login/user
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/platform/login/user
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com/platform/login/user

Logging in to Aruba Central

To log in to Aruba Central:

1. Access the Aruba Central login URL for your zone.
2. Notice that the zone is automatically selected based on your geographical location.
3. Enter the email address and click **Continue**.
4. Log in using your credentials.

If your user credentials are stored in your organization's Identity Management server and SAML SSO authentication is enabled for your IdP on Aruba Central, complete the SSO authentication workflow.

5. Enter the password.

If you have forgotten password, you can click the **Forgot Password** and reset your password. The Forgot Password link resets only your Aruba Central account; hence, it is not available to SSO users.

6. Click **Continue**. The **Initial Setup** wizard opens.
   - If you have a paid subscription, click **Get Started** and set up your account.
   - If you are a trial user, click **Evaluate Now** and start your trial.

Changing Your Password

To change your Aruba Central account:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **Change Password**.
3. Enter a new password.
4. Log in to Aruba Central using the new password.

The **Change Password** menu option is not available for federated users who sign in to Aruba Central using their SSO credentials.

Logging Out of Aruba Central

To log out of Aruba Central:

1. In the Aruba Central UI, click the user icon ( ) in the header pane.
2. Click **Logout**.

Managing License Keys

A license key is an alphanumeric string with 9 to 14 characters; for example, PQREWD6ADWERAS. Aruba Central can manage a device only if the corresponding license key of the device is added to Aruba Central. License keys can either be evaluation license keys that map to evaluation licenses or paid license keys that map to paid licenses. The evaluation license key is valid for 90 days.

To use Aruba Central for managing, profiling, analyzing, and monitoring your devices, you must ensure that you have a valid license key and that the license key is listed in the **Account Home** > **Global Settings** > **Key Management** page.

Evaluation License Key

The evaluation license key is enabled for trial users by default. It allows you to add up to a total of 60 devices. For an evaluation user, a set of evaluation keys is generated.

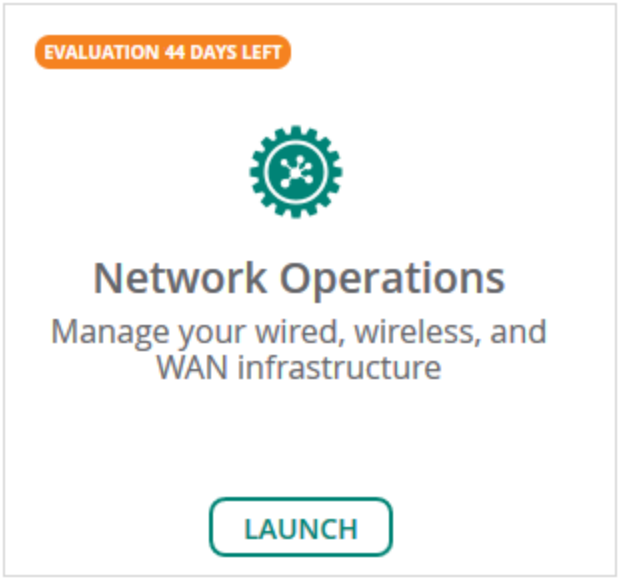
The **Account Home** > **Global Settings** > **Key Management** page displays the license expiration date in the **Key Management** table. You will receive license expiry notifications through email 30, 15, and 1 day before the license expiry and on day 1 after the license actually expires. The number of days left for license expiry is also displayed in the respective app under the **Apps** section of the **Account Home** page.

Upgrading to a Paid Account

If you have purchased a license for an AP, a switch, or a gateway, then upgrade your account by completing the following steps:

1. On the **Account Home** page, in the **Network Operation** app, click the link that shows the number of days left for the evaluation to expire.

   Figure 172 *Network Operations Evaluation Account*

   The **Add a New License** window is displayed.
2. Enter the new license key that you purchased from Aruba.
3. Click **Add License**.

After you upgrade your account, you can add more devices, enable services, and continue using Aruba Central.

Paid License Key

If you have purchased a license key, you must ensure that your license key is added to Aruba Central. If you are logging in for the first time, Aruba Central prompts you to add your license key to activate your account. Ensure that you add the license key before on-boarding devices to Aruba Central.

The **Account Home** > **Global Settings** > **Key Management** page displays the license expiration date. You receive the license expiry notifications through email 90, 60, 30, 15, and 1 day before expiry and two notifications each day on day 1 and day 2 after the license expires.

When you upgrade or renew your license, or purchase another license key, you must add the key details in the **Account Home** > **Global Settings** > **Key Management** page to avail the benefits of the new license.

Adding a License Key

1. On the **Account Home** page, under **Global Settings**, click **Key Management**.

   The **Key Management** page is displayed.
2. Enter your license key.
3. Click **Add Key**.

   The license key is added to Aruba Central and the contents of the license key are displayed in the **Manage Keys** table. Review the license details.

   If you add a **Device Management** token, the key is listed in the **Convert Deprecated Licenses** page. For more information, see Converting Legacy Tokens to New Licenses.

Viewing License Key Details

To view the license key details, navigate to **Account Home** > **Global Settings** > **Key Management**.

The **Key Management** page provides information about license keys available for the devices and their details such as license tier, expiration date, and quantity of licenses. The **Key Management** sections are described in the next topics.

License Summary

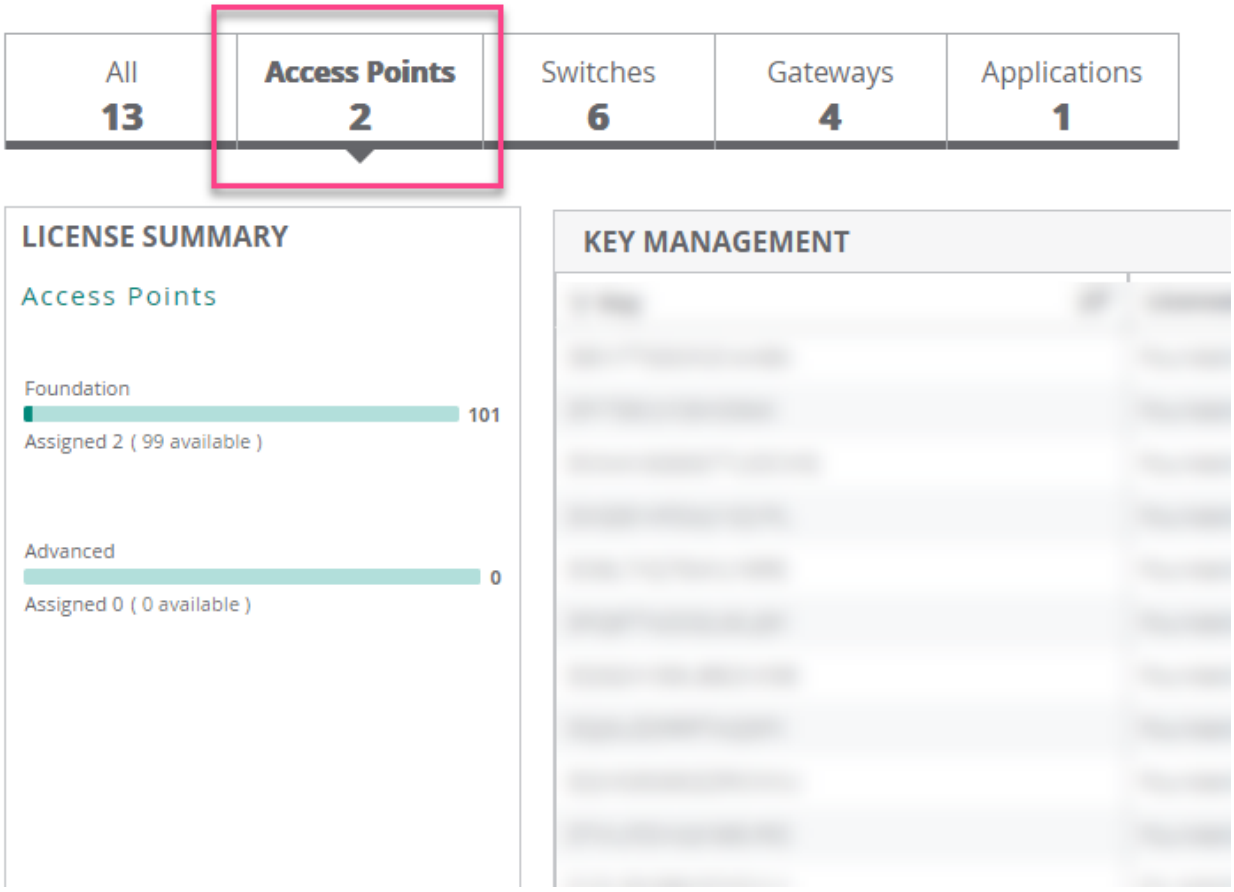
For the selected device type or app, or for all devices, the **License Summary** section lists down all the available licenses, the total number of licenses, the number of assigned licenses, and the number of unassigned licenses.

The available devices are APs, switches, and gateways.

The **Applications** tab currently lists the license keys for the Network Operations app and the Clear Pass Device Insight app (where applicable).

Click a single or multiple licenses in the **License Summary** section to display the details of the license type in the **Key Management** table. To unselect the license, click the selected license type again.

Figure 173 *License Summary Details for APs*



The preceding screenshot shows the following details:

- Total number of AP Foundation Licenses = 101
- Assigned AP Foundation Licenses = 2
- Unassigned AP Foundation Licenses = 99
- Total number of AP Advanced Licenses = 0

Key Management Table Details

The following table describes the contents of the **Key Management** table:

Table 235: *License Key Details*

Data Pane Item	Description
Key	License key number.
License Tier Type	Type of the license. Aruba Central supports the following types of licenses: ■ Foundation ■ Advanced The Foundation and Advanced licenses for APs, switches, and SD-WAN gateways are different from each other and cannot be used interchangeably.
Expiration	Expiration date for the license key.

Data Pane Item	Description
License Quantity	Number of licenses available.

To arrange the rows in ascending or descending order, use the sorting icon ( ) in the table header rows.

You can also use the row header indicated by the filter icon ( ) to type in search queries to refine the search.

License Expiry Date

The **Key Management** table displays the expiration date for each license.

As the licenses expiration date approaches, users receive expiry notifications. The users with evaluation license receive license expiry notifications through email 30, 15, and 1 day before the license expiry and on day 1 after the license actually expires.

The users with paid licenses receive license expiry notifications through email 90, 60, 30, 15, and 1 day before expiry and two notifications per day on day 1 and day 2 after the license expires.

If a license for the particular device expires, Aruba Central no longer manages that device. Currently, Aruba Central does not give an option to remove the expired licenses from the UI. The expired licenses are displayed in the **Key Management** table with the expired date.

Converting Legacy Tokens to New Licenses

The conversion of unassigned Device Management tokens to Foundation Licenses for APs, switches, and gateways is a one-time operation for the selected Device Management tokens. The Device Management token can either be an evaluation token or a purchased token.

The Service Management tokens are not converted into the Aruba Central Licenses.

If you do not convert the unassigned Device Management tokens by 31 December 2021, all the tokens are automatically converted to AP Foundation Licenses. If you wish to revert a conversion, you must contact Aruba Technical Support.

To complete the license conversion:

1. On the **Account Home** page, go to **Global Settings** > **Key Management**.
   The **Key Management** page is displayed.
2. Click **Click here to complete license conversion**.
   The **Convert Deprecated Licenses** page is displayed.
3. Select the key that you want to convert and click **Convert** on the row.
   The **Convert Deprecated Licenses** window is displayed.
4. Select the option to which you want to convert the unassigned device license for the key.
5. Click **Convert**.
   The **Convert** button is available only when all the licenses are assigned for the selected key.
6. View **Global Settings** > **License Assignment** page.
   A list of new licenses assigned for the deprecated keys is displayed.

Download Conversion Logs

This option provides information about how legacy Device Management and Services subscription keys are converted to Aruba Central Licenses either using automatic or manual license assignment.

The information can be downloaded as a PDF document. The document contains a table which provides following information:

- **Conversion Time**—Date and time when the legacy keys are converted to Aruba Central Licenses.
- **SKU Type**—Legacy key type as Device Management or Service subscription.
- **Subscription Key**—Legacy subscription key details.
- **Start Date**—Start date of the legacy subscription.
- **End Date**—End date of the legacy subscription.
- **Remaining Unassigned Quantity**—Number of Aruba Central Licenses that are not yet assigned (after the legacy subscription keys are converted).
- **Converted Subscriptions**—Information about the Aruba Central Licenses to which the legacy keys are converted.

Managing License Assignments

Aruba offers two tiers of device licenses as part of the Aruba Central Licenses. The two tiers are Foundation and Advanced Licenses. The devices in Aruba Central that offer Foundation and Advanced Licenses include the following:

- APs
- Switches
- SD-Branch Gateways

The value-added services that previously required service subscriptions are now packaged as part of either a Foundation or an Advanced License. To know more about the different types of licenses available for the devices, and the services packaged with each license, see Overview of Aruba Central Foundation and Advanced Licenses.

Before proceeding with the license assignment, ensure that all the license keys are available in Aruba Central. For more information on how to add license keys to Aruba Central, see Managing License Keys.

For more information about MSP Licenses, see Managing MSP Licenses.

Licensing Workflow in the Initial Setup Wizard

To enable automatic assignment of licenses from the Initial Setup Wizard:

1. Verify that you have valid license key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the **Assign License** tab, turn on the **Auto Assign License** toggle switch.

Licensing Workflow for a New User

If you are a new user in Aruba Central, you can avail of either the evaluation license or a paid license.

For an evaluation user, see the workflow at Starting Your Free Trial.

For a paid user, see the workflow at Setting up Your Aruba Central Instance.

If you are a new user in Aruba Central and have purchased one or several licenses, ensure that all of your license keys are added to Aruba Central.

For license assignment to devices, you can avail of one of the following options:

- Use the **Auto-Assign Licenses** option
- Manually assign, update, or unassign licenses

Enabling the Auto-Assign Licenses Option

The **Auto-Assign Licenses** option in Aruba Central enables automatic assignment of available licenses to all of the devices available in the inventory. When you enable this option, you must specify the preferred license type as either Foundation or Advanced. You cannot manually assign licenses to devices if the **Auto-Assign Licenses** option is enabled.

The licenses for APs, switches, and gateways cannot be used interchangeably. For example, you cannot use an AP Foundation License on a gateway. Similarly, if an Aruba 25xx Switch is in the inventory but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch. Before enabling the Auto-Assign License option for a specific device type, ensure that there are sufficient available licenses for the specific device type.

To enable automatic assignment of licenses from the License Assignment page:

1. On the **Account Home** page, under **Global Settings**, click **License Assignment**.

   The **License Assignment** page is displayed.
2. Select the device type to assign the license.

   The available tabs are Access Points, Switches, and Gateways. The total number of devices for each device type is displayed for each of the tabs.
3. On the device tab, slide the **Auto-Assign Licenses** toggle switch to the On position.

   The **Manage License Assignment (Auto)** window is displayed.
4. Select the appropriate license type, **Foundation** or **Advanced**, from the drop-down menu, and then click **Update**.

   All the unassigned devices of the selected type in the inventory are enabled for automatic assignment of license.

Manually Assigning, Updating, or Unassigning Licenses

The License Assignment page enables you to assign, update, or even unassign a license from a device.

Aruba Central monitors devices with a valid license only.

The licenses for APs, switches, and gateways cannot be used interchangeably. For example, you cannot use an AP Foundation License on a gateway. Similarly, if an Aruba 25xx Switch is in the inventory but the license available is for an Aruba 29xx Switch, the Aruba 29xx Switch license cannot be applied to the Aruba 25xx Switch.

To manually assign licenses to devices or to change the existing license assignment:

1. On the **Account Home** page, under **Global Settings**, click **License Assignment**.

   The **License Assignment** page is displayed.

2. Select a device type tab.

   The available tabs are **Access Points**, **Switches**, and **Gateways**. The total number of devices for each device type is displayed for each of the tabs.
3. Under **License Summary**, ensure that the **Auto-Assign Licenses** option is disabled.

   You cannot manually assign licenses if the Auto-Assign Licenses option is enabled.
4. Select the device for which you want to assign or update the license.

   Clicking on a device type displays two additional sub-tabs: **Licensed** and **Unlicensed**.

To manually assign or update licenses for all devices of a type, click **Select All**. You can also select devices at random.

5. Click **Manage**.

   The **Manage License Assignment (Manual)** window is displayed.
6. Do one of the following:
   a. To update or assign a license: Select the appropriate license from the drop-down menu and click **Update**.
   b. To unassign a license: Select **Unassign** to remove the existing license from that device.

Migration Workflow for an Existing User

Whether you are an evaluation user or a user with purchased licenses, the following is the migration workflow to the new Aruba Central Licenses:

Any existing rules set about Service Management tokens through APIs are discarded during the migration.

1. For all existing APs and switches that are already assigned licenses in the legacy system, the licenses are automatically converted to device-specific Foundation Licenses in the new model. The gateway licenses remain unchanged.
2. To check how the migration was done, and to learn more about the new license keys and corresponding licenses, in the **Account Home** page, go to **Global Settings** > **Key Management**.

   For more information about the **Key Management** page, see Managing License Keys.
3. To check how the legacy licenses were converted, navigate to **Account Home** > **Global Settings** > **Key Management** page, and click the **Download Conversion Logs** link.
4. If there are unassigned evaluation or purchased Device Management tokens, you can convert the legacy tokens to license keys for the new Aruba Central Licenses.

Service Management tokens are not converted. Instead, the AP licenses are pre-packaged with additional services.

   To know more about converting unassigned Device Management tokens, see Converting Legacy Tokens to New Licenses.
5. If you had the auto-licensing option enabled before migration, in the new licensing model the **Auto-Assign Licenses** option is automatically enabled for APs, switches, and gateways. The **Auto-Assign Licenses** option for APs and switches is set with the corresponding device-specific Foundation Licenses.

NOTE

The **Auto-Assign Licenses** option for gateways is not enabled during the migration.

For more information about the **Auto-Assign Licenses** option, see Enabling the Auto-Assign Licenses Option.

6. If you had the auto-licensing option disabled before migration, this option is also disabled in the new licensing system.

Viewing the License Assignment Details

The License Assignment page consists of three sections for the type of device selected from the tabs. The device can be **Access Points**, **Switches**, or **Gateways**,

License Summary

A summary about the type of licenses available for the selected device type, the number of licenses available, and number of licenses assigned.

The available devices for Aruba Central include APs, switches, and gateways. Clicking on a device type displays two additional sub-tabs: **Licensed** and **Unlicensed**.

Clicking on one or more license type in the License Summary section displays the details of the license type in the License Management section. To deselect the license, click the selected license type again.

License Assignment

The **License Assignment** section provides detailed information about all the devices in the inventory and license status for each of the device. This table provides following information about each device in the inventory:

- Type
- Serial Number
- MAC address
- Model
- Customer
- Assigned License

Use the sorting icon ( ) in the table header row to arrange the rows in ascending or descending order. You can also use the row header indicated by the filter icon ( ) to type in search queries to refine the search.

Renewing License Assignments

To renew your license, contact your Aruba Sales team.

Onboarding Devices to Aruba Central

If you are a registered Aruba Central portal user, Aruba Central automatically retrieves the devices associated with your account and adds it to the device inventory. To verify, if the devices are added to Aruba Central's device inventory, navigate to **Global Settings** > **Device Inventory** in the Aruba Central UI.

NOTE

The users with the evaluation subscription may have to add the devices manually using their Aruba Activate credentials.

- If the devices are listed in the inventory, proceed to assign devices to groups, labels, and sites.
- If the devices do not show up in the inventory, click **Sync Now** to synchronize the inventory with the Activate database.
- If the devices do not show up in the inventory even after the sync operation, manually add these devices.

Adding Devices to Inventory Manually

To manually add the devices, on the **Device Inventory** page, click one of the device addition options described in the following table:

Table 236: *Adding Devices*

Device Addition Method	Description
Add by MAC Address/Serial Number	Allows you to add devices based on MAC address and serial numbers. You can add up to 32 devices.
Add with Cloud Activation Key	Allows you to add multiple devices from a single purchase order by using the cloud activation key. To add devices: 1. Enter the **Cloud Activation Key** and MAC address of the device. 2. Click **Add**. Aruba Central retrieves all devices that belong to the same purchase order and displays the list.
Add Using Activate	Allows you to retrieve the devices associated with an Activate user account. To add devices: 1. Enter the username and password of the Activate user account. 2. Click **Add**. The devices associated with the Activate account are retrieved and added to the list of devices displayed on the **Device Inventory** page. **NOTE:** You can use this option only once. After the devices are added, Aruba Central does not allow you to modify or re-import the devices using your Aruba Activate credentials.

Assigning Subscriptions to Aruba Gateways

For Aruba gateways to start functioning, you must onboard them to the device inventory in Aruba Central and ensure that a valid subscription is assigned to each gateway. A valid subscription allows the gateway to be managed by Aruba Central.

This section includes the following topics:

Gateway Subscriptions

Aruba Central supports the following types of subscriptions for gateways:

- **DM Assigned**—Displays whether the device management subscription has been assigned.
- **Unassigned**—Select gateway(s) and select **Unassigned** from the drop-down list to unassign the subscription.

- **Foundation**—This subscription can be assigned to these gateways:
  - Aruba 70xx series
  - Aruba 72xx series
  - Aruba 90xx series
- **Foundation-Base**—This subscription can be assigned to Aruba 70xx series and Aruba 90xx series Gateways. Gateway devices with the Foundation-Base capacity subscription can support up to 75 client devices per branch.

  When the client capacity reaches the threshold:
  - Aruba Central triggers the **Gateway base license capacity limit exceeded** alert.
  - If the notification options for the **Gateway base license capacity limit exceeded** alert is configured, Aruba Central sends an email notification with a list of Aruba gateways that exceed the client capacity threshold. You can also configure alerts to trigger an incident using Webhook. .
- **Advanced**—This subscription is available for all Aruba gateways. It allows users to use advanced features and services such as SaaS Express. This subscription can be assigned to these gateways:
  - Aruba 70xx series
  - Aruba 72xx series
  - Aruba 90xx series

Gateway Subscriptions with Security License

The following gateway subscriptions are packaged along with security license that includes the Intrusion Detection and Prevention System (IDPS) feature. These subscriptions can be assigned to Aruba IDPS supported gateways:

- **Foundation with Security**—All features of a Foundation subscription along with security license.
- **Foundation-Base with Security**—All features of a Foundation-Base capacity subscription along with security license.
- **Advanced with Security**—All features of an **Advanced** subscription along with security license.

You can evaluate Aruba IDPS with **Advanced with Security** subscription for a period of 90 days.

Assigning Subscriptions to Gateways

1. To assign subscription to a gateway, complete the following steps:
2. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.

   The **Subscription Management** page is displayed.
3. Under **Gateway Subscriptions**, select the device to which you want to assign a subscription.
4. Expand the drop-down in the **Assignment** column for the selected device.
5. Select the subscription; for example, **Foundation**.
6. To assign subscription to multiple devices:
   a. Select the devices in the table.
   b. Click **Batch Assignment**.
   c. Select the subscription to assign.

When a subscription assigned to a gateway expires, Aruba Central automatically assigns a valid subscription from the same subscription category.

When you assign a subscription with security license, the gateways reboot to enable the traffic inspection engine for the first time. It is recommended that you apply the security license after business hours, as this might result in a downtime in the network.

When assigning subscriptions, if you change a subscription with security license to a subscription without a security license, you must reboot the gateway manually to release the CPU resources that were assigned to the traffic inspection engine. It is recommended to reboot the gateway after business hours, as this might result in a down time in the network.

Virtual Gateway Subscriptions

Aruba Virtual Gateway is a virtual instance of headend gateway for SD-WAN. Aruba Central supports licenses based on the bandwidth capacity for virtual gateways. All license assignments are undertaken by the virtual gateway orchestration app.

Aruba Central supports VGW licenses that cater to a variety of requirements. The options include one, three, and five year periods and the bandwidth options are 500 Mbps, 2 Gbps, and 4 Gbps capacity licenses.

The base SKUs available are: VGW-500M, VGW-2G, and VGW-4G. The availability of SKUs is also dependent on the installation consuming the license.

The account maintains a pool of VGW licenses, upon license expiry or if the license pool has no licenses left (all consumed) the license is unassigned from the account. When deployed without valid or paid licenses, four evaluation (90 day) licenses of each base SKU is allocated to every customer account.

License consumption can be tracked in the **Key Management** or **Subscription Assignment** pages.

The list of licenses available against consumed licenses are also displayed during the deployment of a virtual gateway.

When the client capacity reaches the threshold:

- Aruba Central triggers the **Gateway base license capacity limit exceeded** alert.
- If the notification options for the **Gateway base license capacity limit exceeded** alert is configured, Aruba Central sends an email notification with a list Aruba virtual gateways that exceed the client capacity threshold. You can also configure alerts to trigger an incident using **Webhook**. .

For **Paid** licenses email notifications are sent out in 30 day intervals starting at 90th day before expiration and the last notification a day before the expiry of the license.

For **Evaluation** licenses email notifications are sent out on the 30th day before expiration and a day before the expiry of the license.

Assigning Subscriptions to Virtual Gateways

1. Under **Virtual Gateway**, select the device to which you want to assign a subscription.
2. Expand the drop-down in the **Assignment** column for the selected device.
3. Select the subscription SKU. For example, **VGW-500MB**.
4. To assign subscription to multiple devices:

   Aruba Central automatically assigns a valid subscription to a virtual gateway. When a subscription expires, Aruba Central automatically assigns a valid subscription from the same subscription category.

For more information on available SKUs, contact your Aruba Sales Specialist.

Assigning Gateways to a Group

A group in Aruba Central is a primary configuration element that acts like a container. In other words, groups are a subset of one or several devices that share common configuration settings. Aruba Central supports assigning devices to groups for the ease of configuration and maintenance. For example, you can create a common group for Branch Gateways that have similar configuration requirements.

To assign gateways to a group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

2. Under **Maintain**, click **Organization** > **Groups**.

   The **Groups** page is displayed. By default, the **Groups** page is displayed.

3. Under **Manage Groups**, from the devices table on the right, select the gateway that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.
5. Click **Yes** in the confirmation dialog box.

If the group is not available in the list, click ⊕ **New Group** to create a new group, and then drag and drop the gateways to the group that you just created.

Assigning Gateways to Sites

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or a venue. You can create a branch or campus site; for example Branch A or Campus A, for a specific geographical location and assign devices to it. You can use these sites as filters for viewing your deployment topology, monitoring network and device health.

To assign gateways to a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

2. Under **Maintain**, click **Organization** > **Sites and Labels**.

   The **Sites and Labels** page is displayed. By default, the **Sites** page is displayed.

3. Under **Manage Sites**, locate the site to which you want to assign a device.

   You can also add a new site by clicking ⊕ **New Site** and providing details, such as site name and address.

4. Click **Unassigned** to view devices that are not assigned to any site.
5. Select one or several devices from the list of devices.
6. Drag and drop the devices to the site on the left.
7. Click **Yes** in the confirmation dialog box.

For more information, see *Sites* in Aruba Central documentation.

Assigning Labels to Gateways

In Aruba Central, labels refer to the tags attached to a device provisioned in the network. You can use labels for tagging devices to a specific area in a physical location, to an owner or a specific branch, or a business unit. You can use these labels as filters for monitoring branch and device health, and generating reports.

To assign a label to a gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Organization** > **Sites and Labels**.
   The **Sites and Labels** page is displayed. By default, the **Sites** page is displayed.
3. Use the toggle switch to access the **Labels** page.
4. Locate the label to which you want to assign a device. You can also create a new label by clicking  **Add Label** and providing a label name.
5. In the table that lists the labels, you can perform one of the following actions:
   - Click **All Devices** to view all devices.
   - Click **Unassigned** to view all the devices that are not assigned to any labels.
6. Select **Unassigned**. A list of devices that are not assigned to any label is displayed.
7. Select one or several devices from the list of devices.
8. Drag and drop the selected devices to a specific label. A pop-up window opens and prompts you to confirm the label assignment.
9. Click **Yes** in the confirmation dialog box.

For more information, see *Labels* in Aruba Central documentation.

Recovering an Aruba Gateway

The following procedure outlines the steps to recover an account using the `disaster-recovery on` command and the **branchsupport** account options.

Using Command in the Gateway's Local Configuration

Using the `disaster-recovery on` command allows you to enable the config mode and edit the configuration in the Aruba Central local Gateway-node.

To make changes to the configuration that enables communication between the gateway and Aruba Central, complete the following steps.

1. Ensure the configuration sent to the gateway allows communication with Aruba Central. This can be verified by executing a `show aruba-central details` from the CLI.
2. In Aruba Central CLI, execute `show configuration effective <path to local-node of Gateway>` command.
3. When you turn disaster-recovery off using the `disaster-recovery off` command, the gateway contacts Aruba Central again and synchronizes the configuration.

If Aruba Central reverts to the earlier non-functional state, recheck and test the configuration used.

Using the Branchsupport Account

The **branchsupport** account allows the network administrator to gain access to a gateway that is in the factory default state and is failing to connect to Aruba Central.

To prevent security loopholes, this account is deleted automatically as soon as the device gets any configuration pushed from Aruba Central.

The **branchsupport** account is only available when:

- There is no configured admin account.
- The managed device is not in contact with the Aruba Central.

To access the **branchsupport** account, use these credentials:

- Username—*branchsupport*
- Password—*mac-address-lowercase-colondelim*

Assigning a Group Role to an Aruba Gateway Group

The term persona in Aruba Central refers to a group role that you can set for the device groups. To deploy gateways for the SD-WAN or WLAN solution, you must configure a group role to designate gateways as Branch Gateways or VPNCs.

To assign a group role to the gateways in a group, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the group selected contains at least one active gateway.

   The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
4. In the **Set Group Type** pop-up window, select the group role as **Branch Gateway** or **VPNC**.
5. Select a group role and save settings.

After you define a group role as a VPNC or Branch Gateway, Aruba Central does not allow you to edit or modify the group role.

You can configure Aruba IDPS only on Aruba 9004 gateways. For the current release, Aruba 9004 gateways can be deployed only as Branch Gateways.

Gateways in MSP Mode

Aruba Central does not support managing gateways at the MSP level. However, gateways can be configured and managed at the tenant account level. The persona of a default group at the tenant account level in MSP is set to **Branch Gateway**. The VPNC option is disabled.

Connecting Aruba Gateways to Aruba Central

The Aruba gateways have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The gateways also support multiple active uplinks for ZTP (also referred to as automatic provisioning). The supported ZTP ports for different hardware platforms are listed in the following table. All these ZTP ports are assigned to VLAN 4094.

Table 237: *ArubaOS Hardware Platforms and Supported ZTP Ports*

ArubaOS Hardware Platform	Supported ZTP Ports
Aruba 7005 Gateway	ALL ports except 0/0/1
Aruba 7008 Gateway	ALL ports except 0/0/1
Aruba 7010 Gateway	ALL ports except 0/0/1
Aruba 7030 Gateway	ALL ports except 0/0/1
Aruba 7024 Gateway	ALL ports except 0/0/1
Aruba 7210 Gateway	ALL ports except 0/0/1
Aruba 7220 Gateway	ALL ports except 0/0/1
Aruba 7240 Gateway	ALL ports except 0/0/1
Aruba 7280 Gateway	ALL ports except 0/0/1
Aruba 9004 Gateway	ALL ports except 0/0/1
Aruba 9004-LTE Gateway	ALL ports except 0/0/1
Aruba 9012 Gateway	ALL ports except 0/0/1

To know the minimum software version required for the gateways, see Supported SD-Branch Components.

To automatically provision the gateways:

1. Connect your gateway to the provisioning network.
2. Wait for the device to obtain an IP address through DHCP. Gateways support multiple uplink ports. The first port to receive the DHCP IP connects to the Activate server and completes the provisioning procedure:
   - If the device has factory default configuration, it receives an IP address through DHCP, connects to Aruba Activate, and downloads the provisioning parameters. When a device identifies Aruba Central as its management entity, it automatically connects to Aruba Central.
   - If the device is running a software version that does not have the SD-WAN image, the devices are automatically upgraded to a supported SD-WAN software version.

Aruba 72xx gateways with the ArubaOS 8.3.0.9 factory default image use only port 0/0/1 (the last copper port) for ZTP. When the factory default gateways connect to Activate through ZTP for the first time, Activate recommends a base SD-WAN image, which the gateways will download. In the SD-WAN image, port 0/0/1 is used as a debug port, and DHCP requests will not be sent out of port 0/0/1 for subsequent ZTP requests. Hence, ZTP workflow for Aruba 72xx gateways with the ArubaOS 8.3.0.9 factory default image will not work. You must manually upgrade the Aruba 72xx gateways to the SD-WAN image or use other methods like full-setup and static-activate to provision the gateways.

3. Observe the LED indicators. Table 2 describes the LED behavior.

Table 238: *LED Indicators*

LED Indicator	LCD Text	Description
Solid Amber	Getting DHCP IP	Indicates that the uplink connection is UP, but DHCP IP is yet to be retrieved.
Blinking Amber	Activate Wait	Indicates that the device was able to reach the DHCP server and the connection to the Activate server is yet to be established.
Solid Green	Activate OK	Indicates that the device was able to retrieve provisioning parameters from the Activate server.
Alternating Solid Green and Amber	Activate Error	Indicates that the device was not able to retrieve provisioning parameters.

After successfully connecting to Aruba Central, the gateways download the configuration from Aruba Central.

- From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch Gateways no longer require additional reboot when they receive the controller IP from Aruba Central after the ZTP process. Some services are restarted, resulting in an expected network impact, but the gateways do not reload for the second time. However, the gateways will reboot if there are any subsequent controller IP changes.
- The gateways also include service ports that the technicians can use for manually provisioning devices in the event of ZTP failure. For more information on ports available for Aruba 7000 Series Mobility Controllers and Aruba 7200 Series Mobility Controllers, see *ArubaOS User Guide*.

Configuring Communication Ports

The SD Branch appliances use HTTPS WebSockets and IPsec tunnels for secure communication.

- The HTTPS WebSockets is used for the management traffic; that is, for communication between Aruba Central and Aruba gateways.
- The IPsec tunnel is used for communication between Branch Gateways and VPNCs.

For a complete list of domain URLs, ports, and protocols that you must allow over a network firewall, see *Opening Firewall Ports for Device Communication* in *Aruba Central Help Center*.

When configuring ACLs to allow traffic over a network firewall, Aruba recommends that you use the domain names instead of IP addresses. For more information on ACLs, see Configuring Firewall Policies and ACLs. For Branch Gateways to set up IPsec tunnel with the VPNCs, the UDP 4500 port must be open. For more information on firewall ports required for communication between Aruba gateways and other network elements, see *ArubaOS User Guide*.

Certificates

By default, Aruba Central includes a self-signed certificate that is available on the **Certificates** page. The default certificate is not signed by a root certificate authority (CA). For devices to validate and authorize Aruba Central, administrators must upload a valid certificate signed by a root CA.

Aruba devices use digital certificates for authenticating a client's access to user-centric network services. Most devices such as controllers and Instant APs include a server certificate by default for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Aruba Central-managed devices such as Instant AP and switches support the following root CA certificates:

Instant APs	Switches
▪ AddTrust ▪ GeoTrust ▪ VeriSign ▪ Go Daddy	▪ Comodo ▪ GeoTrust

Uploading Certificates

To upload certificates, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
3. Select the **Certificates** tab.

   The **Certificates** page opens.
4. Click the plus icon to add the certificate to the certificate store.
5. In the **Add Certificate** dialog box, do the following:
   a. In the **Name** text box, specify the certificate name.
   b. Select the type of certificate. You can select any one of the following certificates:
      - **CA** —Digital certificates issued by the CA.
      - **Server**—Server certificates required for communication between devices and authentication servers.
      - **CRL**—Certificate Revocation List that contains the serial numbers of certificates that have been revoked. This certificate is required for performing a certificate revocation check.
      - **OCSP Responder Cert**—OCSP responder certificates.
      - **OCSP Signer Cert**—OCSP Response Signing Certificate.

        OCSP certificates are required for OCSP server authentication.
   c. From the **Format** drop-down list, select a certificate format; for example, PEM, DER, and PKCS12.
   d. In the **Passphrase** text box, enter a passphrase.
   e. In the **Retype Passphrase** text box, retype the passphrase for confirmation.

The **Passphrase** and **Retype Passphrase** text boxes are displayed only when you select **Server Certificate** from the **Type** drop-down list.

   f. In the **Certificate File** field, click **Browse** and select the certificate files.
   g. Click **Add**. The certificate is added to the Certificate Store.

Managing Certificates on Instant APs Configured Using Templates

Aruba Central supports uploading multiple certificates to Instant APs configured using templates. You can manage certificates either from the Aruba Central UI or through the API Gateway. For more information about APIs, see *API Documentation*.

To push certificates to Instant APs configured using templates:

1. Upload certificate(s) through one of the following methods:
   - **UI**—See Uploading Certificates.
   - **API**—Use the **[POST] /configuration/v1/certificates** API.
2. Get the certificate name and MD5 checksum through one of the following methods:
   - **UI**—In the **Network Operations** app, filter **All Devices**. Under **Maintain**, click **Organization** and select the **Certificates** tab. The **Certificate Store** table displays these details.
   - **API**—Use the **[GET] /configuration/v1/certificates** API.
3. In the template, anywhere before the **per-ap settings** block, depending on your requirement, add one or more of the following commands:

```
ca-cert-checksum <ca_cert_checksum/ca_cert_name>
cp-cert-checksum <captive_portal_cert_checksum/captive_portal_cert_name>
radsec-ca-checksum <radsed_ca_checksum/radsed_ca_name>
radsec-cert-checksum <radsed_cert_checksum/radsed_cert_name>
server-cert-checksum <server_cert_checksum/server_cert_name>
```

You can either use the certificate name or the checksum value in the command. Or, you can set it as a variable and enter the variable value for the Instant AP. Aruba recommends using the certificate name.

Example 1

```
ca-cert-checksum my_default_cert
```

Example 2

```
ca-cert-checksum %ca_cert_name%
variable:
{
 "ca_cert_name": "my_default_cert"
}
```

Chapter 14
Provisioning Aruba Gateways in Aruba Central

Aruba Central offers the following options to configure Gateways for SD-WAN deployments:

- Groups—You can create a logical subset of devices as groups. If you have devices that must share common configuration settings, ensure that you assign these devices to the same group. Any new device joining a group inherits the configuration that is already applied to the devices in a group. Similarly, you can also maintain separate groups for Branch Gateways and VPNCs by assigning a group role for the devices. For more information, see Assigning Gateways to a Group.
- Device-specific configuration—If you have a considerably lesser number of devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration to one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level. Aruba Central marks the discrepancies in the group and device configuration as overrides on the Configuration Audit page.
- Bulk Configuration—Aruba Central supports several bulk configuration options for Aruba Gateways:
  - Bulk Configuration Upload—Allows you to download a list of Aruba Gateways from Aruba Central in the CSV file format. You can add the configuration parameters for hostname, system IP address, VLAN, and Ports, and then upload the CSV file to Aruba Central. For more information, see Uploading Bulk Configuration Template.
  - Gateway Pools—Allows you to create a common pool of IP addresses and enables automatic assignment of IP addresses to Aruba Gateways. For more information, see Configuring Gateway Pools for Aruba Gateways.
  - DHCP Pools—Allows you to configure a DHCP pool, using which Aruba Central automatically assigns a subnet to each Aruba Gateway for a given VLAN. For more information, see Configuring DHCP Address Pools on Aruba Gateways.
- APIs—Allows you to configure and monitor devices using NB APIs.

Different Modes of Configuring Gateways and Gateway Groups

Aruba Central supports the following methods to configure Gateway groups and Gateways.

- **Guided Setup**—You can use the **Guided Setup** to quickly configure basic and essential parameters on Aruba Gateways for deploying the SD-WAN solution. The **Guided Setup** provides a wizard-based workflow for provisioning Gateways. The wizard allows you to configure Gateways at your own pace, pause, and resume when required. However, the Guided Setup will not be available after you complete the provisioning workflow for a Gateway group or a Gateway.

  For more information on configuring Gateways using the Guided Setup, see the following topics:
  - Configuring Branch Gateways Using the Guided Setup
  - Configuring Branch Gateway Groups Using the Guided Setup
  - Configuring VPNC Group Using the Guided Setup
  - Configuring VPNCs Using the Guided Setup

- **Basic Mode**—Allows you to configure your Gateways in a non-linear fashion. This mode allows you to make configuration changes after you provision your gateways for the first time using a Guided setup. For more information, see Configuring an SD-Branch Network Using the Basic Setup.

Figure 174 *Basic Mode*

- **Advanced Mode**—Allows you to configure advanced features for SD-WAN deployments. For more information, see Configuring an SD-Branch Network Using the Advanced Setup.

Figure 175 *Advanced Mode*

- Before you proceed with the configuration tasks, browse through the recommendations and best practices described in the Aruba SD-Branch Fundamentals Guide and Aruba SD-Branch Security Hardening Guide.

Configuring Branch Gateway Groups Using the Guided Setup

Aruba Branch Gateways operate at the branch to optimize and control WAN, LAN, and cloud security services. The Branch Gateway provides features such as routing, firewall, security, website content filtering, and WAN compression. With support for multiple WAN connection types, the Branch Gateway routes traffic over the most efficient link based on availability, application, user-role, and link health. This allows organizations to take advantage of high-speed, lower-cost broadband links to supplement or replace traditional WAN links such as MPLS.

You can configure a Branch Gateway group or Branch Gateway device using either the Guided Setup, Basic mode, or Advanced mode. This section describes the procedure to configure Branch Gateway groups using the Guided Setup.

Before You Begin

Ensure that you have completed the following procedures:

- Gateways are onboarded to Aruba Central.
- Gateways are assigned valid subscriptions in Aruba Central.
- Gateways are assigned to groups.
- Gateways are assigned the Branch Gateway group role.

Ensure that the devices in the group are not running the guided setup at the device level. If the device is being configured using the Guided Setup, the group level setup will not be executed.

Configuring a Branch Gateway Group using the Guided Setup

To configure a Branch Gateway group, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
   If you are accessing the Branch Gateway group configuration page for the first time, the **Guided Setup** wizard opens automatically. Otherwise, click **Guided Setup**.
   The **Guided Setup** wizard displays the following tabs:
   - **System**—Allows you to configure system parameters.
   - **LAN**—Allows you to configure LAN interfaces.
   - **WAN**—Allows you to configure WAN interfaces.
   - **SD-WAN & Routing**—Allows you to configure an SD-WAN overlay and routing profiles.
   - **Policies**—Allows you to configure various traffic policies such as User Roles, Applications, WAN, and QoS, and security policies also.
4. Click **Begin** to start the guided setup process and complete the steps provided in the following sections:
   - Configuring System Parameters for a Branch Gateway Group
   - Configuring a LAN Interface for a Branch Gateway Group
   - Configuring a WAN Interface for a Branch Gateway Group
   - Configuring VPN Hubs and Routing Profiles for a Branch Gateway Group
   - Configuring Policies for a Branch Gateway Group

Many procedures involve adding or configuring parameters in tables. Note that you have options to edit and delete the existing configurations.

Configuring System Parameters for a Branch Gateway Group

Before you begin, ensure that the following conditions are satisfied:

- Every Aruba Gateway must have a System IP assigned, in order to be fully-functional. Aruba Central does not send any configuration to a Branch Gateway unless it has a System IP assigned to the device.

Control plane traffic such as RADIUS, TACACS+, SNMP, and Syslog are sourced from the System IP address.

- Other parameters such as NTP and DNS are also required for the device's operation.

To configure system parameters, complete the following steps:

1. In the **System** tab configure a **System IP** using one of the following options:
   - **Define system IP address pool**—Select this option to define an IP address pool for the gateways in this group. You can configure an IP address range by providing the start and end IP addresses. Aruba Central automatically allocates an IP address to each gateway, and assigns it to VLAN 4087 which is the System IP address of the device.
   - **Specify static IP addresses later**—Select this option to configure the system IP address at the device level.
2. Click **Next**.

   The **Model** page is displayed.
3. Select the Gateway from the **Model** drop-down list.
4. Click **Next**.

   The **Time** page is displayed.

   Configure the NTP server for system clock synchronization. The system automatically updates the time zone including the relevant daylight savings time (DST) across time zones. You can optionally specify a time zone which is applied to all the gateways in the group. The default time zone is set to GMT.
5. In the **Public NTP Servers** table, click the **+** icon to add a Public NTP Provider:
   - **IPV4 Address/FQDN**—Enter the IPV4 address or the FQDN of the public NTP provider to add the NTP servers to the Branch Gateways in this group.
   - **Burst Mode**—Select this option to expedite the system clock calibration.
6. Choose the time zone from the **Timezone** drop-down list.

   The list contains a list of **Primary** time zones followed by other time zones.
7. Click **Next**.

   The **DNS** page is displayed.
8. Select one of the following options to configure a DNS server:
   - **Specify DNS servers**—Select this option to configure a DNS server and define the following parameters:
     a. Enter a **Domain name**.
     b. Click the **+** icon to add a **Public DNS server**. You can select one or more DNS service providers from the list or you can select **User Defined** for **Provider** and specify the IPv4 addresses of two or more public DNS name servers.
     c. Enter the **IPv4 address** if you have selected **User Defined** for provider. If you have selected the DNS service providers from the list, the IP addresses will be auto-populated.
     d. The **Uplink VLAN** drop-down becomes active when you select **User Defined** for the provider. You can select the VLAN ID from the **Uplink VLAN** drop-down list.
   - **Learn DNS server from ISP**—Select this option if you want the gateway to learn the DNS server dynamically from the ISP.

The DNS servers configured here are the ones that the gateway uses to resolve addresses. It must be reachable through the underlay as the device needs it to communicate with and the SD-WAN Orchestrator.

9. Click **Next**.

   The **Management User** page is displayed.

A management user refers to the admin user with credentials to log in to the local management interface of the device.

1. To add a user, click the **+** icon in the **Local Management Users** table. The **Add Management User** pop-up is displayed.
2. Enter the user name and password that you want to configure.
3. Select a user role from the **Role** drop-down. The following options are the options available:
   - **Super user role**—Administrator user role.
   - **Guest provisioning role**—Administrator role for provisioning guest users.
   - **Read only**—Read-only user role.
4. Click **Save**.
5. To authenticate an admin user using AAA policy, turn on the **AAA authentication** toggle switch.
6. Click the **+** icon in the **AAA Servers** table to create an AAA server for authenticating device management user.

   The **Add AAA Server** pop-up is displayed.
7. Configure the following parameters:
   - **Name**—Name of the authentication server.
   - **Server IP**—IP address of the authentication server.
   - **AAA authentication**—Enables centralized management user authentication using **RADIUS** or **TACACS** servers. For each AAA server, you must specify the IPv4 address or FQDN of the servers along with the protocol and shared secret.
   - **Key**—Shared key for authenticating a device administrator.
   - **Retype key**—Enter the key again to confirm.
8. Click **Save**.
9. Review the summary page and click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

10. Click **Continue** to configure a LAN interface.

Configuring a LAN Interface for a Branch Gateway Group

This section focuses on the LAN configuration of the Branch Gateways. By default, LAN interfaces have LLDP enabled and a role-based security. However, this setting can be changed when you configure security policies.

To configure VLANS on Branch Gateway group:

1. In the **VLAN** tab, select the **IP DHCP server** check box for the gateways to act as DHCP servers.
2. Click the **+** icon in the **VLANs** table to add a new VLAN.
3. Enter the VLAN **Name**.
4. Enter the **VLAN ID**.
5. Select one of the following **IP addressing mode** from the drop-down list:
   - **Static**—Select this option to use a static IP address. If you want to configure the LAN IP addresses at the device level, leave the IPv4 address and netmask fields empty. You can also set the same static IP/netmask for all the devices in the group.

- **IPV4 Address**—Enter a unique static IP address for each gateway in the group or a common address for all gateways in the group.
- **Netmask**—Enter the subnet mask of the IP address.

Ensure that this VLAN is not routable, as it overlaps with the other gateways.

- **Dynamic DHCP Pool**—Select this option to assign IP address from a dynamically carved DHCP pool. To configure an IP address range for dynamic assignment of DHCP IP addresses, configure the following parameters:
  - **Dynamic DHCP pool start address**—The starting IP address in the DHCP pool that gateways allocate to branch devices.
  - **Dynamic DHCP pool end address**—The last IP address in the DHCP pool that gateways allocate to branch devices.
  - **Hosts per branch**—The number of hosts per branch. This determines the subnet size that is allocated to each Branch Gateway in the group.
  - **Domain name**—The DNS domain name assigned to branch devices.
  - **DNS server type**—Type of the DNS server. You can use either a **Public DNS Service** or add a DNS server by selecting the **User Defined** DNS option.
  - **DNS service provider**—If you use a **Public DNS Service**, select the name of the DNS service provider from the list. For example, Google.
  - **DNS server IPv4 addresses**—The IPv4 address of the DNS server. You can specify up to eight IP addresses separated by a comma.

6. To configure branch gateways as DHCP server, turn on the **Act as DHCP server** toggle switch and configure the following parameters:
   - **Network**—The network IP address.
   - **Netmask**—The subnet mask of the network.
   - **Default router**—The IP address of the device used by clients if they want to communicate with devices outside of their subnet. Predominantly, this will be the Branch Gateway IP address for the particular VLAN, or the VRRP virtual IP, if configured.
   - **Reserve first**—The first IPv4 address for the CIDR range.
   - **Reserve last**—The last IPv4 address for the CIDR range.
   - **Domain name**—The DNS domain name assigned to branch devices.
   - **DNS server type**—Type of the DNS server. You can use either a public DNS server or add a DNS server by selecting the user-defined DNS option.
     - **DNS Service Provider**—If you use a **Public DNS Service**, select the name of the DNS service provider from the list. For example, Google.
     - **DNS server IPv4 addresses**—If you use a **User Defined** DNS server, enter the IP addresses here. You can specify up to eight IP addresses separated by a comma.
7. Turn on the **Enable DHCP relay** toggle switch to relay the incoming DHCP requests to an external DHCP server. Select this option when centralized DHCP servers are deployed to provide addressing to branch devices or if device profiling is performed by services such as Aruba ClearPass.
8. Click the **+** icon in the **External DHCP Server** table.
9. Add the IPV4 addresses.
10. Click **Save**.

11. Click **Next**.

    The **LAN Ports** page is displayed.

12. To add a LAN port, click the **+** icon in the **LAN Ports/Port Channel** table.
13. Enter a **Name** for the port.
14. Select a port channel or a port from the **Ports** drop-down list.
    - If you have selected **Port Channel** for the LAN port, configure the following parameters:
      - **Port channel protocol**—Select a port channel protocol; for example, LACP (Link Aggregation Control Protocol). If you have selected LACP, select the LACP mode as active or passive from the **LACP mode** drop-down list.
      - **Port channel members**—Select the port channel members.
15. Select one of the following **VLAN mode**s:
    - **Access**—Select this option to allow the LAN port to carry traffic only for the VLAN to which they are assigned. All transmitted and received traffic on the port is untagged.
    - **Access**—Select the VLAN ID assigned to the port or port channel.
    - **Trunk**— Select this option to allow the LAN port to carry traffic for multiple VLANs. If you select the **Trunk** mode, configure a list of allowed VLANs.
    - **Native VLAN**—The untagged VLAN ID for the port or port channel.
    - **Allowed VLAN**—The range of VLAN IDs assigned to the port or port channel including the Native VLAN.
16. Click **Next**.
17. Review the summary page and click **Finish**.
18. Click **Continue** to configure a WAN interface.

Configuring a WAN Interface for a Branch Gateway Group

This section focuses on the WAN configuration of the branch gateways.

To configure a WAN interface, complete the following steps:

1. In the **WAN** tab, turn on the **Enable health checks** toggle switch.

   The WAN health check enables sending probes to measure availability and SLA of the uplinks. When the health check feature is enabled, the probes are sent through the underlay at regular intervals to verify if the Internet is reachable over the uplink interfaces configured on Gateways.

2. Configure the following health check parameters:
   - **Health check destination**—You can configure a **User defined** IP address or use the default **Aruba cloud** instance to send WAN health check probes.
   - **Health check IP address**—If it is a **User defined** destination, enter the IPv4 address or FQDN of a host that is reachable through the WAN paths outside the VPN tunnel.
   - **Health check probe mode**—Select one of the following probe modes:
     - **Ping**—Sends ICMP probes to measure latency and packet loss.
     - **UDP**—Sends UDP Probes through UDP port 4500 to measure latency, packet loss, and jitter.
3. Click **Next**.

   The **Load Balancing** page is displayed.

4. Select one of the following modes for uplink load balancing:
   - **Round robin**—Select this option to sequentially distribute outgoing sessions between WAN links. It is the simplest algorithm to configure and implement, but may result in uneven traffic distribution over time.
   - **Session count**—Select this option to balance traffic among the uplinks based on the current number of active sessions managed by each link, so that the load for each active uplink stays within 5% of the other active uplinks. For example, if there are two active uplinks with the **Weight** parameter defined as 10 and 20, the active uplink with a weight of 20 will have more sessions assigned.
   - **Uplink utilization**—Select this option to distribute traffic between active WAN uplinks based on the utilization % of each active WAN uplink. Uplink utilization considers the link speed to calculate the utilization and allows a maximum percentage of bandwidth threshold to be defined. When the bandwidth threshold exceeds the defined value, the WAN uplink will no longer be considered for session allocation. When you configure WAN ports, it is important that you configure the WAN uplink speed appropriately.
5. Click **Next**.

   The **WAN Details** page is displayed. This section defines uplink interfaces by creating WAN-facing VLANs, labeling them as uplink interfaces, and assigning them to the desired uplink ports.
6. Turn on **Enable HA deployment** toggle switch to deploy LAN redundancy.
7. To add a WAN port, click the **+** icon in the **WAN Uplinks/Ports** table.

   The **New WAN Uplink / Port** pop-up is displayed.
8. Enter a name for the WAN port in the **Uplink** field.
9. Select the **WAN type** from the drop-down list; for example, Internet, MPLS, or Metro-Ethernet.
10. Configure the **WAN speed**. By default, the WAN uplink speed is set to 20 Mbps. You can configure a custom value for uplink speed as per your requirements. The allowed range of values is 1–10000 Mbps.
11. To enable NAT for the outbound traffic on the WAN interface, select **Source NAT**.
12. To use the uplink in the standby mode, select the **Use as backup** check box. By default, all uplinks operate as active uplinks.
13. Select an **IP addressing method** from the following options :
    - **Static**—For static IP addressing method, enter the IPv4 address.
    - **DHCP**—If you select this option, the IP address is dynamically assigned from a DHCP pool for the WAN uplink.
    - **PPPOE**—This is the Point to Point Protocol over Ethernet (PPPOE). When selected, you need to select an authentication type to connect to the ISP.
      - Turn on the **Group credentials** toggle switch.
      - Select an **Authentication type**. If you select Password Authentication Protocol (**PAP**), enter the username and password for PPPoE authentication. If you select Challenge handshake authentication protocol (**CHAP**), enter the user name and CHAP secret for authentication.
14. Select a port from the **Port** drop-down list.
    a. If you select **LTE**, the **WAN type** field displays **Cellular**.
    b. Select the connection type (**Internal** or **USB**) in the **Cellular type** drop-down list.
15. To apply the default inbound security ACL for WAN ports, select the **Secure with ACL** check box.
16. Click **Next**.

17. Review the summary page and click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

18. Click **Continue** to configure VPN hubs and routing profiles.

Configuring VPN Hubs and Routing Profiles for a Branch Gateway Group

To configure VPN hubs and routing profiles, complete the following steps:

1. In the **DC Preference** page, click the **+** icon in the **DC Preference** table.
2. Add a **VPN Hub Group**.
3. Select a primary and secondary VPNC from the respective drop-down list.
4. Review the overlay topology configuration.
5. Click **Next**.

   The **Static Routing** page is displayed.
6. To create a default route, click the **+** icon in the **Default Routes** table and configure the following parameters:
   - **Type**—Select the default route type; **Nexthop** or **VPNC**.
   - **Next Hop/VPNC**—Enter the IP address of the Next Hop or VPNC.
   - **Uplink**—Select the uplink from the drop-down list.
   - **Cost**—The cost metric of the route.
7. To create a static route, click the **+** icon in the **Static Routes** table:
   - **Destination IP**—The destination IP address.
   - **Destination Mask**—The subnet mask of the destination IP address.
   - **Type**—Select the type of route.
     - **Nexthop**—Select this option to configure a nexthop destination.
     - **Blackhole**—Select this option to route packets to a Blackhole. Blackholes refer to places in the network where incoming or outgoing traffic is discarded (or dropped), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic.
   - **Next Hop**—The IP address for the next hop.
   - **Cost**—The cost metric for the route.
8. Click **Next** to configure an **Overlay Routing** profile.
9. To allow Branch Gateways to **Redistribute connected vlans** to hubs, select the VLANs to be advertised.
10. To allow Branch Gateways to redistribute static routes, select the **Redistribute static routes** check box.
11. Click **Next**.

12. Review the summary page and click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

13. Click **Continue** to configure security and traffic steering policies.

Configuring Policies for a Branch Gateway Group

In the **Policies** tab, you can configure the following types of policies on Branch Gateway groups:

- Role assignment policy—Policy for determining client access based on the user roles assigned to a client.
- Application usage policy—Policy for deep packet inspection of application usage by clients.
- Traffic steering policy—Policy for dynamically steering client traffic to best performing uplink.
- QoS policy—Quality of service (QoS) policy allows you to prioritize critical traffic, prevent bandwidth hogging, and manage network bottlenecks to prevent packet drops.
- Security policy—Firewall policies website content filtering.

Configuring a Role Assignment Policy

To configure a role assignment policy, complete the following steps:

1. In the **Policies** > **Roles** page of the Guided Setup wizard, click the **+** icon to add a user role in the **Roles** table. The policies that are associated to this role are configured in subsequent steps.
2. Click the **+** icon in the **Role assignment** table.
3. Select a VLAN ID to which this role needs to be applied, from the **VLAN ID** drop-down list.
4. Select a role from the **Initial role** drop-down list. This is the default user role that would be assigned to the clients connecting through this VLAN.
5. To enable authentication, turn on the **Authentication** toggle switch.
6. Select the **Default authentication role** from the drop-down list.
7. Select one of the following authentication modes:
   - **MAC authentication**—Select this check box to assign a role after a client device completes MAC authentication. The default role for MAC authentication is the **guest** user role.
   - **802.1X authentication**—Select this check box to assign a role after a client device completes 802.1X authentication. You can also enable MAC authentication fail through to allow clients to complete 802.1X authentication when MAC authentication fails and vice-versa.
8. Configure primary and backup authentication servers. This configuration defines them as Authentication, Accounting and CoA (RFC3676) servers.
9. To add a AAA server, click the **+** icon in the **Select AAA servers** table and configure the following parameters:
   - **Name**—The server name.
   - **Server IP**—The IP address or FQDN of the server.
   - **Password**—The password to use for authentication.
   - **Retype Password**—Confirm password.
10. Click **Save**.
11. Click **Next** to configure application policies.

Configuring Applications

To define applications, and other security aliases, complete the following steps:

1. In the **Policies** > **Applications** page of the Guided Setup wizard, view the list of applications and application categories available for Branch Gateways to create a policy.
2. Click the **+** icon in the **Applications** table and configure the following parameters:
   - **Name**—Enter the name of the application.
   - **Category**—Enter the application category.
   - In the **Servers** table, click the **+** icon to add the server name and the URI that the application uses.
3. View the list of network aliases that are available on Branch Gateways. To create a network alias, click the **+** icon in the **Network Aliases** table and configure the following parameters:
   - **Name**—Enter a name of the network alias.
   - **Description**—Enter description text for the alias.
   - **Invert**—Select this check box if you want to apply the firewall rules to all the destinations except the one configured in the alias.
   - **User Rules**—Click the **+** icon to add user rules. The following rule types are available:
     - **Host**—Allows you to configure a rule for a specific host IP address.
     - **Name**—Allows you to configure a rule for a specific domain name.
     - **Range**—Allows you to configure a rule for a range of IP addresses.
     - **Network**—Allows you to configure a rule for a specific network IP address and subnet mask.
     - **Override VLAN**—Allows you to configure a rule for overriding a specific VLAN.
     - **Override Host**—Allows you to configure a rule for overriding a specific host.
4. Click **Save**.
5. View a list of service aliases available on Branch Gateways. To create a service alias, click the **+** icon in the **Service Aliases** table and configure the following parameters:
   a. Enter a value in the **Service name** field.
   b. In the **Protocol** drop-down list, select one of the following options:
      - **TCP**
      - **UDP**
      - **Protocol**
   c. If you select **Protocol**, enter the IP protocol number in the **Protocol number** field.
   d. If you select **UDP** or **TCP**, in the **Port type** drop-down list, select one of the following options:
      - **Range**—If you select **range** to provide a contiguous list of ports, enter the starting and ending port numbers in the **Start port** and **End port** fields, respectively.
      - **List**—If you select **List**, enter a comma-separated list of port numbers in the **Port list** field.
   e. To limit the service alias to a specific application, select a service type from the **ALG** (Application Level Gateway) drop-down list.
6. Click **Save**.
7. Click **Next** to add a traffic steering policy.

Configuring a Traffic Steering Policy

To configure a traffic steering policy, complete the following steps:

1. In the **Policies** > **DPS** page of the Guided Setup wizard, view the list of default traffic policies. If you want to create a new traffic steering policy.
2. Click the **+** icon in the **Policies** table.
3. Select **DPS** or **SAAS** in the **Policy Type** drop-down list.
4. If you have selected **SAAS**, select the **Application** in the drop-down list.

5. If you have selected **DPS**, enter the name of the policy and click **Save**.
6. In the **Policies** table, select the policy for which you want to set rules.
7. In the **Traffic Rules for <Policy name>** table, click the edit icon to create traffic specification rules for the policy, and configure the following parameters.
   - **Source**—Select one of the following options from the drop-down list to define a source point for the traffic policy rule:
     - **Any**—Applies rule to incoming traffic from any source.
     - **Host**—Applies rule to traffic originating from a specific host IP address. Enter the host IP address.
     - **Network**—Applies rule to the traffic that originates from a specific network. Enter the IP address and the subnet mask of the source network.
     - **Alias**—Applies rule to the traffic originating from an alias of a host or network. Select the **Source alias** from the drop-down list.
     - **User Role**—Applies rule to traffic originating from a specific user role. Select a user role from the default list, or create a custom role.
   - **Destination**—Select one of the following options to define a destination for the traffic policy rule:
     - **Any**—Applies rule to the outgoing traffic to any destination.
     - **Host**—Applies rule to the traffic routed to a specific host IP address. Enter the host IP address.
     - **Network**—Applies rule to the traffic routed to a specific network. Enter the IP address and the subnet mask of the source network.
     - **Alias**—Applies rule to the traffic routed to a specific alias of a host or network. Select the **Source alias** from the drop-down list.
   - **Application/Port**—Select one of the following options for application or port:
     - **Application**—Applies rule to the selected applications.
     - **Application categories**—Applies rule to the selected application categories.
     - **Web Categories/Reputations**—Applies rule to the selected web category based on reputation.
     - **Service**—Applies rules to the selected services.
     - **TCP**—Applies rules for the source and the destination ports.
     - **UDP**—Applies rules for the source and the destination ports.
     - **Any**—Applies the policy to all applications and application service ports.
8. Click **Save**.
9. Review the default SLAs available for the traffic policy. To create an SLA profile, click the edit icon in the **SLA** table.

   The default list of SLA profiles is displayed. The default SLA profiles include **BestForInternet**, **BestForVoice**, **BestForSaas**, and **HighlyAvailable**. The threshold set in these profiles are just placeholders and should be taken as best-practice values.

The default SLA profile for SaaS policies is BestForSaaS.

10. Click the **+** icon to create a new SLA profile and configure the following parameters:
    - **Name**—Name of the SLA profile.
    - **Latency (MS)**—The latency threshold in milliseconds to measure the round-trip ping time.

- **Jitter (MS)**—The jitter threshold value in milliseconds to measure if the packets are delivered in a proper order.
- **Loss (%)**—The percentage of packet loss allowed.
- **Utilization (%)**—The percentage of bandwidth utilization as a metric to prioritize and load-balance the traffic.

11. For **DPS** policies, If you want to enable FEC, select the **Loss Correction (FEC)** check box.
12. Enter the FEC threshold in percentage in the **Loss % with FEC** field.
13. Select the **FEC Ratio** from the drop-down list.
14. Click **Save**.
15. To create a new WAN uplink path profile, click the edit icon in the **WAN Path** table for DPS policies or click the edit icon next to **Exit Profile:<SLA Name>** for SAAS polices and configure the following parameters:
    - **Primary path**—Select a primary uplink path. For example, if you are configuring policies for critical traffic such as voice or VOIP, you can set MPLS as the primary path. The list shows uplinks configured on Branch Gateways. You can select multiple uplinks in a sequential order.
    - **Secondary path**—Select a secondary uplink path to route traffic through the secondary path in the event of failover or for load balancing. The session continues on the link as long as it is good irrespective of the status of the primary uplink. When a primary path becomes active and meets the configured SLA, the new sessions are steered back to the primary path.
    - **Last resort path**—Select a last-resort uplink path to route traffic through another path as a last attempt (when both primary and secondary paths are down). When a session is steered to a tertiary path, it stays on the link until the end. When a primary path becomes active and meets the configured SLA, the new sessions are steered back to the primary path.

The default exit profile for SaaS policies is BestforSaaS.

16. Click **Save**.
17. Click **Next** to configure QoS policies.

Configuring a QoS Policy

To configure a QoS policy, complete the following steps:

1. In the **Policies** > **QOS** page of the Guided Setup wizard, review the bandwidth contracts, and QoS priorities assigned for each role or an application.
2. To edit the QoS for a user role, select the user role in the **Roles** table. Click the **+** icon in the **QOS for <role name>** table and configure the following parameters:
    a. **Type**—Select the policy type as Application or Application Category from the drop-down list.
        - Enter the **Application** or **Application category** based on the policy type that is selected.
    b. **QOS Profile**—Select one of the following from the drop-down list for QoS profile:
        - **Realtime**—Select this option if the policy applies to realtime, delay-sensitive data transmission such as audio and video conferencing.
        - **Transactional**—Select this profile for applications such as SAP, PeopleSoft where the response time required is more than the generic client-server applications.
        - **Collaboration**—Select this option for highly interactive applications that require user feedback such as Instant Messaging applications.

- **Best effort**—This profile is used for majority of the data traffic unless the data requires a preferential treatment.

c. **Upstream bandwidth**—Define the upstream bandwidth in Mbits or Kbits.
d. **Downstream B/W**—Define the downstream bandwidth in Mbits or Kbits.

3. Click **Save**.
4. Click **Next** to configure security policies.

You can view the DSCP marking for individual QoS profiles in the **Show QOS Profiles** table.

Configuring Security Policies

To configure **Security Policies**, complete the following steps:

In the **Policies** > **Security Policies** page of the Guided Setup wizard, view the list of roles and policies.

1. To add a role, click the **+** icon in the **Roles** table.
2. To add a policy to a role, select a role type and click the **+** icon in the **Policies** table.
3. To add an access rule to a policy, select a policy and click the **+** icon in the **Rules** table and configure the following parameters:
   - **Source** —Select one of the following options from the drop-down list to define the source of the traffic:
     - **Any**—Applies a rule to incoming traffic from any source.
     - **User**—Applies a rule to the traffic originating from a specific user.
     - **Host**—Applies a rule to traffic originating from a specific host IP address. Enter the host **IP** address.
     - **Network**—Applies a rule to the traffic that originates from a specific network. Enter the **IP** address and the subnet **Mask** of the source network.
     - **Network Alias**—Applies rule to the traffic routed to a specific alias of a host or network. Select the **Source alias** from the drop-down list.
     - **Role**—Applies a rule to traffic originating from a specific user role. Select a **User role** from the drop-down list.
   - **Destination**—Select one of the following options from the drop-down list to define a destination for the traffic policy rule:
     - **Any**—Applies a rule to the outgoing traffic to any destination.
     - **User**—Applies a rule to the traffic from a specific user.
     - **Host**—Applies a rule to the traffic routed to a specific host IP address. Enter the host IP address.
     - **Network**—Applies a rule to the traffic routed to a specific network. Enter the IP address and the subnet mask of the source network.
     - **Network Alias**—Applies rule to the traffic routed to a specific alias of a host or network. Select the **Source alias** from the drop-down list.
     - **Role**—Applies a rule to traffic outgoing from a specific user role. Select a **User role** from the drop-down list.

- **Service/App**—Select one of the following network services from the drop-down list :
  - **Any**—Applies a rule to all network services.
  - **TCP**—Applies a rule to the incoming and outgoing traffic from the TCP ports. If you have selected the TCP service, specify a list of TCP ports. Select **Min/Max Port** radio-button to specify the start and end port or select the **Source/Dest Port** radio-button to specify the source and destination ports.
  - **UDP**—Applies a rule to the incoming and outgoing traffic from the UDP ports. If you have selected the UDP service, specify a list of UDP ports. Select **Min/Max Port** radio-button to specify the start and end port or select the **Source/Dest Port** radio-button to specify the source and destination ports.
  - **Service**—Applies a rule to the incoming and outgoing traffic from a set of predefined services and protocols; for example, HTTPS and HTTP. Select the **Service Alias** from the drop-down list.
  - **Protocol**—Applies a rule to the traffic that uses a specific routing protocol. Enter the protocols in the **Protocol** field.
  - **Application**—Applies rule to the applications. Enter the application names in the **Application** field.
  - **Application category**—Applies rule to the application categories. Enter the Application Categories in the **App category** field.
  - **Web Category/Reputation**—Applies rule to the web category. Enter the web categories in the **Web Category** field and select the **Web reputation** from the drop-down list.
- **Action**—Select one of the following options from the drop-down list:
  - **Deny**—Denies traffic from or to a specific network or network service.
  - **Permit**—Allows traffic from or to a network or network service.
  - **Log**—Creates a log when a policy is applied based on the rules configured.
  - **Mirror**—Mirrors session packets to datapath or remote destination.

4. Click **Save**.
5. Click **Next** to view a summary of the policies.
6. Click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to save your configurations.

Configuring Branch Gateways Using the Guided Setup

Aruba Branch Gateways operate at the branch to optimize and control WAN, LAN, and cloud security services. The Branch Gateway provides essential features such as routing, firewall, security, website content filtering, and WAN compression. With support for multiple WAN connection types, the Branch Gateway routes traffic over the most efficient link that is based on availability, application, user-role, and link health. It allows organizations to take advantage of high-speed, low-cost broadband links to supplement or replace traditional WAN links such as MPLS.

You can configure a Branch Gateway group or Branch Gateway device using either the Guided Setup, Basic mode, or Advanced mode. This section describes the procedure to configure Branch Gateways using the Guided Setup.

Before You Begin

Ensure that you have completed the following procedures:

- Gateways are onboarded to Aruba Central.
- Gateways are assigned valid subscriptions in Aruba Central.
- Gateways are assigned to groups.
- Gateways are assigned the Branch Gateway group role.

Configuring a Branch Gateway Device in the Guided Setup

To configure a Branch Gateway device, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.

If you are accessing the Branch Gateway configuration page for the first time, the **Guided Setup** wizard opens automatically. Otherwise, click the **Guided Setup**.

The **Guided Setup** wizard displays the following tabs for device level configuration:

1. **System**—Allows you to configure the system IP address.
2. **LAN**—Allows you to configure LAN ports.
3. **WAN**—Allows you to modify WAN ports.
4. **SDWAN & Routing**—Allows you to configure SD-WAN routing profiles.
5. **Redundancy**—Allows you to configure LAN redundancy for high availability of the SD-Branch devices.
6. Click **Begin** to start the guided setup process and complete the steps provided in the following sections:
   - Configuring a System IP Address for a Branch Gateway
   - Configuring a LAN Interface for a Branch Gateway
   - Configuring a WAN Interface for a Branch Gateway
   - Configuring Routing Profiles for a Branch Gateway
   - Configuring LAN Redundancy for High Availability

Many procedures involve adding or configuring parameters in tables. Note that you have options to edit and delete the existing configurations.

Configuring a System IP Address for a Branch Gateway

Each Branch Gateway requires a unique system IP address that is used by the gateway to communicate with network services such as VPN, RADIUS, Syslog, TACACS+ and SNMP. The system IP addresses for your

gateways can be assigned from the group using a pool or a per device or a bulk configuration upload.

To configure a system IP for a Branch Gateway device:

1. Click the **System IP** tab in the **Guided Setup** wizard.
2. Configure the following parameters:
   - If you have configured the system IP address pool for VLAN 4087, which is the reserved system VLAN and a Controller IP VLAN, then the **VLAN Interface** is a read-only field that displays **VLAN 4087**.
   - If you have defined a system IP address pool during group configuration, complete the following step:
     - **VLAN Interface**—Select the VLAN interface from the drop-down list to assign an IP address to the Branch Gateway.
   - If you have not configured a system IP address pool during group configuration, complete the following steps:
     - **IPv4 Address**—Enter the IP address for the gateway.
     - **Netmask**—Enter the subnet mask of the system IP address.
   - **Specify interface for this device**—Select this option to assign IP address from a specific VLAN interface to the Branch Gateway. When you select this option, ensure that you select the VLAN interface for IP address assignment.
   - **Use IP address assigned by group**—Select this option to assign an IP address from the address pool configured for the Branch Gateway group.
3. Click **Next**.
4. Enter the host name in the **Hostname** field.
5. Click **Next**.
6. Review the summary page and click **Finish**.

The Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

7. Click **Continue** to configure a LAN interface.

Configuring a LAN Interface for a Branch Gateway

This section focuses on the LAN configuration of the Branch Gateways. By default, LAN interfaces have LLDP enabled and a role-based security. However, this setting can be changed when you configure security policies.

To configure VLANS on Branch Gateway group:

1. In the **VLAN** page, select the **IP DHCP server** check box for the gateways to act as DHCP servers.
2. Click the **+** icon in the **VLANs** table to add a new VLAN.
3. Enter a **Name** for the VLAN.
4. Enter the **VLAN ID**.
5. Select one of the following **IP addressing mode** from the drop-down list:
   - **Static**—Select this option to use a static IP address. If you want to configure the LAN IP addresses at the device level, leave the IPv4 address and netmask fields empty. You can also set the same static IP/netmask for all the devices in the group.

- **IPV4 Address**—Enter a unique static IP address for each gateway in the group or a common address for all gateways in the group.
- **Netmask**—Enter the subnet mask of the IP address.

Ensure that the VLAN used here is configured as a non-routable VLAN, as the VLAN overlaps with the other gateways.

6. To configure branch gateways as DHCP server, turn on the **Act as DHCP server** toggle switch and configure the following parameters:
   - **Network**—The network IP address.
   - **Netmask**—The subnet mask of the network.
   - **Default Router**—The IP address of the device used by clients if they want to communicate with devices outside of their subnet. By default, this is the Branch Gateway IP address for the particular VLAN, or the VRRP virtual IP, if configured.
   - **Reserve first**—The first IPv4 address for the CIDR range.
   - **Reserve last**—The last IPv4 address for the CIDR range.
   - **Domain name**—The DNS domain name assigned to branch devices.
   - **DNS server type**—Type of the DNS server. You can use either a public DNS server or add a DNS server by selecting the **User Defined** DNS option.
     - **DNS Service Provider**—If you use a **Public DNS Service**, select the name of the DNS service provider from the list. For example, Google.
     - **DNS server IPv4 addresses**—If you use a **User Defined** DNS server, enter the IP addresses here. You can specify up to eight IP addresses separated by a comma.
7. Turn on the **Enable DHCP relay** toggle switch to relay the incoming DHCP requests to an external DHCP server. Select this option when centralized DHCP servers are deployed to provide addressing to branch devices or if device profiling is performed by services such as Aruba ClearPass.
   a. Click the **+** icon in the **External DHCP Server** table.
   b. Add the IPV4 addresses.
8. Click **Save**.
9. Click **Next**.

   The **LAN Ports** page is displayed.
10. To add a LAN port, click the + icon in the **LAN Ports/Port Channel** table.
11. Enter a **Name** for the port.
12. Select a port channel or a port from the **Ports** drop-down list.
    - If you have selected **Port Channel** for the LAN port, configure the following parameters:
      - **Port channel protocol**—Select a port channel protocol; for example, LACP (Link Aggregation Control Protocol). If you have selected LACP, select the LACP mode as active or passive from the **LACP mode** drop-down list.
      - **Port channel members**—Select the port channel members.
13. Select one of the following **VLAN mode**s:
    - **Access**—Select this option to allow the LAN port to carry traffic only for the VLAN to which they are assigned. All transmitted and received traffic on the port is untagged.
      - **Access VLAN**—Select the VLAN ID assigned to the port or port channel.
    - **Trunk**— Select this option to allow the LAN port to carry traffic for multiple VLANs. If you select the **Trunk** mode, configure a list of allowed VLANs.

- **Native VLAN**—The untagged VLAN ID for the port or port channel.
- **Allowed VLAN**—The range of VLAN IDs assigned to the port or port channel including the Native VLAN.

14. Click **Save**.
15. Click **Next**.
16. Review the summary page and click **Finish**.

The Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

17. Click **Continue** to configure a WAN interface.

Configuring a WAN Interface for a Branch Gateway

This section focuses on the WAN configuration of the branch gateways.

To configure a WAN interface, complete the following steps:

1. In the **WAN** tab, turn on the **Enable health checks** toggle switch.

The WAN health check enables sending probes to measure availability and SLA of the uplinks. When the health check feature is enabled, the probes are sent through the underlay at regular intervals to verify if the Internet is reachable over the uplink interfaces configured on Gateways.

2. Configure the following health check parameters:
   - **Health check destination**—You can configure a **User defined** IP address or use the default **Aruba cloud** instance to send WAN health check probes.
     - **Health check IP address**—If it is a **User defined** destination, enter the IPv4 address or FQDN of a host that is reachable through the WAN paths outside the VPN tunnel.
   - **Health check probe mode**—Select one of the following probe modes:
     - **Ping**—Sends ICMP probes to measure latency and packet loss.
     - **UDP**—Sends UDP Probes through UDP port 4500 to measure latency, packet loss, and jitter.
3. Click **Next**.

   The **Load Balancing** page is displayed.
4. Select one of the following modes for uplink load balancing:
   - **Round robin**—Select this option to sequentially distribute outgoing sessions between WAN links. It is the simplest algorithm to configure and implement, but may result in uneven traffic distribution over time.
   - **Session count**—Select this option to balance traffic among the uplinks based on the current number of active sessions managed by each link, so that the load for each active uplink stays within 5% of the other active uplinks. For example, if there are two active uplinks with the **Weight** parameter defined as 10 and 20, the active uplink with a weight of 20 will have more sessions assigned.
   - **Uplink utilization**—Select this option to distribute traffic between active WAN uplinks based on the utilization % of each active WAN uplink. Uplink utilization considers the link speed to calculate the utilization and allows a maximum percentage of bandwidth threshold to be defined. When the bandwidth threshold exceeds the defined value, the WAN uplink will no longer be considered for

session allocation. When you configure WAN ports, it is important that you configure the WAN uplink speed appropriately.

5. Click **Next**.

   The **WAN Details** configuration page is displayed. This section defines uplink interfaces by creating WAN-facing VLANs, labelling them as uplink interfaces, and assigning them to the desired uplink ports.
6. Turn on the **Enable High Availability deployment** toggle switch for LAN redundancy.
7. Select the **Peer gateway** from the list.
8. Enter the **Site ID** to which the peer gateway belongs.
9. Click **Next**.
10. To add a WAN port, click the **+** icon in the **WAN Uplinks/Ports** table.

    The **New WAN Uplink / Port** pop-up is displayed.
11. Enter a name for the WAN port in the **Uplink** field.
12. Select the type of WAN uplink to use from the **WAN type** drop-down list. For example, Internet or MPLS.
13. Configure the **WAN Speed**. By default, the WAN uplink speed is set to 20 Mbps. You can configure a custom value for uplink speed as per your requirements. The allowed range of values is 1–10000 Mbps.
14. To enable NAT for the outbound traffic on the WAN interface, select **Source NAT**.
15. To use the uplink in the standby mode, select the **Use as backup** check box. By default, all uplinks operate as active uplinks.
16. Select an **IP addressing method** from the following options :
    - **Static**—For static IP addressing method, enter the IP address and subnet mask.
    - **DHCP**—When selected, the IP address from a DHCP pool is assigned for the WAN uplink.
    - **PPPOE**—This is the Point to Point Protocol over Ethernet. When selected, you need to select an authentication type to connect to the ISP.
    - Turn on the **Group credentials** toggle switch.
    - Select an **Authentication type**. If you select Password Authentication Protocol (**PAP**), enter the username and password for PPPoE authentication. If you select Challenge handshake authentication protocol (**CHAP**), enter the user name and CHAP secret for authentication.
17. To apply the default inbound security ACL for WAN ports, select the **Secure with ACL** check box.
18. Click **Save**.
19. Click **Next**.
20. Review the summary page and click **Finish**.

The Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

21. Click **Continue** to configure routing profiles.

Configuring Routing Profiles for a Branch Gateway

To configure a routing profile on a Branch Gateway device:

1. In the **SDWAN & Routing** tab, configure a **Static Routing** profile.
2. To create a default route, click the **+** icon in the **Default Routes** table:
   - **Type**—Select the default route type; **Next Hop** or **VPNC**.
   - **Next Hop/VPNC**—Enter the IP address of the Next Hop or VPNC.
   - **Uplink**—Select the uplink from the drop-down list.
   - **Cost**—Enter the cost metric of the route.
3. To create a static route, click the **+** icon in the **Static Routes** table and enter the following:
   - **Destination IP**—Enter the destination IP address.
   - **Destination Mask**—Enter the subnet mask of the destination IP address.
   - **Type**—Select the type of route.
     - **Nexthop**—Select this option to configure a nexthop destination.
     - **Blackhole**—Black holes refer to places in the network where incoming or outgoing traffic is discarded (or dropped), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic.
   - **Next Hop**—The IP address for the next hop.
   - **Cost**—The cost metric for the route.
4. Click **Next**.
5. Review the summary page and click **Finish**.
6. Click **Continue** to configure LAN redundancy for high availability.

Configuring LAN Redundancy for High Availability

Before you proceed, ensure that you have enabled High Availability on the WAN page and configured peer gateway for redundancy.

To configure LAN redundancy, complete the following steps:

1. In the **Redundancy** > **VRRP** page, configure a VRRP instance.
2. Click the **+** icon in the **VRRP Interfaces** table and configure the following parameters:
   - **VLAN ID**—VLAN ID for which you want to set up the redundant gateway.
   - **IP Address on Local**—The IP address of the VLAN on the local gateway.
   - **IP Address on Peer**—The IP address of the VLAN on the peer gateway.
   - **Virtual IP**—The virtual IP of the VLAN.
   - **Conductor** —The designated active gateway of the redundant pair.
3. Review the WAN port sharing details for the peer Gateways.
4. Click **Next**.

   The VRRP Instance configuration page is displayed.
5. Click **Finish** to apply the settings.

Configuring VPNC Group Using the Guided Setup

Aruba Gateways deployed at a data center can function as a headend Gateway or a VPNC. The VPNCs aggregate traffic from all branch offices. Branch Gateways (BGWs) establish secure Internet Protocol security (IPsec) tunnels to one or more headend gateways over the Internet or other untrusted networks.

You can configure a VPNC group using the Guided Setup, Basic mode, or Advanced mode. This section describes the procedure for configuring VPNCs using the Guided Setup.

Before You Begin

Before you begin, ensure that you have completed the following procedures:

- Gateways are onboarded to Aruba Central.
- Many procedures involve adding or configuring parameters in tables. Note that you have options to edit and delete the existing configurations.
- Gateways are assigned valid subscriptions in Aruba Central.
- Gateways are assigned to groups.
- Gateways are assigned the VPNC group role.

NOTE

Ensure that the devices in the group are not running the guided setup at device level. If the device is being configured using the Guided Setup, the group level setup will not be executed.

Configuring a VPNC Group in the Guided Setup

To configure a VPNC group using the Guided Setup, perform the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway that is configured as a VPNC.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.

   The gateway group configuration page is displayed.

   The **Guided Setup** wizard displays the following tabs:
   - **System**—Allows you to configure system parameters.
   - **LAN**—Allows you to configure LAN interfaces.
   - **SDWAN & Routing**—Allows you to configure the SDWAN overlay and routing profiles.
4. Click **Begin** to start the guided setup process and complete the steps provided in the following sections:
   - Configuring System Parameters for a VPNC Group
   - Configuring a VLAN Interface for a VPNC Group
   - Configuring VPN Routing Profiles for a VPNC Group (Static Routing)

NOTE

Many procedures involve adding or configuring parameters in tables. Note that you have options to edit and delete the existing configurations.

Configuring System Parameters for a VPNC Group

To configure system parameters, complete the following steps:

1. In the **System** tab, navigate to the **Model** page.
2. Select a model from the **VPNC Model** drop-down list.

3. Click **Next**.

   The **Time** page is displayed.

   Configure the NTP server for system clock synchronization. The system automatically updates the time zone including the relevant daylight savings time (DST) across time zones. You can optionally specify a time zone which is applied to all the gateways in the group. The default time zone is set to GMT.

4. In the **Public NTP Servers** table, click the **+** icon to add a Public NTP Provider:
   - **IPV4 Address/FQDN**—Enter the IPV4 address or the FQDN of the public NTP provider. The provider's NTP server is automatically added to the Branch Gateways in the group.
   - **Burst Mode**—Select this option to expedite the system clock calibration.
   - **Timezone**—Choose the time zone from the drop-down list. The list contains the list of **Primary** time zones followed by other time zones.
5. Click **Next**.

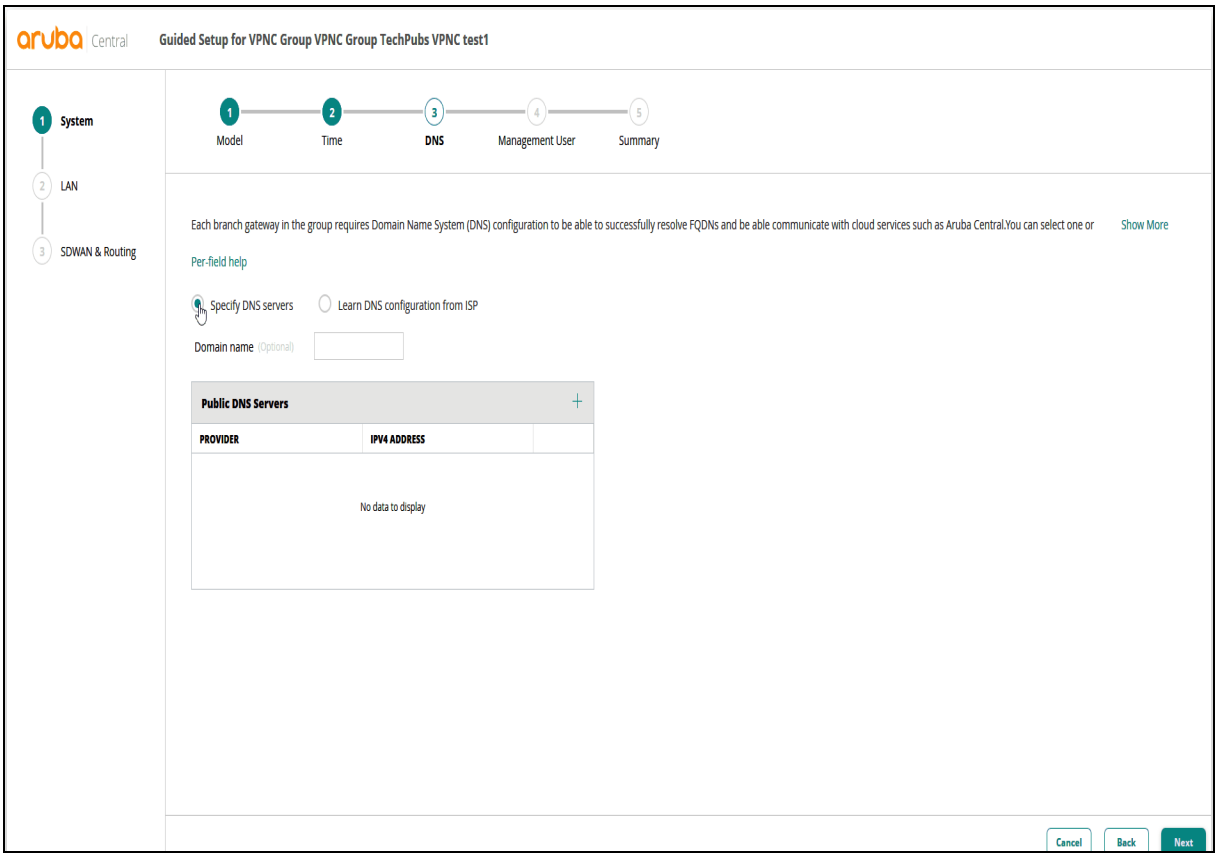
   The **DNS** page is displayed.
6. Select one of the following options to configure DNS server:
   - **Specify DNS servers**—Select this option to configure a DNS server and define the following parameters:
     - Enter a **Domain name**.
     - Click the **+** icon to add a **Public DNS servers**. You can select one or more DNS service providers from the list or you can select **User Defined** from the **Provider** drop-down list.
     - Enter the **IPv4 address** if you have selected **User Defined** from the **Provider** drop-down list. If you select a DNS provider from the **Provider** drop-down list, the **IPv4 Address** is auto populated.
   - **Learn DNS server from ISP**—Select this option if you want the gateway to learn the DNS server dynamically from the ISP.

The DNS servers configured here are the ones that the gateway uses to resolve addresses. It must be reachable through the underlay, as it is required by the device to communicate with and the SD-WAN Orchestrator.

   - Click **Next**.

     The **Management User** page is displayed.

Figure 176 *Configuring DNS*



A management user has administrative credentials to log in to the local management interface of the device.

1. Enable **AAA Authentication** for an admin user, to centrally manage user authentication using RADIUS or TACACS servers.
2. Click the **+** icon to create an AAA server for authenticating device management user.

   The **Add AAA Server** pop-up is displayed.

   Configure the following parameters:
   - **Name**—Name of the authentication server.
   - **Server IP**—IP address of the authentication server.
   - **AAA authentication**—Authentication protocol to use; for example, **TACACS** or **RADIUS**.
   - **Key**—Shared key for authenticating a device administrator.
   - **Retype key**—Reenter the key to confirm.
3. Click **Save**.
4. To add a local user, click the **+** icon in the **Local Management Users** table.

   The **Add Management User** pop-up is displayed.

   Configure the following parameters:
   - **Name**—Enter the username of the management user.
   - **Password**—Enter the password for the management user.
   - **Retype Password**—Enter the password for the management user.

- **Role**—Set the role of the management user. Select a user role from the **Role** drop-down list. The following options are available:
  - **Super user role**—Administrator user role.
  - **Guest provisioning role**—Administrator role for provisioning guest users.
  - **Network operations role**—Administrator role for managing SD-WAN deployments.
  - **Read-only**—Read-only user role.

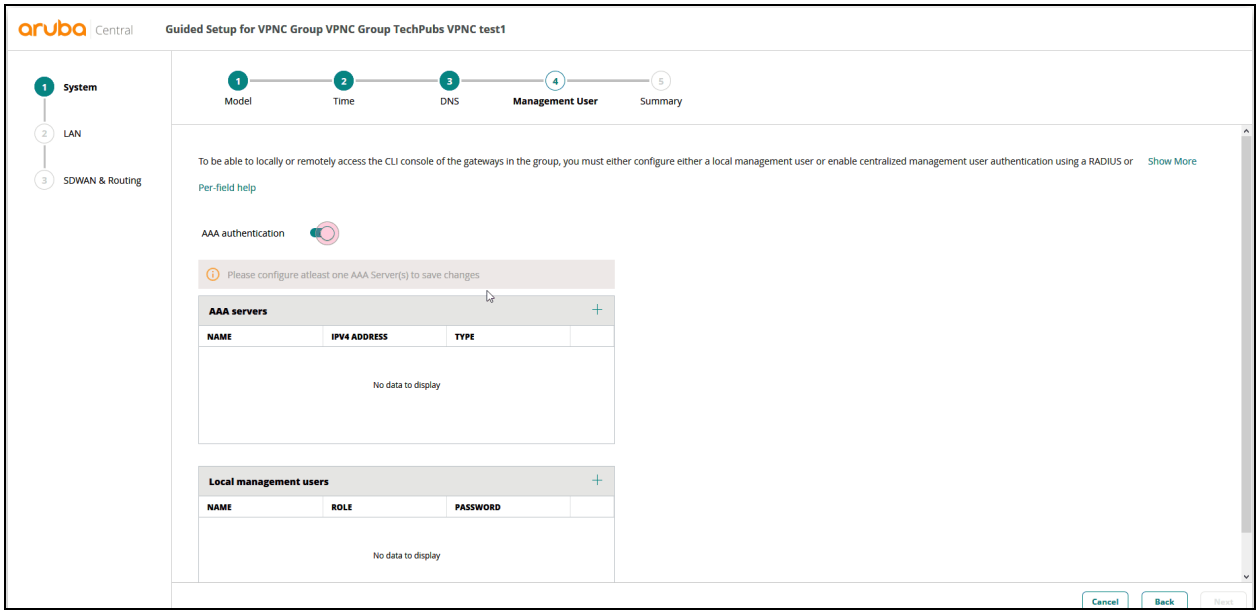
5. Click **Save**.
6. Click **Next** to view the system configuration summary, and then click **Finish**.

NOTE

The **Finish** button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

7. Click **Continue** to configure VLANs and LAN Ports for VPNCs.

Figure 177 *Configuring Management User*



Configuring a VLAN Interface for a VPNC Group

This section focuses on the LAN configuration of the VPNC group.

To configure VLANs on VPNC groups, complete the following steps:

1. In the **VLAN** tab, click the **+** icon in the **VLANs** table to add a new VLAN.
2. Configure the following parameters:
   - Enter a **Name** for the VLAN.
   - Enter the **VLAN ID**.
   - Enter a description text for the VLAN.
   - Enter a unique **IPv4 address**.
   - Enter the **Netmask**.
3. Click **Save**.

4. Click **Next**.

   The **LAN ports** page is displayed.

To configure LAN Ports for VPNC groups, complete the following steps:

1. To add LAN ports or a port channel, click the **+** icon in the **LAN Ports/Port Channel** table.
2. Specify an unique **Name** for the LAN port.
3. Select an unused **Port** from the list of available ports.
4. Select either **Access** or **Trunk**from the **VLAN mode** drop-down list.
   - **Access**—Select this option to allow the LAN port to carry traffic only for the VLAN to which they are assigned. All transmitted and received traffic on the port is untagged. In Access mode, the port or port-channel is assigned a single LAN VLAN ID (Access VLAN).
   - **Trunk**— Select this option to allow the LAN port to carry traffic for multiple VLANs. Traffic transmitted and received on the Native VLAN will be untagged, while traffic transmitted and received from other VLANs in the Allowed VLANs list will be 802.1Q tagged. In Trunk mode, the port or port-channel can be assigned to multiple LAN VLAN IDs. If you select the **Trunk** mode, configure a list of allowed VLANs. The following options are available:
     - **Native VLAN (Optional)**—This is the untagged VLAN ID for the port or port channel.
     - **Allowed VLAN (Optional)**—This is the range of VLAN IDs assigned to the port or port channel. This range includes the native VLAN.
   - If you have selected **Port Channel** for the LAN port, configure the following parameters:
     - **Port channel protocol**—Select a port channel protocol; either: **Static** or **LACP**. The gateways support **Static** and **LACP** (Link Aggregation Control Protocol) protocols. Select the protocol based on the port channel configuration of the upstream device.
     - **Static**—Allows manual bundling of links. The link state of the port determines if the port is an active member of the port-channel bundle.
   - **LACP**—Link Aggregation Control Protocol allows devices to negotiate an automatic bundling of links by sending LACP BPDUs to the peer. LACP provides failure detection and failover in the event that a peer fails or becomes unreachable.
     - **LACP mode**—Select **Active** or **Passive** mode from the **LACP mode** drop-down list. If LACP is enabled, you must specify if the ports on the gateway operate in Active or Passive mode. Active enables LACP unconditionally; Passive enables LACP only when a LACP peer device is detected. For the port-channel to become active, one side must be operating in an Active mode.
     - **Port channel members**—Select the port channel members. You must add two or more port members of the same speed.
5. Click **Next** to view the configuration summary, and then click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

6. Click **Continue** to configure **SDWAN** and **Routing** profiles.

Configuring VPN Routing Profiles for a VPNC Group (Static Routing)

This section focuses on the VPN Routing Profiles configuration for a VPNC group.

To configure VPN Routing Profiles on VPNC groups, complete the following steps:

1. In the **SD-WAN Overlay** tab, click the **Overlay Orchestrator Orchestration** toggle switch.
2. Click the **Forward branch internet traffic to a specific Next-Hop router IP using PBR** toggle switch.
   - Enter the **Next-Hop Router Ipv4 Address**.
   - Enter the **Backup Next-Hop Router IPv4 Address**.
3. Click **Next**.

   The **Static Routing** page is displayed.
4. In the **Static Routing** tab, configure the static routing profile.
5. In the **Default Routes** table, click the **+** icon to configure the **Next Hop IP** address and define a **cost** metric.
6. In the **Static Routes** table, click the **+** icon to configure the following parameters:
   - **Destination IP**—Destination IP address.
   - **Destination Mask**—Subnet mask of the destination IP address.
   - **Type**—Set the route to either **Nexthop** or **Blackhole**.
   - **Next Hop**—The IP address for the next hop.
   - **Cost**—The cost metric for the route. The lower the cost, the higher the priority assigned.
7. Click **Next** to configure route maps for underlay and overlay routing.

Configuring Route Maps

In the **Route Maps** tab, you can configure **Community List Rules**, **Prefix Lists**, and **Route Maps**.

Configuring Community List Rules

The Community List feature allows administrators to configure a set of community attributes to apply on routes exchanged between Aruba Gateways and their peers. The community attribute allows grouping routes with similar properties and is generally used for tagging routes and modifying BGP routing policies.

To create a community list, complete the following steps:

1. Click on the **Community List** accordion.
2. Click the **+** icon in the **Community list rules** table.
3. Enter a **Name** for the community list rule.
4. From the **Action** drop-down list select **Permit** or **Deny**, to match the community specifications.
5. Select a **Well Known Community** from the following options in the drop-down list:
   - **Internet**—Advertises the prefix to all BGP neighbors.
   - **No-Export**—Does not advertise the prefix to any eBGP neighbor. It advertises the prefix only to iBGP neighbors.
   - **No-Advertise**—Does not advertise the prefix to any peer, iBGP or eBGP neighbor.
   - **Local-AS**— Does not advertise the prefix outside of the local Autonomous System.
6. Set a match from the **Community Values**.
7. Configure the community string in the **AS:NN** format, where AS refers to the Autonomous System number and NN refers to the Network Number. The valid range of values is 0-65535.

Configuring a Prefix List

A prefix list allows routing systems to determine which routes must be accepted when they peer with other networks. Prefix lists contain one or more ordered entries which are processed sequentially.

Prefix lists can be used as a match criteria for applying route map rules on network subnets. For example, if you want to prevent a route for 10.0.0.0/24 from being redistributed, you can define a rule to match the prefix and add it a as match criterion in the BGP redistribution route map.

To create a prefix list, complete the following steps:

1. Click on the **Prefix List** accordion.
2. Click the **+** icon in the **Prefix rules** table.
3. Enter a **Name** for the prefix rule.
4. Enter a **Sequence** number.
5. Select an **Action** to be performed from the drop-down list, when the traffic matches the condition defined in the prefix rule.
6. Enter the network **Address** to which you want to apply the prefix rule.
7. Enter the **Mask** of the network.
8. If you want to define a prefix length parameter and use it as a match criteria for applying rules, enter a value greater than or equal to this value for the **GE** operator. The allowed range of values is 1–32.
9. If you want to define a prefix length parameter and use it as a match criteria for applying rules, enter a value lower than or equal to this value for the **LE** operator. The allowed range of values is 1–32.

Configuring Route Maps

Route maps allow you to configure a filtering criteria by defining a set of rules or match statements with a permit or deny condition. A route map includes a series match statements to determine if a route matches the criteria defined in the statement and then apply the permit or deny rule accordingly.

Important Points to Note

The following list includes some of the important points to consider when configuring a route map:

- A route map includes name, sequence number, permit or deny rule, the match and set statements. The match statements determine the route or the traffic to which the rule must be applied, whereas the set statements allow you configure attributes or adjust metrics for the route that matches the criteria defined in the match statement.
- The route map rules are applied sequentially; that is, based on the sequence number defined for each entry.
- The route map can use a prefix list in the match statement to apply the allow or deny rule. For more information on prefix lists, see Configuring a Prefix List.
- Route maps can be attached to the BGP neighbor profiles for the inbound and outbound routes. You can associate route maps for the inbound and outbound traffic when configuring a BGP neighbor profile. When the route map policy is applied to the inbound or outbound BGP route, and if the traffic matches the specified criteria, the attribute set for the match condition is applied. If you do not have a route map attached to an iBGP neighbor profile, the iBGP neighbor can access all inbound and outbound routes. For more information on BGP neighbor profiles. see Adding BGP Neighbors.

To create a routing map, complete the following steps:

1. Click on the **Route Maps** accordion.
2. To add a route map, click the **+** icon in the **Route Maps** table.

   The **Add/Edit Route Map** window opens.
3. Configure the following parameters as per your network requirements:
   - Enter a **Name** for the route map.

- Enter a **Sequence Number** for the route map. Sequence numbers allow route maps to be executed in an order. If you are configuring multiple match clauses or statements, ensure that you define a sequence number to uniquely identify each match statement.
- Select an **Action** to be performed from the drop-down list, when the traffic matches the condition defined.

4. Click the **+** icon in the **Match** table to configure the **Match** condition for the routes that have a destination network.

   The match statements define a set of conditions for determining if the route redistribution must be allowed or denied. You can set match type to any of the following:
   - **IP address**— You can assign a prefix list to a match statement. The match condition determines if the route advertisements from the BGP neighbor with the prefixes must be allowed or denied.
   - **Next-hop IP**— You can assign a prefix list to a match statement. The match condition determines if the route advertisements from the BGP neighbor with the prefixes must be allowed or denied.
   - **Well known community**—A well known community allows you to configure one of the following options:
     - **Internet**—Advertises subnets to all BGP neighbors.
     - **No-Export**—Does not advertise prefix to any eBGP neighbor.
     - **No-Advertise**—Does not advertise subnets to BGP neighbors.
     - **Local-as**—Prevents sending packets outside the local autonomous system.
   - **Community AS:NN**— the community string is in the AS:NN format, where AS refers to the Autonomous System number and NN refers to the network number. The valid range of values is 0-65535.
   - **Community Value**—Allows you to specify a community value string. The valid range of values is 1–4294967295.
   - **Community list**—Allows you to select a community list configured on the Gateway.
   - **Interface VLAN**—Enter the interface VLANS separated by comma. You can enter up to 10 Interface VLANs. The value you enter must be between 1 to 4095. To know how to configure VLANs, see Configuring VLANs on Aruba Gateways.
   - **OSPF route tag**—You need to enter the tag names separated by comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.

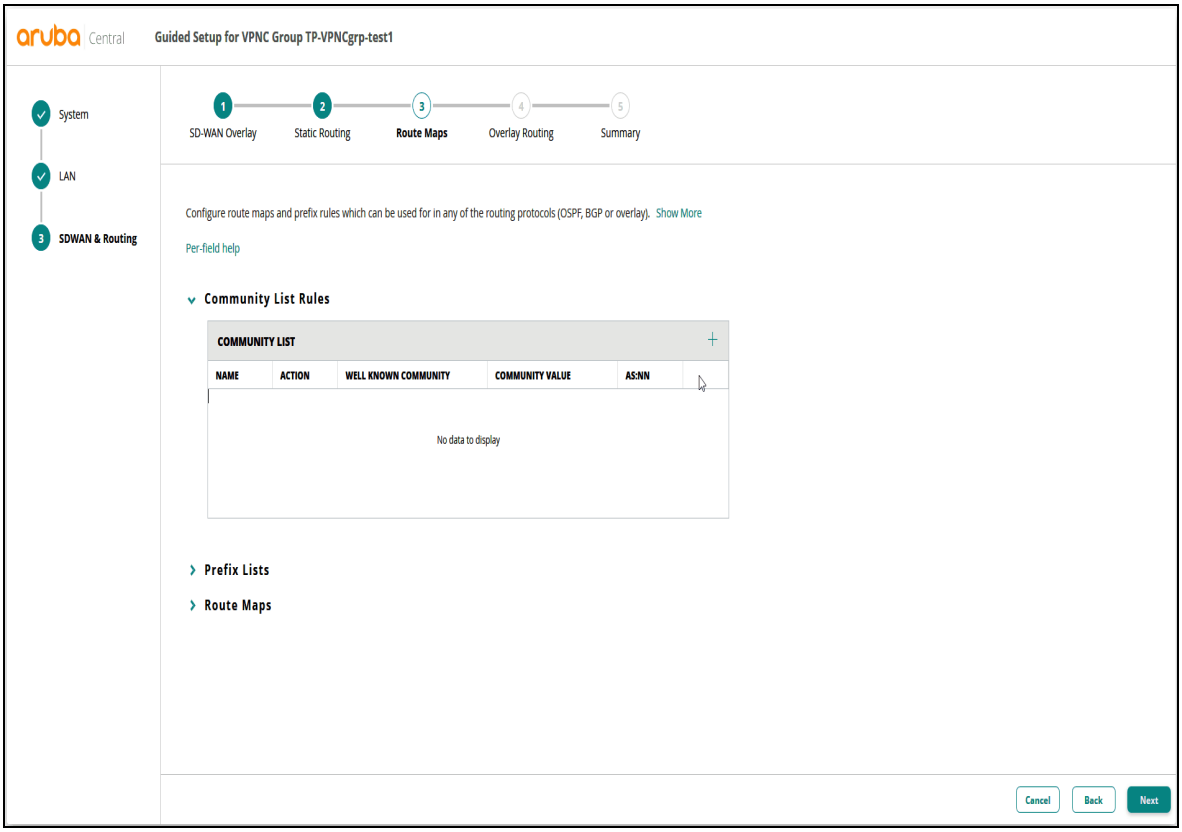
5. Click the **+** icon in the **Set** table to configure a set of rules or attributes to apply to the BGP traffic that matches the conditions defined in a match statement.

   Configure the following attributes as per your requirement:
   - **as-path-prepend**—Prepends AS numbers through which the packets have traversed. You can apply the AS path prepending criteria to the BGP traffic to determine the best path.
   - **last-as**—Prepends the last AS number to the AS path. The valid range of values is 1–10.
   - **Community value**—The BGP community Value string. The valid range of values is 1–4294967295.
   - **Community AS:NN** for match type, the community string is in the AS:NN format. The valid range of values is 0-65535.
   - **Well known community**—A well known community. You can configure one of the following options:
     - **Internet**—Advertises subnets to all BGP neighbors.
     - **No-Export**—Does not advertise prefix to any eBGP neighbor.

- **No-Advertise**—Does not advertise subnets to BGP neighbors.
- **Local-AS**—Prevents sending packets outside the local autonomous system.

- **Local-as**—Sets a local autonomous system string as an attribute in the routes.
- **metric**—Sets a metric value for determining the preferred path into an Autonomous System. You can define a metric value between 0—4294967295. When a metric value in a route matches this value, the route is advertised.
- **origin**—Sets the origin of the route. The following options are available:
  - **incomplete**(EGP)—To specify that the route is originated from exterior routing protocol.
  - **igp**—To specify that the route is originated from interior routing protocol.
- **OSPF route-type**—Sets the external metric (**External Type-1** or **External Type-2**) attribute of the route. To redistribute as routes as **External type 1** which applies both external cost to the destination and the cost to reach the boundary router in an Autonomous System. To redistribute routes as **External type-2** and apply only the external cost to the destination.
- **OSPF route tag**—Sets the tag attribute of the route. You need to enter the tag names separated by comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.

Figure 178 *Configuring Route Maps*



6. Click **Next** to proceed to **Overlay Routing**.

Configuring Overlay Routing

VPNCs use the Overlay Agent Protocol (OAP) to automatically build the SD-WAN overlay topology. The OAP allows advertising local routes to the SD-WAN Orchestrator in Aruba Central.

Configuring Redistributing Rules

Redistribution rules allow you to enable advertising of routing information from the connected, static, OSPF, and BGP interfaces into overlay routing. Routing information from other sources is not automatically redistributed into overlay routing, but need to be configured for each source protocol locally on each Gateway.

To configure redistributing rules, complete the following steps:

1. Click the **Redistribution** accordion to open the **Redistribution Rules** table.
2. To add a redistribution rule, click the **+** icon in the **Redistribution Rules** table.
3. From the **Source Protocol** drop-down list, select a protocol to be redistributed into the overlay routing. The following options are available:
   - **Static**—To redistribute IP static routes.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site. If you have selected **Connected**, select the **VLAN1** or **Loopback** interfaces to which the Gateway is connected.
   - **OSPF**—To redistribute routes learnt from the OSPF neighbors. If you have selected **OSPF**, select the OSPF path type from Filter column. The following filter options are available:
     - **Intra Area**—To redistribute routes to same area from which they originated.
     - **Inter Area**—To redistribute routes to another area in the OSPF domain.
     - **External Type 1**—To redistribute as routes as External type 1 which applies both external cost to the destination and the cost to reach the boundary router in an Autonomous System.
     - **External Type 2**—To redistribute routes as External type 2 and apply only the external cost to the destination.
   - **BGP**—To redistribute routes using BGP.

Configuring Data Center Aggregating Routes

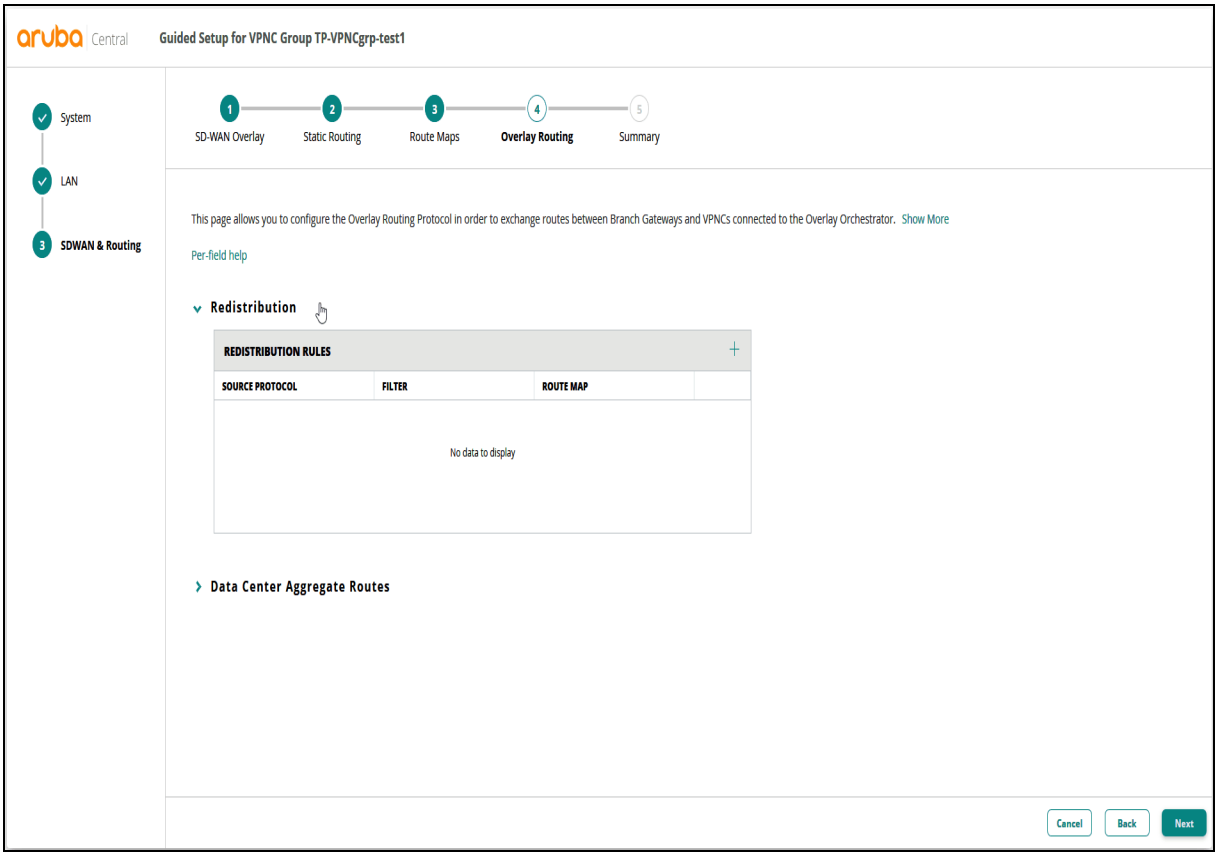
For dynamic route summarization and faster calculation of best routing paths, you can configure a route aggregation criteria. The route aggregation feature summarizes multiple routes into a single route advertisement, and thus helps in reducing the number of routing tables exchanged between BGP peers.

To aggregate data center routes, complete the following steps:

1. Click the **Data Center Aggregating Routes** accordion to open the **DC Aggregate Routes** table.
2. To allow branch route aggregation, click **Allow branch to branch** check box.
3. Click the + icon in the **DC Aggregate Routes** table to add the following details:
   - **IP Address**—Enter a network IP address.
   - **Mask**—Enter the subnet mask.

4. Click **Next** to view a summary of configuration.

Figure 179 *Configuring Overlay Routing*



5. Click **Finish** to complete the Guided Setup.

NOTE

The **Finish** button is disabled if there are any errors in the configuration. Resolve the errors to save your configurations.

Configuring VPNCs Using the Guided Setup

Aruba Gateways deployed at a data center can function as a headend Gateway or a VPNC. The VPNCs aggregate traffic from all branch offices.

You can configure a VPNC device using the Guided Setup, Basic mode, or Advanced mode. This section describes the procedure for configuring VPNCs using the Guided Setup.

Before You Begin

Before you begin, ensure that you have completed the following procedures:

- Gateways are onboarded to Aruba Central.
- Gateways are assigned valid subscriptions in Aruba Central.
- Gateways are assigned to groups.
- Gateways are assigned the VPNC group role.

NOTE

Ensure that the device is not part of a group that is running the guided setup. If the group is being configured using the Guided Setup, the device level setup will not be executed.

Configuring a VPNC using the Guided Setup

To configure aVPNC using the Guided Setup, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group that contains at least one Branch Gateway that is configured as a VPNC.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Device**.

   The gateway configuration page is displayed.

   The **Guided Setup** wizard displays the following tabs for device level configuration:
   - **System**—Allows you to configure system IP address.
   - **LAN**—Allows you to configure LAN ports.
   - **WAN**—Allows you to modify WAN ports.
   - **SDWAN & Routing**—Allows you to configure SD-WAN routing profiles.
5. Click **Begin** to start the guided setup process and complete the steps provided in the following sections:
   - Configuring a System IP Address for a VPNC
   - Configuring a LAN Interface for a VPNC
   - Configuring a WAN Interface for a VPNC
   - Configuring SDWAN and Routing Profiles for a VPNC

NOTE

Many procedures involve adding or configuring parameters in tables. Note that you have options to edit and delete the existing configurations.

Configuring a System IP Address for a VPNC

Each VPNC requires a unique system IP Address that is used by the gateway to communicate with network services such as VPN, RADIUS, Syslog, TACACS+, and SNMP. The system IP addresses for your device can be assigned from the group using a pool or per device or bulk configuration upload.

To configure a System IP for a VPNC, complete the following steps:

1. Click the **System IP** tab in the **Guided Setup** wizard.
2. Configure the **VLAN Interface:**
   - If a system IP address is configured using **Advanced Mode** on a VPNC, then that VLAN is populated in the drop-down list.
   - If system IP is not set, then enter the system IP in the text box.

3. Click **Next**.

   The **Hostname** page is displayed.
4. Enter the **Hostname**.
5. Click **Next**.
6. Review the summary and click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

7. Click **Continue** to configure a LAN interface.

Configuring a LAN Interface for a VPNC

To configure the LAN interface on a VPNC, complete the following steps:

1. In the **VLANs** tab, click the **+** icon in the **VLANs** table to add a new VLAN.
2. In the **New VLAN** pop-up, configure the following parameters:
   - **Name**—Enter a name for the VLAN.
   - **VLAN ID**—Enter the VLAN ID.
   - **IPv4 Address**—Enter an IP address.
   - **Netmask**—Enter the subnet mask.
3. Click **Save**.
4. Click **Next**.

   For more information see, Configuring VLANS.

   The **LAN ports** page is displayed.
5. Click the **+** icon in the **LAN Ports/Port Channel** table.
6. Configure the following parameters in the **New LAN Port / Port Channel** pop-up window:
   - Enter a **Name** for the port.
   - Select the **Port** from the list of available ports.
   - Select one of the following modes from the **VLAN mode** drop-down list:
     - **Access**—Select this option to allow the LAN port to carry traffic only for the VLAN to which they are assigned.
     - **Trunk**— Select this option to allow the LAN port to carry traffic for multiple VLANs. If you select the **Trunk** mode, configure a list of allowed VLANs. The following options are available:
       - **Native VLAN** (optional)
       - **Allowed VLAN** (optional)
7. Click **Next**.
8. Review the summary page and click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

9. Click **Continue** to configure a WAN interface.

Configuring a WAN Interface for a VPNC

This section defines uplink interfaces by creating WAN-facing VLANs, labeling them as uplink interfaces, and assigning them to the desired uplink ports.

To configure a WAN interface, complete the following steps:

1. To add a WAN port, click the **+** icon in the **Uplinks** table.

   The **New Uplink** pop-up is displayed.
2. Enter a name for the WAN port in the **Uplink** field.
3. Select the **Interface VLAN ID** from the drop-down list.
4. Select the type of WAN uplink to use from the **WAN type** drop-down list. For example, Internet or MPLS.

   The selection of **Internet** or **MPLS** determines the type of IP address used:
   - Select **Internet** to use a **Public IP** address.
   - Select **MPLS** to use a **Private IP** address.
5. Enter an IP address based on the **WAN type** selected.
6. Click **Save**.
7. Click **Next**.
8. Review the summary page and click **Finish**.

Finish button is disabled if there are any errors in the configuration. Resolve the errors to proceed to the next step.

9. Click **Continue** to configure SDWAN routing profiles.

Configuring SDWAN and Routing Profiles for a VPNC

This section focuses on the VPN Routing Profiles configuration for a VPNC.

To configure VPN Routing Profiles on VPNC, complete the following steps:

Enabling Overlay Orchestrator Peering

Click the toggle switch to enable **Overlay Orchestrator Peering**.

To configure VPN hubs and routing profiles, complete the following steps:

1. In the **SD-WAN Overlay** tab, click the **Overlay Orchestrator Orchestration** toggle switch.
2. Click the **Forward branch internet traffic to a specific Next-Hop router IP using PBR** toggle switch.
   - Enter the **Next-Hop Router Ipv4 Address**.
   - Enter the **Backup Next-Hop Router IPv4 Address**.
3. Click **Next**.

   The **Static Routing** page is displayed.
4. In the **Static Routing** tab, configure a static routing profile.
5. In the **Default Routes** table, click the **+** icon to configure the **Next Hop IP** address and define a **cost** metric.

6. In the **Static Routes** table, click the **+** icon to configure the following parameters:
   - **Destination IP**—Destination IP address.
   - **Destination Mask**—Subnet mask of the destination IP address.
   - **Type**—Set the route to either **Nexthop** or **Blackhole**.
   - **Next Hop**—The IP address for the next hop.
   - **Cost**—The cost metric for the route.
7. Click **Next** to configure route maps.

Figure 180 *Enabling Overlay Orchestrator Peering*

Configuring Route Maps

In the **Route Maps** tab, you can configure **Community Lists Rules**, **Prefix Lists**, and **Route Maps**.

Configuring Community List Rules

The Community List feature allows administrators to configure a set of community attributes to apply on routes exchanged between Aruba Gateways and their peers. The community attribute allows grouping routes with similar properties and is generally used for tagging routes and modifying BGP routing policies.

To create a community list, complete the following steps:

1. Click on **Community List Rules** to display the **Community List** table.
2. Click the **+** icon in the **Community list rules** table.
3. Enter a **Name** for the community list.
4. From the **Action** drop-down list select **Permit** or **Deny**, to match the community specifications.
5. Select a **Well Known Community** from the following options in the drop-down list:
   - **Internet**—Advertises the prefix to all BGP neighbors.
   - **No-Export**—Does not advertise the prefix to any eBGP neighbor. It advertises the prefix only to iBGP neighbors.
   - **No-Advertise**—Does not advertise the prefix to any peer, iBGP or eBGP neighbor.
   - **Local-AS**— Does not advertise the prefix outside of the local Autonomous System.

6. Set a match from the **Community Value**.
7. Configure the community string in the **AS:NN** format. The valid range of values is 0-65535.

Configuring a Prefix List

A prefix list allows routing systems to determine which routes must be accepted when they peer with other networks. Prefix lists contain one or more ordered entries which are processed sequentially.

Prefix lists can be used as a match criteria for applying route map rules on network subnets. For example, if you want to prevent a route for 10.0.0.0/24 from being redistributed, you can define a rule to match the prefix and add it a as match criterion in the BGP redistribution route map.

To create a prefix list, complete the following steps:

1. Click on **Prefix List** to display the **Prefix rules** table.
2. Click the **+** icon in the **Prefix rules** table.
3. Enter a **Name** for the prefix rule.
4. Enter a **Sequence** number.
5. Select an **Action** to be performed from the drop-down list, when the traffic matches the condition defined in the prefix rule.
6. Enter the network **Address** that the prefix rule applies to.
7. Enter the **Mask** of the network.
8. If you want to define a prefix length parameter and use it as a match criteria for applying rules, enter a value greater than or equal to this value for the **GE** operator. The allowed range of values is 1–32.
9. If you want to define a prefix length parameter and use it as a match criteria for applying rules, enter a value lower than or equal to this value for the **LE** operator. The allowed range of values is 1–32.

Configuring Route Maps

Route maps allow you to configure a filtering criteria by defining a set of rules or match statements with a permit or deny condition. A route map includes a series match statements to determine if a route matches the criteria defined in the statement and then apply the permit or deny rule accordingly.

Important Points to Note

The following list includes some of the important points to consider when configuring a route map:

- A route map includes name, sequence number, permit or deny rule, the match and set statements. The match statements determine the route or the traffic to which the rule must be applied, whereas the set statements allow you configure attributes or adjust metrics for the route that matches the criteria defined in the match statement.
- The route map rules are applied sequentially; that is, based on the sequence number defined for each entry.
- The route map can use a prefix list in the match statement to apply the allow or deny rule. For more information on prefix lists, see Configuring a Prefix List.
- Route maps can be attached to the BGP neighbor profiles for the inbound and outbound routes. You can associate route maps for the inbound and outbound traffic when configuring a BGP neighbor profile. When the route map policy is applied to the inbound or outbound BGP route, and if the traffic matches the specified criteria, the attribute set for the match condition is applied. If you do not have a route map attached to an iBGP neighbor profile, the iBGP neighbor can access all inbound and outbound routes. For more information on BGP neighbor profiles. see Adding BGP Neighbors.

To create a route map, complete the following steps:

1. Click on **Route Maps** to display the **Route Maps** table.
2. To add a route map, click the **+** icon in the **Route Maps** table. The **Add/Edit Route Map** pane opens.

Configure these parameters as per your network requirements:

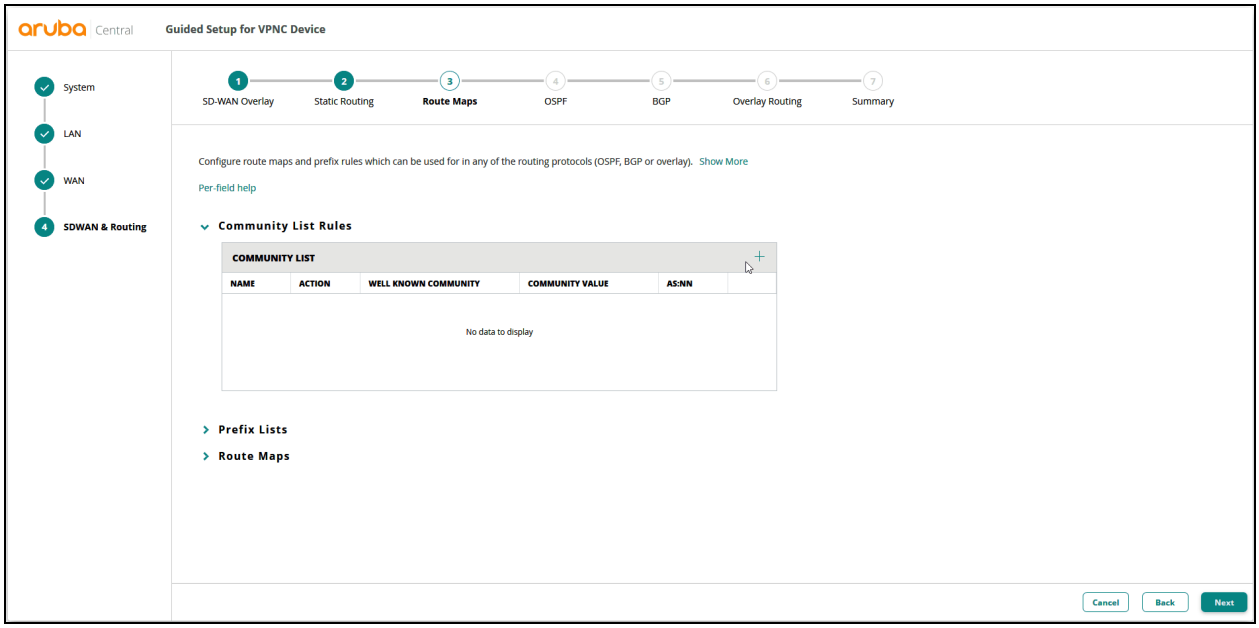
1. Enter a **Name** for the route map.
2. Enter a **Sequence number** for the route map. Sequence numbers allow route maps to be executed in an order. If you are configuring multiple match clauses or statements, ensure that you define a sequence number to uniquely identify each match statement.
3. Select an **Action** to be performed from the drop-down list, when the traffic matches the condition defined.
4. Click the **+** icon in the **Match** table to configure the **Match** condition for the routes that have a destination network.

   The match statements define a set of conditions for determining if the route redistribution must be allowed or denied. You can set match type to any of the following:
   - **IP address**— You can assign a prefix list to a match statement. The match condition determines if the route advertisements from the BGP neighbor with the prefixes must be allowed or denied.
   - **Next-hop IP**— You can assign a prefix list to a match statement. The match condition determines if the route advertisements from the BGP neighbor with the prefixes must be allowed or denied.
   - **Well known community**—A well known community allows you to configure one of the following options:
     - **Internet**—Advertises subnets to all BGP neighbors.
     - **No-Export**—Does not advertise prefix to any eBGP neighbor.
     - **No-Advertise**—Does not advertise subnets to BGP neighbors.
     - **Local-as**—Prevents sending packets outside the local autonomous system.
   - **Community AS:NN**— the community string is in the AS:NN format, where AS refers to the Autonomous System number and NN refers to the network number. The valid range of values is 0-65535.
   - **Community value**—Allows you to specify a community value string. The valid range of values is 1–4294967295.
   - **Community list**—Allows you to select a community list configured on the Gateway.
   - **Interface VLAN**—Enter the interface VLANS separated by comma. You can enter up to 10 Interface VLANs. The value you enter must be between 1 to 4095. To know how to configure VLANs, see Configuring VLANs on Aruba Gateways.
   - **OSPF route tag**—You need to enter the tag names separated by comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.
5. Click the **+** icon in the **set** table to configure a set of rules or attributes to apply to the BGP traffic that matches the conditions defined in a match statement.
   Configure the following attributes as per your requirement:
   - **as-path-prepend**—Prepends AS numbers through which the packets have traversed. You can apply the AS path prepending criteria to the BGP traffic to determine the best path.
   - **last-as**—Prepends the last AS number to the AS path. The valid range of values is 1–10.
   - **Community value**—The BGP community Value string. The valid range of values is 1–4294967295.

- **Community AS:NN** for match type, the community string is in the AS:NN format. The valid range of values is 0-65535.
- **Well known community**—A well known community. You can configure one of the following options:
  - **Internet**—Advertises subnets to all BGP neighbors.
  - **No-Export**—Does not advertise prefix to any eBGP neighbor.
  - **No-Advertise**—Does not advertise subnets to BGP neighbors.
  - **Local-AS**—Prevents sending packets outside the local autonomous system.
  - **Community list**—Allows you to select a community list configured on the Gateway.
- **Local-as**—Sets a local autonomous system string as an attribute in the routes.
- **metric**—Sets a metric value for determining the preferred path into an Autonomous System. You can define a metric value between 0—4294967295. When a metric value in a route matches this value, the route is advertised.
- **origin**—Sets the origin of the route. The following options are available:
  - **incomplete**(EGP)—To specify that the route is originated from exterior routing protocol.
  - **igp**—To specify that the route is originated from internal routing protocol.
- **OSPF route-type**—Sets the external metric (**External Type-1** or **External Type-2**) attribute of the route.
  - To redistribute as routes as **External type 1** which applies both external cost to the destination and the cost to reach the boundary router in an Autonomous System.
  - To redistribute routes as **External type-2** and apply only the external cost to the destination.
- **OSPF route tag**—Sets the tag attribute of the route. You need to enter the tag names separated by comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.

6. Click **Save**.
7. Click **Next** to configure OSPF.

Figure 181 *Configuring Route Maps*



Configuring OSPF

The OSPF configuration allows advertising branch networks into an OSPF area and also enables VPNCs to learn corporate routes. You can configure the General, Interface and Redistribution settings in this section.

Configuring General Setting

To enable the OSPF, complete the following steps:

1. Click on **General** accordion.
2. Click the **Enable OSPF** toggle switch.
3. Select the **Default originate** check box to generate a default external route to OSPF.
4. Enter the **Router ID**. The router ID is the IPv4 address used for identifying it as the router in an autonomous system.
5. Set the OSPF **Area ID** for the interface VLAN.

Configuring the Interface

To configure an interface, complete the following steps:

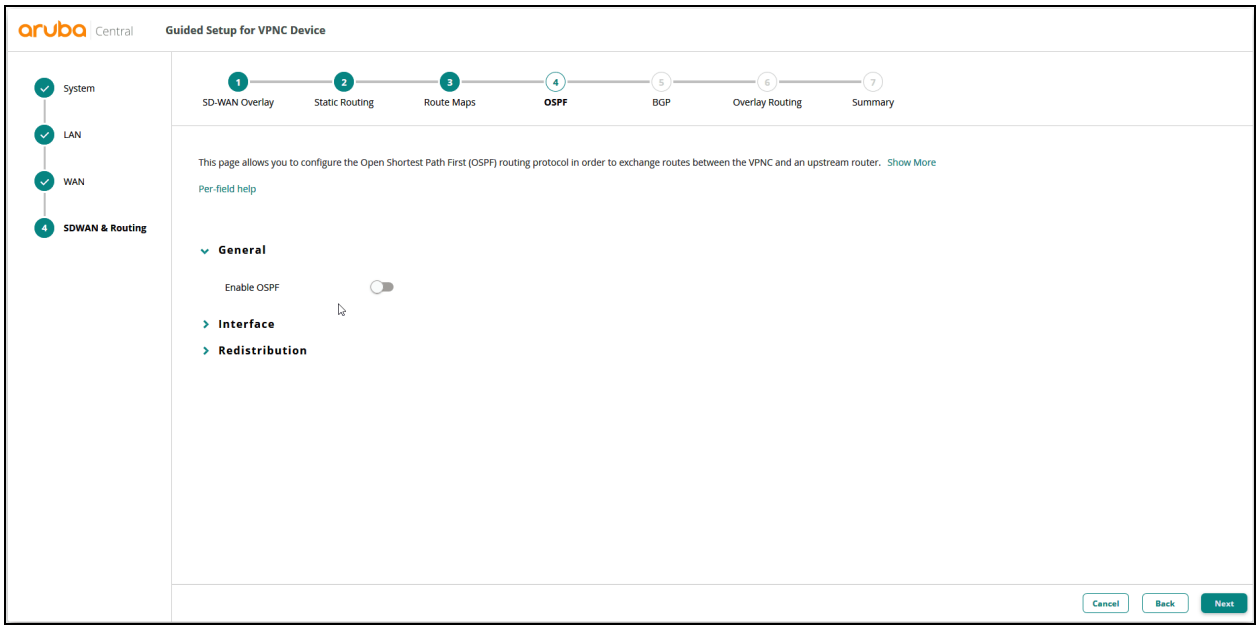
1. Click on **Interface** accordion to display the **VLANs** table.
2. To add an interface, click the **+** icon in the **VLANs** table.
3. Select a OSPF interface **VLAN** from the drop-down list.
4. Set the OSPF **Area ID** for the interface VLAN.
5. Set the **Cost** for the interface VLAN.
6. Set the **Hello Interval** timer to send messages to neighbors.

Configuring Redistribution Rules

To configure redistribution rules, complete the following steps:

1. Click the **Redistribution** accordion to display the **Redistribution Rules** table.
2. To add redistribution rules, click the **+** icon in the **Redistribution Rules** table.
3. From the **Source Protocol** drop-down list, select the type of routes to redistribute. The following options are available:
   - **Static**—To redistribute IP static routes.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site.
   - **SDWAN Overlay**—To redistribute routes learnt from the SD-WAN overlay network through the Overlay Agent Protocol.
   - **IAP-VPN Overlay**—To redistribute routes that were received from deployments with Instant APs.
4. Set the **Filters** for the list of VLANs to be redistributed into OSPF. This is applied only when the source protocol is set to **Connected**.
5. Select the **Route Type** based if the route is redistributed as **External-Type 1** (E1) or **External-Type 2** (E2). If you want to steer to the closest exit use E1, to steer the traffic to a specific exit use E2.
   - E1 increases the cost, reflecting the in the internal OSPF domain path cost.
   - E2 has a fixed cost as configured in the Cost field.
6. Select a **Route Map** to associate with the routes.
7. Click **Next** to configure BGP.

Figure 182 *Configuring OSPF*



Configuring BGP

To support interoperability with an existing network infrastructure, BGP a dynamic routing protocol enables VPNCs to redistribute overlay routes learned from Branch Gateways into BGP and advertise those routes in the data center network.

Configuring General setting

1. Click the **General** accordion.
2. Click the **Enable BGP** toggle switch to enable BGP.
3. Select the **Default orignate** check box to generate a default external route to OSPF.
4. Enter the **AS number** to determine if the BGP neighbor is in the same autonomous aystem (AS).
5. Enter the **Router ID**. The router ID is the IPv4 address of Gateway used for identifying it as the router in an autonomous system.

Configuring Neighbors

To configure neighbors, complete the following steps:

1. Click **Neighbors** accordion to display the **Neighbors** table.
2. To add neighbors, click the **+** icon in the **Neighbors** table.
3. Enter the **Peer Address** (IP address) of the neighbor you want to establish communication with.
4. Enter the number of **Remote AS** to which the peer router belongs.
5. Select the **Multi-Hop** check box if you want the Gateway to route packets to its remote BGP peer that is more than one hop away.
6. Set the **Update Source** for the Interface or IP address used for the BGP updates in a multi-hop scenario.
7. Select the **Route Map In** value from the drop-down list. This is a per-neighbor routing policy that is applied to information received from the neighbor.

8. Select the **Route Map In** value from the drop-down list. This is a per-neighbor routing policy that is applied to information sent to the neighbor.

Advertising Networks to BGP

To advertise networks, complete the following steps:

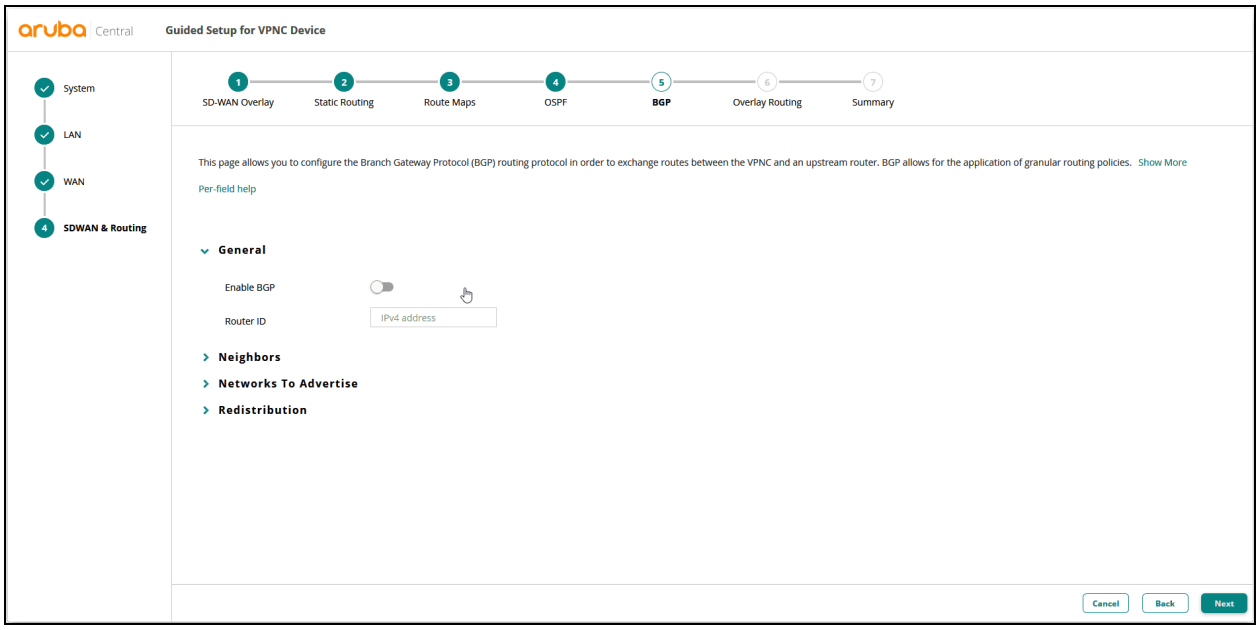
1. Click the **Networks To Advertise** accordion to display the **Prefixes to Aggregate** table.
2. To add networks, click the **+** icon in the **Prefixes to Aggregate** table.
3. Select the prefix type as **Network** or **Aggregate** from the **Type** drop-down list.
4. Enter the network IP **Address** that you want advertised.
5. Enter the subnet **Mask** for the advertised network.
6. If you select **Aggregate** from the **Type** drop-down list, then select the **Route Map** from the drop-down.

Configuring Redistribution Rules

To configure Redistribution Rules, complete the following steps:

1. Click the **Redistribution** accordion to display the **Redistribution Rules** table.
2. To add rules, click the **+** icon in the **Redistribution Rules** table.
3. From the **Source Protocol** drop-down list, select the type of routes to redistribute. The following options are available:
   - **Static**—To redistribute the static routes manually configured on Branch Gateways.
   - **OSPF**—To redistribute the routes learnt from an OSPF neighbor.
   - **SD-WAN Overlay**—To redistribute routes learnt from the SD-WAN overlay network through the Overlay Agent Protocol.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site.
   - **IAP-VPN Overlay**—To redistribute routes that were received from micro-branch deployments with Instant APs.
4. Optionally, you can select a **Route Map** to associate to the routes.
5. Click **Next** to configure Overlay Routing.

Figure 183 *Configuring BGP*



Configure Overlay Routing

Redistribution rules allow you to enable advertising of routing information from the connected, static, OSPF, and BGP interfaces into overlay routing. Routing information from other sources is not automatically redistributed into overlay routing, but need to be configured for each source protocol locally on each Gateway.

Configuring Redistributing Rules

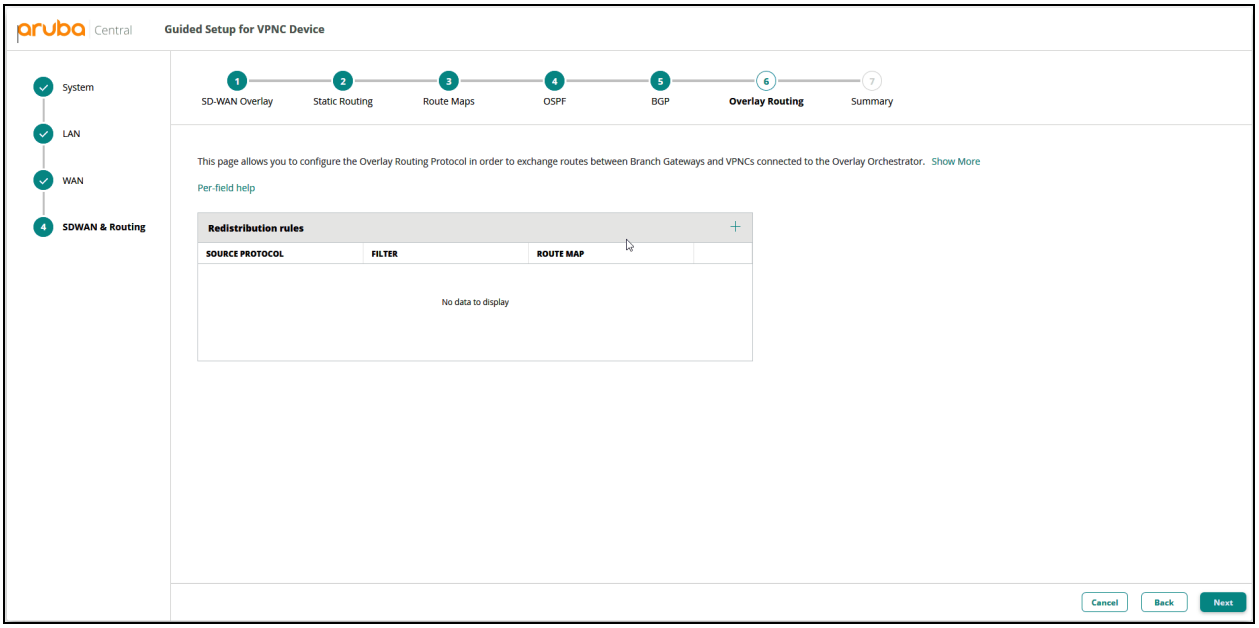
To redistribute routes as overlay routes, complete the following steps:

1. To add a redistribution rule, click the **+** icon in the **Redistribution rules** table.
2. From the **Source Protocol** drop-down list, select the type of routes to redistribute. The following options are available:
   - **Static**—To redistribute IP static routes.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site. If you have selected **Connected**, select the VLAN interfaces to which the Gateway is connected.
   - **OSPF**—To redistribute routes learnt from the OSPF neighbors. If you have selected **OSPF**, select the OSPF path type from Filter column. The following options are available:
     - **Intra Area**—To redistribute routes to same area from which they originated.
     - **Inter Area**—To redistribute routes to another area in the OSPF domain.
     - **External Type 1**—To redistribute as routes as External type 1 which applies both external cost to the destination and the cost to reach the boundary router in an Autonomous System.
     - **External Type 2**—To redistribute routes as External type 2 and apply only the external cost to the destination.
   - **BGP**—To redistribute routes using BGP.
3. Set a **Filter** for the selected protocol.
4. Associate an existing **Route Map** with the **Source Protocols** if required. The route map association

is applicable only for available routes.

5. Click **Next** to view a summary of the configuration.

Figure 184 *Configure Overlay Routing*



6. Click **Finish** to complete this Guided Setup.

NOTE

The **Finish** button is disabled if there are any errors in the configuration. Resolve the errors to save your configurations.

This section guides you through the steps required to set up your SD-WAN network using the Advanced Setup.

NOTE

Before you proceed with the configuration tasks, browse through the recommendations and best practices described in the Aruba SD-Branch Fundamentals Guide and Aruba SD-Branch Security Hardening Guide.

Configuration Checklist

Table 239 describes the configuration workflow for the SD Branch devices.

Table 239: *SD Branch Configuration Checklist*

VPNCs	Branch Gateways
■ Configure Address Pools ■ Configure Hostname and IP address ■ Configure VLAN Interfaces ■ Assign VLANs to Switchports ■ Whitelist Branch Gateways ■ Configure Static Routes ■ Configure OSPF	■ Configure Address Pools ■ Configure Hostname and IP address ■ Configure VLAN Interfaces ■ Configure Ports ■ Assign VLANs to Switchports ■ Configure WAN Uplinks ■ Configure Hub and Spoke VPN ■ Configure Site to Site VPN ■ Configure Dynamic Path Steering Policies ■ Configure Policies for PBR ■ Configure Firewall Policies ■ Configure User Roles ■ Configure Authentication Profiles ■ Install CA and Server Certificates

Configuring Address Pools for Aruba Gateways

In a branch site, the SD Branch requires a pool of IP addresses to allow dynamic assignment of IP addresses to itself and its client devices.

The SD Branch deployment requires the following types of address pools:

- Gateway Pool—A gateway pool is used to assign a range of IP addresses for a device group. IP addresses are assigned to each SD-WAN Gateway that joins this device group.
- DHCP pools—A DHCP pool for a configuration group defines a set of IP addresses that can be assigned to client devices associated to Branch Gateways.
- NAT Pools—A NAT pool is used to translate the source IP address when forwarding port traffic or allowing traffic from the outside network to the designated hosts in the branch network.
- Tunnel Pools — A tunnel pool defines a range of IP addresses that can be used by the Branch Gateway to create a GRE tunnel to the headend gateway. When you add a Branch Gateway, an IP address is removed from the tunnel pool on the hierarchy node and is leased to the added device. Addresses those are no longer in use are automatically returned to the pool for reallocation.

NOTE

Tunnel pools and gateway pools can be configured only at the group level as they are not applicable to the device level configuration.

Configuring Gateway Pools for Aruba Gateways

A gateway pool refers to a pool of IP addresses configured for a device group. The system IP addresses for the SD-WAN Gateways are assigned from the gateway pool when a device joins the group.

NOTE

Gateway pools can be configured only at the group level and is not applicable for the device level configuration.

Creating Gateway Pools for Branch Gateway or VPNC Group

To create the gateway pools for a device group, complete the following steps:

1. Set the filter to a group containing at least one Branch Gateway or VPNC group.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Interface** > **Pool Management**.
6. Expand **Gateway Pool**.
7. To create a new gateway pool, click the **+** icon in the **Gateway pool** table.
8. The **Add New Gateway Pool** pane is displayed.
9. In the **Pool name** field, enter a name for the new pool.
10. In the **Start IP address** field, enter the first IP address of the IP address range.
11. In the **End IP address** field, enter the last IP address of the IP address range.
12. Click **Save Settings**. The gateway pool must be assigned to a VLAN to allow Aruba Centraldynamic assignment of IP addresses from the pool.

Assigning a VLAN to a Gateway Pool

To assign a VLAN to a gateway pool complete either of the following steps:

1. Set the filter to a group containing at least one Branch Gateway or VPNC group.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Interfaces** > **VLANs**.
6. Select a VLAN from the **VLANs** table.
7. Select the VLAN ID from the **VLAN IDs** table. The VLAN details are displayed.
8. From the **IP assignment** drop-down list, select **Gateway pool**.

9. Select the required gateway pool from the **VLAN Pool** drop-down list.
10. Save the changes. To enable IP address assignment to SD-WAN Gateways from the gateway pool, see Configuring System Information on Aruba Gateways.

Configuring DHCP Address Pools on Aruba Gateways

A DHCP pool is a set of IP addresses that can be assigned to the client devices associated to the Branch Gateway of a specific branch. When the Aruba Gateway acts as the DHCP server, DHCP pools allow dynamic and automatic assignment of IP addresses for VLAN interfaces.

A DHCP pool can be configured at both the device and group level for Branch Gateway and VPNC.

Creating a DHCP Pool

To create a DHCP address pool, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **DHCP**.
4. Select the **IP DHCP server** check box to enable the Aruba Gateway to act as a DHCP server.
5. To add a new pool, click the **+** icon below the **Pool Configuration** table.
6. Configure the following parameters:

Table 240: *DHCP Pool Configuration Parameters*

Parameter	Description
IP version	Enter the IP version of the pool.
Pool Name	Enter the name of the new address pool.

Table 240: *DHCP Pool Configuration Parameters*

Parameter	Description
Network IP address type	Network address type. Select **Static** to add a static IP address and netmask to the pool, or select **Dynamic** to define a range of addresses that the DHCP server may assign to clients. ■ If you select **Static**, you must enter the IP address and IP mask of the network in the **Network IP address** and **Network IP mask** fields. You must also specify the IP address of the default router for the DHCP client in the **Default routers** field. The client should be on the same subnet as the default router. You can specify up to eight IP addresses. ■ If you select **Dynamic**, you must enter the starting and ending IP addresses for the address range, as well as the maximum number of hosts to be supported by the pool.
Network IP address	Enter the network IP address.
Network IP mask	Enter the subnet mask for the network IP.
Default routers	Enter multiple routers separating each one with a space.
Domain Name	Enter the domain name to which the client belongs.
DNS Servers	Configure the DNS server IP address by selecting one of the following options: ■ **Specify Servers**—Select this option and specify the IP addresses of the DNS servers in the **DNS servers IP addresses** field. You can specify up to eight IP addresses. Multiple IP addresses must be separated by a space. ■ **Import from DHCP/PPPoE**—Select this option to import DNS server address obtained through PPPoE or DHCP. ■ **Use gateway address**—Select this option to use the Aruba Gateway as the DNS server.
DNS servers IP addresses	Enter multiple DNS server IP addresses separating each one with a space.
Enable PXE	Use this to enable network boot on Preboot Execution Environment (PXE) capable Gateway clients. Configure the following parameters for PXE boot support: ■ **Server Name**—Enter a hostname or the IP address of the server from which the Gateway clients can download the boot file. Ensure that the hostname or IP address configured for the boot server can be resolved by the PXE-enabled clients through a DNS server. ■ **Next Server**—Enter a hostname or IP address of the next server from which the Gateway clients can download the boot file. ■ **Boot File**—Specify the boot file that the Gateway clients can use for network boots.
Import WINS server from DHCP/PPPoE	Enable this to import the NetBIOS name server address that is obtained through PPPoE or DHCP.
WINS	Provide the IP address of a NetBIOS Windows Internet Naming Service (WINS) server if you are not importing the WINS address from DHCP or PPPoE. You can specify up to eight IP addresses. Multiple IP addresses must be separated by a space.

Table 240: *DHCP Pool Configuration Parameters*

Parameter	Description
	NOTE: This field is not applicable if you enable the **Import WINS server from DHCP/PPPoE** option.
Lease time	Specify the number of days, hours, or minutes for which the assigned IP address is valid for the client.
Pool type	Select any of the following options: ▪ **public**—To assign addresses from a public pool. ▪ **private**—To assign addresses from a private pool. ▪ **ipupsell**—To assign either private or public address from a designated DHCP pool.
Option	Click the **+** icon to add the following client-specific information: ▪ **Option**—option code ▪ **DHCP option format**—Select the DHCP option from the drop-down list. Options available are **IP**, **Text**, and **Hex**. ▪ **Value**—Enter the value.

Excluding IP Address Range

To exclude an IP address or a range of IP addresses from the DHCP pool, complete the following steps:

1. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
2. Click **Interfaces** > **DHCP**.
3. Click the **+** icon from the **IP excluded address range** table.
4. Specify the IP address range in the **IPv4 excluded range** field.

Reserving IP addresses

By default, Gateways dynamically lease IP addresses from a DHCP pool to their connected clients. As IP addresses are randomly assigned to clients, the client devices may not acquire the same IP address every time they request for a network connection.

If your site has client devices, such as printers and scanners, for which you want to assign a static IP address, you can use IP reservation to manually bind IP addresses from a DHCP pool to a client MAC address. With IP reservation, Gateways can assign the same IP address to a client whenever it requests for a network connection.

To reserve an IP address from the DHCP pool, complete the following steps:

1. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
2. Click **Interfaces** > **DHCP**.
3. Click the **+** icon in the **IP reservations** table.
4. In the **Add clients** window, specify the **Client Name**, **MAC Address**, and the **IP Address** that you want to reserve.

   The table allows five entries by default. Click the **+** icon to add another row. You can configure up to 64 clients.

5. Click **Save Settings**.

To delete a client, select the client in the **IP reservations** table and click the delete icon.

Configuring NAT Pools

A NAT pool provides a set of IP addresses that can be used for translating network addresses for the outgoing traffic from the branch network.

A NAT Pool can be configured at the device and group level for both Branch Gateways and VPNCs.

Creating a NAT Pool

To create a NAT pool, complete either of the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interfaces** > **Pool Management**.
4. Expand **NAT Pools**.
5. To add a new pool, click the **+** icon below the **NAT Pools** table.
6. In the **Pool name** field, enter a name for the new pool.
7. In the **Start IP address** field, enter the first IP address of IP address range.
8. In the **End IP address** field, enter the last IP address of the IP address range.
9. In the **Destination NAT IP address** field, enter the IP address to configure the destination NAT.
10. Select the **Used by VPN** if this NAT pool is used by the VPN.
11. Click **Save Settings**.

Creating a Static 1:1 NAT

To create a static 1:1 NAT on a Branch Gateway, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interfaces** > **Pool Management**.
4. Expand **Static 1:1 NAT** and click the **+** icon below the **NAT mapping** table to edit the settings.
5. In the **INTERNAL ADDRESS** field, enter the internal IP address of the device.
6. In the **EXTERNAL ADDRESS** field, enter the IP address to be mapped to the device; this IP address is exposed outside of the network.
7. Click **Save Settings**.

Based on your branch requirements, you can enable NAT on VLAN interfaces for the traffic that is routed through the tunnel. For more information on enabling NAT for egress traffic, see Configuring VLANs on Aruba Gateways.

Configuring Tunnel Pools for Aruba Gateways

A tunnel pool defines a range of IP addresses that can be used by the Branch Gateways in a group to create a GRE tunnel to the headend gateway. When you add a Branch Gateway to the group, an IP address is removed from the tunnel pool on that hierarchy node and is leased to that device. Addresses no longer in use are automatically returned to the pool for reallocation.

Tunnel pools can be configured only at the group level and is not applicable for the device level configuration.

To create a tunnel pool on a Branch Gateway group or VPNC group, complete the following steps:

1. Set the filter to a group containing at least one Branch Gateway or VPNC group.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.

3. Click **Config**.

   The configuration page is displayed for the selected group.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Interface** > **Pool Management**.
6. Expand **Tunnel Pools**.
7. To add a new pool, click the **+** icon below the **Add New Tunnel Pool** table.
8. Configure the following parameters:
   - **Pool Name**—Enter the name of the new tunnel pool.
   - **Start IP address**—Enter the IP address to define the start of the range of addresses.
   - **End IP address**—Enter the IP address to define the end of the range of addresses.
9. Click **Save Settings**.

Uploading Bulk Configuration Template

Aruba Central allows you to configure VLANs, ports, DHCP Pools, PPPoE credentials or IP addresses for SD-WAN Gateways in bulk.

The Bulk Configuration can be done at the device and group level for both Branch Gateways and VPNCs.

To upload a template for bulk configuration, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click **Config**.

        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.

        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.

        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **Bulk configuration upload**.
4. Click **Download sample file** to download a sample file.
5. Click **Download device template**. A CSV file with a list of Aruba Gateways is downloaded to your local directory.

6. Update the CSV file with configuration parameters for VLANs, DHCP pools, and IP address assignment.
7. Click **Browse** to upload the template.
8. Click **Save Settings**.

Configuring System Information on Aruba Gateways

This section describes the procedures for configuring system parameters for Aruba Gateways. Click on the links listed here for more information:

- Configuring or Renaming Gateway Hostname
- Configuring System IP Address
- Setting System Clock and Time Zone
- Configuring Domain Name System
- Configuring Redirect DNS Servers
- Configuring Dynamic Domain Name System
- Configuring Dynamic Domain Name System (HTTPS)
- Setting Capacity Threshold
- Configuring Device Administrator Credentials for Aruba Gateways
- Configuring Switching Parameters
- Configuring AMON Receivers for Aruba Gateways

Configuring or Renaming Gateway Hostname

You can create a hostname in Advanced Mode and can modify a hostname in Basic and Advanced modes.

Hostname can be configured only at the device level for Branch Gateway and VPNC.

To assign or modify a gateway hostname, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group that contains at least one Branch Gateway.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **Basic Info**.
7. Enter a **Hostname**.

If a gateway hostname already exists, you can modify the string. For offline gateways, the change is reflected in Aruba Central after the gateway comes online.

8. If required, configure admin credentials.
9. Click **Save Settings**.

Configuring System IP Address

The system IP configuration is required on each Gateway provisioned in Aruba Central. Each Gateway uses one VLAN interface as its system IP address for communicating with network services such as RADIUS, syslog, TACACS+, and SNMP.

You can assign a system IP address to Gateways using one of the following methods:

- Gateway pools—You can assign a VLAN interface from a Gateway pool and allow Aruba Central to automatically allocate a host address to a dedicated VLAN interface from the range of addresses configured for the device group.
- Dynamic DHCP Pools—If you have a dynamic pool of addresses configured for the Branch Gateway group, Aruba Central can automatically allocate a subnet to the LAN VLAN interface on a Branch Gateway.
- Bulk configuration templates—You can assign a system IP address by using the Bulk configuration upload feature. The Bulk configuration upload feature allows you to upload Gateway configuration parameters to Aruba Central using a CSV file.
- Manual assignment of VLAN interfaces—If you want to configure a system IP address per device, you can manually configure a static IP address for the VLAN interface.

If the system IP address is not assigned to Gateways, Aruba Central will not push configuration to Gateways, which may lead to configuration discrepancies.
A system reboot is required when you change the system IP address of a Gateway.

To configure system IP address for Aruba Gateways, complete the following steps:

1. In the **Network Operations** app, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **General**.
4. Expand **System IP Address**.

- To configure system IP address for Gateways at the group-level, complete the following checks:
  - To dynamically assign system IP addresses using a Gateway pool, ensure that a gateway address pool is configured and assigned to a VLAN interface. Aruba Central dynamically assigns system IP addresses from the gateway address pool to the devices when they join the group. For more information on gateway pools, see Assigning a VLAN to a Gateway Pool.
  - To dynamically assign system IP address from a dynamic DHCP pool, ensure that a dynamic DHCP pool is configured and assigned to a VLAN interface.
  - To assign a system IP address at the device level, ensure that a VLAN interface is configured on the device with a static IP.

5. From **IPv4** drop-down, select a VLAN interface.
6. Click **Save Settings**.

A pre-provisioned gateway configured using the complete setup does not consider the system IP configured here.

Configuring a Loopback Interface

The loopback IP address is a logical IP interface used for terminating VPN and GRE tunnels, originating requests to RADIUS servers, and accepting administrative communications. You can configure the loopback address as a host address for Gateways The loopback address is not bound to any specific interface and is operational at all times. To use this interface, ensure that the IP address is reachable through one of the VLAN interfaces.

If your deployment requires OSPF configuration, Aruba recommends that you configure a loopback interface per VPNC and set the same as the OSPF router ID. For more information, see Routes Advertisement Using OSPF.

To configure a loopback interface, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group that contains at least one Branch Gateway or VPNC.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **System** > **General**.
7. Expand **Loopback Interface**.
8. Enter an **IPv4 address**.
9. Click **Save Settings**.

Configuring Location Access

You can configure access to the gateway location by enabling GPS. You can view the GPS coordinates in the Gateway Monitoring dashboard.

To configure location access, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **General**.
4. Expand **Location**.
5. The **GPS** check box is selected by default.
6. Click **Save Settings**.

Setting System Clock and Time Zone

You can set the clock on a device and group level manually or you can configure the Aruba Gateways to use an NTP server to synchronize its system clock with a central time source. The system automatically updates the time zone including the relevant Daylight Savings Time (DST) across time zones. This is done to automatically keep the time up-to-date and precise with DST adjustments.

This configuration can be done at the device and group level for both Branch Gateway and VPNC.

Configuring NTP Server

To add an NTP server, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To select a VPNC or a Branch Gateway device in the filter:

a. Set the filter to **Global**.

b. Under **Manage**, click **Devices**, and then click **Gateways**.

A list of gateways is displayed in the **List** view.

c. Click a gateway listed under **Device Name**.

The dashboard context for the device is displayed.

d. Under **Manage**, Click **Device**.

The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **General**.
4. Click **Clock**.
5. Select **Get time from NTP server** from the **Time** drop-down list.
6. Click the **+** icon in the **NTP servers** table.
7. In the **Add NTP Server** pane, select **IPv4** or **IPv6** or **FQDN** from the drop-down list.
8. Enter the **IPv4** or **IPv6** or **FQDN** address of the NTP server based on your selection in the previous step.
9. Select the **Burst mode** check box, if required. It is disabled by default.

   The **Burst Mode** is a configurable option and not the default behavior for the Branch Gateway, as this option is considered recommended by some public NTP servers. If an NTP server is unresponsive, the **Burst Mode** continues to send frequent queries until the server responds and time synchronization starts.
10. Enter the authentication key to be used by NTP server in the **Authentication key** text box. The range of allowed values is 1–65534.
11. Select **Source interface** from the drop-down list.

Enabling NTP Authentication

NTP authentication allows NTP clients to authenticate before synchronizing clocks. NTP authentication works by using a symmetric key that is configured by the user. The secret key is shared both by the SD-WAN Gateway and an external NTP server. NTP authentication is disabled by default.

1. Enable **Use NTP authentication**.
2. In the **NTP Authentication** table, click the **+** icon.

   The **Add NTP Authentication** section is displayed.
3. Enter the authentication key in the **Authentication key** text box. The allowed range of numeric values is 1–65534.
4. Enter value for the **MD5 secret**. The valid key value must be an ASCII string from 0 to 255 characters.
5. Select the **Trusted key** check box to specify that the authentication key is trusted. By default, the check box is cleared.
6. Click **Save Settings**.

Setting Time Zone

To set a time zone, complete the following steps:

1. Click **System** > **General**.
2. Click **Clock**.
3. In the **Timezone** section, select the appropriate time zone from the drop-down list.
4. Click **Save Settings**.

Configuring Domain Name System

Network devices on the Internet use an IP address to route your request to the site you are trying to reach. Once you connect through a DNS server, it manages a database that maps domain names to IP addresses and routes your query to the next appropriate server.

To enable Aruba Gateways to connect to a DNS server, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **General**.
4. Click **Domain Name System**.
5. Enter a **Domain name**.
6. Enable **DNS name resolution**.
7. To add a DNS server, click the **+** icon in the **DNS servers** table.
8. Enter the IP address of the DNS server in the **IPv4 Address** field.
9. Select the VLAN ID from the **Uplink VLAN** drop-down list. This list displays all uplink VLANs except LTE uplink VLAN. VLAN 4095 is not displayed in the list.
10. Click **Save Settings**.

Configuring Redirect DNS Servers

Aruba Gateways can redirect DNS queries to dedicated DNS servers configured for the corporate and public domains. You can use this feature to optimize the load on the corporate DNS servers by splitting and redirecting non-corporate traffic to a separate DNS server configured on the Branch Gateway.

Before enabling DNS traffic redirection, ensure that the Branch Gateway is configured as a DNS server. To configure Branch Gateway as the DNS server, go to **Interfaces** > **DHCP** > **IP Pool** and set Gateway address as the DNS server.

The Redirect DNS Servers can be configured at the device and group level for both Branch Gateways and VPNCs.

To enable devices to redirect DNS queries, and to configure name servers for specific domains, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **General**.
4. Click **Domain Name System**.
5. Enable DNS name resolution.
6. Click the **Redirect DNS** toggle switch.
7. To add domains, click the **+** icon in the **Domains to Redirect** table.
8. Enter the following information in the **New Redirect DNS Server** pop-up window:
   - **Domain**—Enter the domain name.
   - **IP Version**—Select the IP version.
   - **IP address**—Enter the IP address of the DNS server to be redirected for the specified domain name.

You can configure up to three IPv4 and three IPv6redirect DNS servers.

9. Click **Save Settings.**

Configuring Dynamic Domain Name System

Dynamic DNS, also known as DDNS, solves the problem of ever changing IP addresses by associating your address with a consistent domain name without the need for a static IP.

The dynamic IP addresses assigned through a DHCP server frequently change, as the ISPs manage their own online systems. This makes it difficult to access the Branch Gateway if the DHCP issued address continues to change without notice.

The dynamic DNS feature assigns a custom domain name to your home IP address that updates automatically whenever your home IP changes. A device on your network periodically communicates your IP to the dynamic DNS service. The domain name resolution changes as your IP changes. Thus, even if your IP changes, you can still connect to your device to the network using the same hostname.

The Dynamic Domain Name System configuration can be done at the device and group level for both Branch Gateway and VPNC.

To configure Aruba Gateways to connect to a dynamic DNS server, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.

1. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
2. Click **System** > **General**.
3. Expand the **Dynamic Domain Name System**.
4. Specify the **Server interval** and **Server IP** values.
5. Select one of the following values for **Authentication type**:
   - **hmac-md5**
   - **hmac-sha1**
   - **hmac-sha256**

6. Enter appropriate values in **Authentication name** and **Authentication key** for the specified authentication type.
7. Click the edit icon next to **DHCP pools** to from the Available DHCP Pool list.
8. Click **OK**.
9. Save the changes.

Configuring Dynamic Domain Name System (HTTPS)

A dynamic DNS keeps the DNS records up-to-date automatically when an IP address changes. The branch gateway receives the IP address from the specified WAN interface and communicates to the DDNS service provider via an HTTPS connection to maintain the confidentiality of the information over the internet.

To enable Aruba Gateways to connect to a dynamic DNS server over an HTTPS connection, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **General**.
4. Expand **Dynamic Domain Name System (HTTPS)**.
5. To create a Dynamic DNS Server, click the **+** icon in the **DDNS Servers** table.
6. Select one of the following DDNS service providers from the **Provider name** drop-down list:
   - **DynDNS**
   - **Noip**
   - **ChangeIP**
7. Enter the host name of the gateway in the **Hostname & domain (FQDN)** field.
8. Enter the user name in the **Username** field.
9. Enter the password and retype the password in the respective fields.

10. Select the uplink VLAN from the **WAN Interface VLAN** drop-down list.
11. Click **Save Settings**.

Setting Capacity Threshold

You can set capacity thresholds for Gateways to trigger alerts when they exceed the set percentage of the total capacity configured for its resources.

Capacity Threshold configuration can be done at the device and group level for both Branch Gateway and VPNC.

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **General**.
4. Expand **Capacity Threshold**.
5. Configure the threshold parameters listed in the following table as per your requirement.

Table 241: *Capacity Alert Thresholds*

Category	Description
Datapath CPU	Sets an alert threshold for datapath CPU capacity. When the total datapath CPU capacity exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 30%.
Controlpath CPU	Sets an alert threshold for controlpath CPU capacity. When the total controlpath CPU capacity exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 45%.

Category	Description
Controlpath memory	Sets an alert threshold for controlpath memory consumption. When total memory capacity exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 85%.
Total tunnels	Sets an alert threshold for the tunnel capacity. When the total tunnel capacity of the device exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 80%.
Total users	Sets an alert threshold for the user capacity. When the total resource capacity of the device exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 80%.

Configuring Device Administrator Credentials for Aruba Gateways

The Gateway administrator or a management user referred in this topic denotes a user who can access the device user interface for troubleshooting purposes. We need to configure credentials for these administrators to access the Aruba Gateway user interface for troubleshooting device specific issues. The Aruba Central system administrators or other Aruba Central system users need not be the management users of the Gateway device user interface or console.

For more information about configuring and managing users, refer to the following topics:

- Configuring Management User Accounts for Aruba Gateways
- Configuring Management User Authentication Options
- Configuring Servers for Management User Authentication

The management user of Aruba Gateways have restricted to access and troubleshoot only the device related issues through the device user interface. Any other tasks such as configuration, management, or device upgrade for a Gateways can be performed only from the Aruba Central UI.

Configuring Management User Accounts for Aruba Gateways

To create a management user account, complete the following steps:

1. To configure a management user account, select one of the following options:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.

c. Click a gateway under **Device Name**.
   The dashboard context for the gateway is displayed.
d. Under **Manage**, click **Device**.
   The gateway device configuration page is displayed.

2. Click **System** > **Admin**.
3. Under **Management User**, enable the **Enable local authentication** toggle switch.
4. Click the **+** icon from the **Management User** table.
5. Enter values for **Username** and **Password**.
6. Select a role from the drop-down list.
7. Click **Save Settings**.

Creating a New User with Certificate Authentication

This section describes the steps to create a new user with certificate authentication.

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **System** > **Admin** > **Management User**.
3. Click **Show users with certificate authentication**.
4. Click the **+** icon in the **Management Users with Certificate Authentication** table.
5. In the **Management Users with Certificate Authentication > New User** section, complete the following steps:
   a. Select one of the following options from the **Interface to connect** drop box:
      - **WebUI**—Select this option to enable only the WebUI authentication and configure **Username**, **Role**, **Trusted CA certificate name**, and **Client certificate serial number**.
      - **CLI through SSH**—Select this option to enable only CLI through SSH and configure **Username**, **Role**, **Client Certificate**, and **Revocation checkpoint**.
      - **WebUI & CLI through SSH**—Select this option to enable both WebUI authentication and CLI through SSH and configure all the required parameters.

The default username and password to login to the device using the CLI or user interface are admin and admins respectively.

6. Click **Save Settings**.

Enabling Console Block

To enable console block, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **System** > **Admin**.
3. Under **Management User**, select **Enable console block**. Disabling this option locks down all console ports such as micro USB and mini USB on the Gateways to enable high level security.
4. Click **Save Settings**.

Configuring Management User Authentication Options

The Gateway supports client certificate authentication for users accessing the user interface. (The default is for username and password authentication.) You can use client certificate authentication only or client certificate authentication with username and password (if certificate authentication fails, the user can log in with a configured username and password).

To configure management user authentication options, complete the following steps:

1. Select one of the following options:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. Click **System** > **Admin**.
3. Click **Admin Authentication Options** and configure the following:
   - Select a **Default role** from the drop-down list. Options available are **root**, **read-only**, and **guest-provisioning**.
   - Select the **Enable** check box.
   - Select the **MSCHAPv2** check box, if it is the desired authentication method.
   - Select a **Server group** from the drop-down list. Options available are **default** and **internal**.
   - Select the **Management telnet access** check box to enable management access through Telnet.
4. Click **Save Settings**.

Configuring WebUI Authentication

To configure the **WebUI authentication** for management users, complete the following steps:

1. Select one of the following options:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

     The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the **List** view.
     c. Click **Config**.

     The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.

     The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.

     The gateway device configuration page is displayed.
2. Click **System** > **Admin**.
3. Click **Admin Authentication Options**.

4. Under **WebUI Authentication**, make the following changes:
   - Select the **Username/password** check box if you do not want to use certificate authentication for WebUI management.
   - Select the **Webui HTTPS port (443) access** check box.
   - Select the **Client certificate** check box to use certificate authentication for WebUI management.
   - Select the server certificate to be used for this service from the **Server certificate** drop-down.
   - Enter a value for **Idle session timeout** in minutes or seconds.
   - Enter a value for **Re-authentication timeout** in minutes or seconds.
5. Click **Save Settings**.

Configuring SSH Authentication for CLI Access

Aruba Gateways support public key authentication of users who access the device using SSH. (The default is for username and password authentication).

Enabling Ciphers and MAC Algorithms

You can configure SSH to enable or disable the following ciphers and MAC algorithms based on your preference:

- AES-CBC
- AES-CTR
- HMAC-SHA1
- MAC-SHA1-96

By default, all the algorithms are enabled. However, the Gateway allows you to enable or disable a specific cipher or the HMAC-SHA1-96 authentication algorithm using the WebUI.

To enable or disable a cipher encryption, complete the following steps:

1. Select one of the following options:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **System** > **Admin** > **Admin Authentication Options**.

3. Under **SSH (Secure Shell) Authentication Method**, select **AES-CBC**, **AES-CTR**, or **Both** as the encryption option.
4. Click **Save Settings**.

To enable or disable HMAC-SHA1-96 authentication:

1. Select one of the following options:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.

Configuring Servers for Management User Authentication

You can use an external authentication server or the internal user database of Gateways to authenticate management users.

For more information on configuring authentication servers and server groups, refer to the following topics:

- Configuring RADIUS Authentication Server on Aruba Gateways
- Configuring Other External Authentication Servers on Aruba Gateways
- Configuring Server Groups

Configuring Servers for Management User Authentication

You can use an external authentication server or the internal user database of Gateways to authenticate management users.

For more information on configuring authentication servers and server groups, refer to the following topics:

- Configuring RADIUS Authentication Server on Aruba Gateways
- Configuring Other External Authentication Servers on Aruba Gateways
- Configuring Server Groups

Configuring Switching Parameters

To avoid bridge loops between network nodes and to maintain a single active path between the network nodes, you may want to enable Spanning Tree for the VLANs.

To enable Spanning Tree and other switching parameters on Branch Gateways, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **Switching**.
4. Expand Spanning Tree and configure the parameters described in the following table:

Table 242: *Switching Parameters*

Code	Description
Spanning Tree	Enable Spanning Tree.
Mode	Select one of the following Spanning Tree modes: ■ **Rapid**— RSTP takes advantage of point-to-point links and provides rapid convergence of the Spanning Tree. RSTP is enabled by default on all Branch Gateway devices. RSTP provides rapid convergence when interfaces are configured as either edge ports or point-to-point links. ■ **Rapid-PVST**—Rapid-PVST provides load-balancing of VLANs across multiple ports, resulting in optimal usage of network resources. Rapid-PVST also ensures interoperability with industry-accepted Rapid-PVST protocols. Rapid-PVST is disabled by default.
Forward Time	Specify the number of seconds that the port must spend in listening and learning states before forwarding packets. The value must be within a range of 4–30.
Hello Time	Specify a keep alive interval for BPDU within a range of 1-10.
Max Age	Specify a waiting interval in seconds for the root bridge to receive a hello packet before changing the STP topology. This allows the protocol to determine if a port is currently unusable for forwarding. The value must be within a range of 6-40.
Priority	Specify a value for priority to determine if a bridge must act as a root. The priority value must be within a range of 0-65536, with 0 being the highest priority.

Table 242: *Switching Parameters*

Code	Description
LACP	Specify a value for **Priority**. When the LACP priority is configured, the LACP data units exchange their corresponding system identifier or priority along with their port key or priority. This information determines the LAG of a port. The LAG for a port is selected based on its keys. The port is placed in that LAG only when its system ID or key and system ID or key of its partner matches the other ports in the LAG (if the group has ports). LACP is disabled by default.

Configuring AMON Receivers for Aruba Gateways

You can configure Gateways to send Aruba Monitoring (AMON) feeds to the Aruba ALE server or Aruba IntroSpect for data processing and analytics. When configured, Gateways constantly feed the receivers with the real-time application data and firewall logs.

To configure the AMON receivers on Gateways, complete the following steps:

1. Select either of the following options:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** >**External Monitoring**.
4. Click **AMON**.
5. Click the **+** icon to add a new **AMON destination**.
6. Select one of the following AMON receivers from the **Type** drop-down.
   - **ALE**—To send AMON feeds to the ALE server.
   - **IntroSpect**—To send AMON feeds to a server on which the Aruba IntroSpect Analyzer application is installed.
7. Enter the IP address of the AMON receiver.

8. Click **Save Settings**.

For AMON data logging, ensure that the Deep Packet Inspection and Firewall Visibility features are enabled on Gateways.

Configuring VLANs on Aruba Gateways

As a layer 2 switch, the Branch Gateway requires an external router to route traffic between VLANs. The Branch Gateway can also operate as a layer 3 switch that can route traffic between VLANs.

You can configure one or more physical ports on the Branch Gateway to be a member of a VLAN. Additionally, each wireless client association constitutes a connection to a virtual port on the Branch Gateway, with membership in a specified VLAN. You can place all authenticated wireless users into a single VLAN or into different VLANs, depending on your network requirements. You can also configure an IP address and netmask for a VLAN. The IP address is *up* when at least one physical port in the VLAN is up. The VLAN IP address can be used as a gateway by external devices; packets that are not destined for the Branch Gateway and directed to a VLAN IP address are forwarded according to the Branch Gateway's IP routing table.

For the SD-WAN deployment, each Branch Gateway requires VLAN interfaces for WAN uplinks and LANs. Each VLAN must have a unique VLAN ID assigned to it. By default, the Branch Gateways are pre-configured with the VLAN 4094.

See the following topics for instructions on configuring VLANs:

- Adding VLANs for Aruba Gateways
- Configuring VLANs for WAN Interfaces
- Configuring VLANs for LAN Interfaces
- Configuring Other Parameters for VLAN

Adding VLANs for Aruba Gateways

Complete the following tasks to add VLANs to the Aruba Gateway and configure the VLAN parameters:

1. To configure Gateway group or Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.

d. Under **Manage**, click **Device**.

The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **VLANs**.
4. Click **+** from the **VLANs** table to add a new VLAN interface.
5. In the **New VLAN** window, specify the following parameters and save the changes:
   - **VLAN name**
   - **VLAN ID/Range**

Configuring VLANs for WAN Interfaces

To configure VLAN for WAN interfaces on a Branch Gateway or a VPNC, complete the following steps:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

     The dashboard context for a group is displayed.

     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the **List** view.

     c. Click **Config**.

     The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the List view.

     c. Click a gateway under **Device Name**.

     The dashboard context for the gateway is displayed.

     d. Under **Manage**, click **Device**.

     The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface**> **VLANs**.
4. Select a VLAN from the **VLANs** table.
5. Select the WAN-facing VLAN ID from the **VLAN IDs** table.
6. Under the **IPv4** tab configure the following parameters:
   a. Select the **Enable routing** option.
   b. Select one of the following options from the **IP assignment** drop-down list.
      - **Static**
      - **DHCP**
      - **PPPOE**
        - Select the **NAT outside** check box to enable NAT only for the outbound traffic on public-facing egress VLAN interfaces. When this feature is enabled on an uplink VLAN interface, the source address is translated with the IP address of the VLAN interface to all the outbound traffic. Ensure that the NAT pool is configured for source NAT IP allocation. For more information see, Configuring NAT Pools.

7. Save the changes.

Configuring VLANs for LAN Interfaces

To configure VLAN for LAN interfaces on a Branch Gateway, complete the following steps:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface**> **VLANs**.
4. Select a VLAN from the **VLANs** table.
5. Select the WAN-facing VLAN ID from the **VLAN IDs** table.
6. Under the **IPv4** tab configure the following parameters:
   a. Select the **Enable routing** option.
   b. Select **Static** from the **IP assignment** drop-down list. If you configure the VLANs at the group level, you can also choose **Dynamic DHCP Pool**. This option is not applicable for device level configuration.
   c. Enable **Relay to external** option.
   d. Add the IP address of the RADIUS server to which you want to relay the DHCP requests in the **DHCP helper** table.
   e. Under **Other option**, ensure to apply a AAA profile to the VLAN from the **AAA Profile** drop-down list. Alternately, you can assign a AAA profile to the VLAN interface from the **Apply Policies** tab under **Gateway Management** > **Security**. For more information, see Assigning AAA profile to VLAN Interfaces for Role Assignment.
7. Save the changes.

Configuring Other Parameters for VLAN

Complete the following tasks to configure the VLAN parameters:

1. To configure Gateway group or Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **VLANs**.
4. To configure the parameters for a VLAN ID, select the required VLAN from the **VLANs** table. The **VLAN IDs** table is displayed.
5. From the **VLAN IDs** table, select a VLAN that you want to configure. The VLAN details are displayed in the following tabs:
   - **IPv4**
   - **Port Members**
6. To add or modify the port members associated to a VLAN ID, complete the following tasks:
   a. Select the **Port Members** tab.
   b. Click **Edit**. The **Available/Selected Ports** window is displayed.
   c. Select the required ports from the list of available ports and click **OK**.
7. Select the **IPv4** tab to configure the other VLAN parameters as described in Table 243 based on your network requirements.
8. Save the changes.

Table 243: *VLAN IPv4 Tab Parameters*

Parameter	Description
IP Assignment	
Enable routing	Enable this option to route traffic between the VLANs that are mapped to the IP subnetworks.
IP assignment	Select one of the following IP assignment types for the Aruba Gateways to select the system IP address: ▪ **Static**—Specify an IP address in the **IPv4 address** field. You can also optionally enable the following DHCP settings: ◦ **Act as DHCP server**—Enables the device to act as a DHCP server with the specified **Network**, **Netmask**, **Pool name**, **Default router**, **DNS servers**, and **Netbios name**

Parameter	Description
	server configurations. ◦ **Relay to external**—Relays the DHCP requests for the interface to the external DHCP servers configured in the **DHCP helpers** table. You need not configure this parameter if the VLAN interface is in the same subnetwork as that of the DHCP server. ■ **DHCP**—Specify the **Client ID** for the DHCP client. ■ **PPPoE**—Configure the PPPoE server credentials in the **Service name**, **User name**, **Password**, and **Retype password** fields. To configure CHAP secret, enable **Configure CHAP Secret** and enter CHAP secret key. Based on the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. When you enable CHAP authentication on VLAN interface, the interface and its peer use the CHAP secret key for mutual authentication. ■ **Dynamic DHCP Pool**—Select a DHCP pool from the **Dynamic DHCP pool** drop-down list. You can also optionally enable the **Relay to external** setting to relay the DHCP requests for the interface to the external DHCP servers. You can add the DHCP server IP addresses in the **DHCP helpers** table. You need not configure this parameter if the VLAN interface is in the same subnetwork as that of the DHCP server. ■ **Gateway Pool**—Select the required gateway pool from the **VLAN pool** drop-down list. **NOTE: Dynamic DHCP Pool** and **Gateway Pool** options are applicable only for group level configurations and not for device level configuration.
MTU	Provide the MTU setting for the VLAN. The allowed range is 1280-1500. The default value is 1500.
Suppress ARP	Select this option to prevent flooding of ARP broadcasts on all the untrusted interfaces. By default, this is disabled. **NOTE:** This option is not applicable if you selected **DHCP** or **PPPoE** as the **IP assignment** option.
VLAN status	Select this option to enable the operational state of the VLAN ID. By default, this is disabled. Enabling this option keeps the state of the VLAN interface as up irrespective of the state of the physical interface.
NAT inside	Select this option to perform NAT with the desired IP address of the VLAN interface as the source address.
NAT outside	Select this option to enable NAT only for the outbound traffic on public-facing egress VLAN interfaces. When this feature is enabled on an uplink VLAN interface, the source address is translated with the IP address of the VLAN interface to all the outbound traffic. Ensure that the NAT pool is configured for source NAT IP allocation. For more information see, Configuring NAT Pools.
Admin state	Select this option to enable the admin state of the VLAN interface.
Other Option	
Description	A text string to describe the VLAN interface.
Local-proxy ARP	Select this option to activate the local proxy ARP feature on the interface. **NOTE:** From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch gateways,

Parameter	Description
	with proxy-ARP enabled, can now be configured to either respond to ARP requests with their own MAC address or the MAC address of any client in the user table.
Broadcast multicast optimisation	Select this option to enable controlled flooding of broadcast or multicast traffic without compromising the client connectivity.
Bandwidth contract	Select the bandwidth contract policy to be applied to the VLAN interface. The selected contract policy limits both broadcast and multicast traffic on the interface.
Enable OSPF	Select this to enable OSPF protocol on the interface and configure the following OSPF parameters: ■ **Area network (eg. 0.0.0.0)** ■ **Authentication** ■ **Password** ■ **Retype password** ■ **Cost [1-65535]** ■ **Dead interval [1-65535]** ■ **Hello interval [1-65535]** ■ **Priority [0-255]** ■ **Retransmit interval [1-65535]** ■ **Transmit delay [1-65535]**
AAA profile	Select a AAA profile to be applied to the VLAN interface. Alternately, you can assign AAA profiles to the VLAN interfaces from the **Apply Policies** tab under **Gateway Management** > **Security**. For more information, see Assigning AAA profile to VLAN Interfaces for Role Assignment.
ACL	Select a routing policy to be applied to the VLAN interface. Alternately, you can assign routing policies to the VLAN interfaces from the **Apply Policies** tab under **Gateway Management** > **Security**. For more information, see Applying Route ACLs for VLAN Interfaces.

Configuring SLB using NAT

Server Load Balancing (SLB) is a key feature in today's network deployments. It improves scalability of servers with increasing session loads. Aruba uses NAT to offer Load Balancing feature, where session load can be distributed across a pool of servers, instead of directing to a single server. NAT also enhances security by hiding the real IP address of the source and provides more flexibility to move source across IP pools. You can also configure health-check parameters to keep a tab on the performance.

Configuring Health-Check Profile

To configure a health-check profile, complete the following steps:

1. Configure health-check profile for a Branch Gateway or a Branch Gateway group:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.

     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **SLB**.
4. Click **+** in the **Health-check configuration** table. The **Create Health-check** table is displayed.
5. Provide the following details in the Create Health-Check table:
   a. Enter a **Profile name**.
   b. **Frequency (secs)**—Indicates how often the Branch Gateway checks to see if the server is up and running. Default: 5 seconds.
   c. **Timeout (secs)**—Indicates the number of seconds the Branch Gateway waits for a response to its health check query before marking the health check as failed. Default: 2 seconds.
   d. **Retry count**—Is the number of failed health checks after which the managed device marks the server as being down. Default: 2.
6. Click **Save Settings** to add the new health check profile.

Configuring an SLB Server Group

To configure a server group, perform the following task:

1. Configure SLB server group on a Branch Gateway or a Branch Gateway group:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

     The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the **List** view.
     c. Click **Config**.

     The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.

     The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.

     The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **SLB**.
4. Click **+** in the **Server groups** table. The **Create Server Group** table is displayed.
5. Provide the following details in the **Create Server Group** table:
   a. Enter a **Group name**.
   b. In the **Health-check profile** drop-down list, select a health check profile.
6. Click **Save Settings**.

Configuring an SLB Server

To configure a server, perform the following task:

1. Configure SLB server for a Branch Gateway or a Branch Gateway group:
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **SLB**.
4. Click **+** in the **Servers** table. The **Create Server** table is displayed.
5. Provide the following details in the **Create Server** table:
   a. Enter a **Server name**.
   b. **Server group**—Use the drop-down list to assign this server to a group from the existing configured groups.
   c. **Server mode**—Use the drop-down list to choose the mode (bridge, nat, or route)as per your network requirement.
      - For **bridge** mode, enter the **Trusted Port** number (the port connected to the trusted side of the SLB server) and the **Untrusted Port** number (the port connected to the untrusted side of the SLB server).
      - For **nat** mode, enter the **Trusted IP Address** (the trusted interface on the SLB server) and the **NAT Destination Port** number (the port to which a packet is redirected to rather than the original destination port in the packet). You can enable **Health-Check** on the trusted IP address interface.
      - For **route** mode, enter the **Trusted IP Address** (the IP address of the trusted interface on the SLB server device) and the **Untrusted IP Address** (the IP address of the untrusted interface on the SLB server device). You can enable **Health-Check** on either or both of these interfaces.
6. Click **Save Settings**.

Configuring Ports

Physical ports on the Branch Gateways are trusted and are usually connected to internal networks by default. The untrusted ports connect to third-party APs, public areas, or other networks. When you define a physical port as untrusted, the traffic passing through that port needs to go through a predefined ACL policy.

Ports can also be classified as trusted or untrusted based on the VLAN interface associations. For example, traffic on the port is trusted only if the VLAN interface associated to that port is trusted. When a port and its associated VLANs are untrusted, any incoming and outgoing traffic must pass through a predefined ACL. For example, you can configure an Ethernet port as an untrusted access port; assign VLANs and classify them as untrusted; and designate a policy through which VLAN traffic on this port must pass. This configuration is useful if your business provides wired user guest access and you want the guest user traffic to pass through an ACL and connect to captive portal.

NOTE

LAN ports are configured as untrusted so that users are authenticated using AAA profile. WAN ports do not require users to authenticate and hence are configured as trusted ports.

You can set a range of VLANs as trusted or untrusted in trunk mode.

The following table lists the trusted or untrusted ports, VLAN configuration, and the impact on the network:

Table 244: *Classifying Trusted and Untrusted Traffic*

Port	VLAN	Traffic Status
Trusted	Trusted	Trusted
Untrusted	Untrusted	Untrusted
Untrusted	Trusted	Untrusted
Trusted	Untrusted	Untrusted

See the following topics to know how to configure ports:

- Adding Ports
- Configuring Ports for LAN Interfaces
- Configuring Ports for WAN Interfaces
- Configuring Other Parameters for Port

Adding Ports

Complete the following tasks to add ports to the Aruba Gateway and configure the port parameters:

1. To configure Gateway group or Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interfaces** > **Ports**.

4. Click **+** from the **Ports** table to add a new port.
5. From the **New Port** window, select the required ports to be added to the **Ports** table and save the changes.

Configuring Ports for LAN Interfaces

To configure ports for LAN interfaces at the device or group level, complete the following steps:

1. To configure a gateway group or gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interfaces** > **Ports**.
4. Select the port from the **Ports** table.
5. Select the port type as **LAN**.
6. Clear the **Trust** check box to set the port to **Untrusted**.
7. To apply a policy to the LAN interface, select one of the following options from the **Policy** drop-down list:
   - **Inbound and Outbound**—Select this option to apply a firewall policy of the incoming and outgoing traffic.
   - **Per-Session**—Select this option to apply a firewall policy for the session.
8. Select the port mode. You can set ports to either access mode or trunk mode.
   - **Access**—By default, ports are set to access mode to carry traffic only for the VLAN to which they are assigned. For Access mode, select the VLAN and the **VLAN trust** check box. To apply a policy for the VLAN traffic on access port, see Applying Policies for VLANs on Access Ports.
   - **Trunk**— In trunk mode, a port can carry traffic for multiple VLANs. When the **Trunk** mode is selected, specify whether the port must carry traffic for all VLANs configured for the branch or for specific VLANs only. You can also configure the native VLAN for a port. To apply a policy for VLANs in trunk mode, see Applying Policies for VLANs on Trunk Ports.
9. Save the changes.

NOTE

Ensure to apply a AAA profile to the VLANs that are assigned to the port. For more information, see Assigning AAA profile to VLAN Interfaces for Role Assignment.

Configuring Ports for WAN Interfaces

To configure port for WAN interfaces at the device or group level, complete the following steps:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interfaces** > **Ports**.
4. Select a port from the **Ports** table. The port details are displayed.
5. Select the port type as **WAN**.
6. Select the **Trust** check box.
7. To apply a policy to the WAN interface, select one of the following options from the **Policy** drop-down list:
   - **Inbound and Outbound**—Select this option to apply a firewall policy for the incoming and outgoing traffic.
   - **Per-Session**—Select this option to apply a firewall policy for the session.
8. Select the port mode. You can set ports to either access mode or trunk mode.
   - **Access**—By default, ports are set to access mode to carry traffic only for the VLAN to which they are assigned. For Access mode, select the VLAN and the **VLAN trust** check box. To apply a policy for the VLAN traffic on access port, see Applying Policies for VLANs on Access Ports.
   - **Trunk**— In trunk mode, a port can carry traffic for multiple VLANs. When the **Trunk** mode is selected, specify whether the port must carry traffic for all VLANs configured for the branch or for specific VLANs only. You can also configure the native VLAN for a port. To apply a policy for VLANs in trunk mode, see Applying Policies for VLANs on Trunk Ports.
9. Save the changes.

Configuring Other Parameters for Port

Complete the following tasks to configure the port parameters:

1. To configure a gateway group or gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interfaces** > **Ports**.
4. To configure the port parameters, select the required port from the **Ports** table. The port details are displayed.
5. Configure the parameters described in Table 245 as per your network requirements.
6. Save the changes.

Table 245: *Port Parameters*

Parameter	Description
Basic Options	
Type	Select the port type as WAN or LAN for WAN interface and LAN interface respectively.
Admin state	Select this option to set the user state of the port interface as admin.
Speed	Select one of the following values (Mbps) for speed operation of the port: ▪ **10** ▪ **100** ▪ **1000** ▪ **auto**
Duplex	Select one of the following values for duplex operation of the port: ▪ **auto** ▪ **half** ▪ **full**

Parameter	Description
PoE	Enable this option to set the port interface as a PoE source.
Trust	Enable this option to configure the port as a trusted interface.
Policy	Select one of the following options from the drop-down list: ▪ **Inbound and Outbound**—Select this option to apply a firewall policy for the incoming and outgoing traffic. ▪ **Per-Session**—Select this option to apply a firewall policy for the session.
Mode	Select the port mode. You can set ports to either access mode or trunk mode. ▪ **Access**—By default, ports are set to access mode to carry traffic only for the VLAN to which they are assigned. For Access mode, select the VLAN and the **VLAN trust** check box. To apply a policy for the VLAN traffic on access port, see Applying Policies for VLANs on Access Ports. ▪ **Trunk**— In trunk mode, a port can carry traffic for multiple VLANs. When the **Trunk** mode is selected, specify whether the port must carry traffic for all VLANs configured for the branch or for specific VLANs only. You can also configure the native VLAN and session firewall policy on a port. To apply a policy for VLANs in trunk mode, see Applying Policies for VLANs on Trunk Ports.
VLAN	Select the VLAN interfaces that you want to associate to the port.
VLAN trust	Enable this option to set the VLAN interface as trusted.
VLAN policy	The firewall policy that is applied to the trusted VLAN which is associated to the port. You can apply firewall policies only for trusted VLANs. For more information on applying VLAN policies, see Applying Policies to Gateway Interfaces.
Description	Optional text string to describe the port interface.
Tunneled node	Select this option to enable tunneled node capability for the port interface. By default, this is disabled. The tunneled node connects to one or more client devices at the edge of the network to establish a secure GRE tunnel.
Jumbo MTU	Select this option to enable Jumbo frame MTU configured on the interface. This setting is functional only if the Jumbo frame processing is enabled in the firewall policies.
Advanced Options **NOTE:** The following advanced options appear only if you click the **Show advanced options** link below the **Ports** table.	
Port monitoring	Select this to enable the switch to send a copy of all network packets seen on one port to another port.
Spanning tree	Select this option to enable spanning tree protocol on the port. This is enabled by default.
Spanning tree cost	Specify the spanning tree path cost of the port. The allowed range is 1-65535. The default value is 2000.
Spanning tree priority	Specify the spanning tree priority of the port. The allowed range is 0-255. The default value is 128.

Parameter	Description
Spanning tree port fast	Select this option to enable forwarding of traffic from the port. By default, this option is disabled.
Spanning tree point-to-point	Select this option to enable the port as a point-to-point link. By default, this option is disabled.
Spanning tree BPDU guard	Enable BPDU guard to protect the port from receiving STP BPDUs. However, the port can transmit STP BPDUs.
LLDP transmission	Enable this option if you want the port to transmit LLDP packets and configure the following LLDP transmissions parameters: ■ **Transmit interval**—Specify the interval between LLDP TLV transmission in seconds. The supported range is 1-3600 seconds and the default value is 30 seconds. ■ **Transmit hold**—Enter a value from 1-100. This value is multiplied by the transmit interval to determine the number of seconds to cache the learned LLDP information before it is cleared. If the transmit-hold value is at the default value of 4, and the transmit interval is at its default value of 30 seconds, then the learned LLDP information is cached for 4 x 30 seconds, or 120 seconds. ■ **Fast transmit interval**—Set the LLDP fast transmission interval in seconds. The supported range is 1-3600. The default value is 1. ■ **Fast transmit hold**—Enter a value from 1-100. This value is multiplied by the fast transmit interval to determine the number of seconds to cache the learned LLDP information before it is cleared. If the fast transmit-hold value is at the default value of 4, and the fast transmit interval is at its default value of 1 second, then the learned LLDP information is cached for 4 x 1 seconds, or 4 seconds.
LLDP reception	Select this option to enable the port to receive LLDP packets.
LLPD-MED	Select this option to enable LLDP-MED on the port.
Port security	Set or limit the number of MAC addresses learnt on the port. The allowed range is 1-16384.

Configuring Uplinks

Uplinks connect Branch Gateways to underlay networks. By default, both wired and cellular uplinks are set as active links with load balancing enabled on Branch Gateways. Branch Gateways support a total of five uplinks which include four wired uplinks and one cellular uplink.

Uplink Load Balancing

An uplink can be configured as an active uplink or as standby. The uplink load balancing feature supports both active and standby uplinks, for example, traffic can be load balanced across two wired uplinks, while the backup cellular uplink remains idle and is used when a wired link fails. When a Branch Gateway has multiple active uplinks, uplink load balancing can modify the Internet Key Exchange (IKE) parameters for the Branch Gateway to create multiple IPsec tunnels, one on each uplink. When multiple uplinks and IPsec tunnels are up, the layer 3 traffic can be load-balanced across these uplinks using internal routing ACLs and next hop lists.

WAN Bandwidth Optimization

Data compression reduces the size of data frames that are transmitted over a network link. This in turn reduces the time required to transmit the frame across the network. IP payload compression is one of the key features of the WAN bandwidth optimization solution, which consists of the following elements:

- IP Payload Compression
- Tunnel bandwidth negotiation
- Traffic Management and Quality of Service (QoS)
- Caching

IP Payload Compression

NOTE

WAN optimization through IP payload compression is not supported on 7205 Branch Gateway.

Branch Gateways can send traffic to destinations other than the corporate headquarters on the same link; therefore payload compression is enabled on the IPsec tunnel between the Branch Gateway and VPNC. Dynamic compression is used for the IP payload to achieve a high compression ratio. However, compression is not applied to data, for example, an embedded image file that may already be in a compressed format.

Tunnel Bandwidth Negotiation

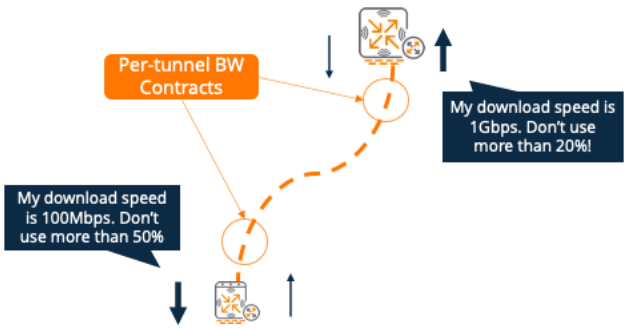
The Gateways at the tunnel endpoints, perform tunnel bandwidth negotiation with each other, to ensure that the Gateways at the tunnel endpoints exchange their respective WAN speed and maximum bandwidth threshold values with each other. This is done to ensure that one Gateway does not send more traffic than the other Gateway can ingest.

During the tunnel bandwidth negotiation, the tunnel endpoints inform each other about the maximum bandwidth they can ingest based on the value configured in the **Speed** field and the percentage configured in the **Tunnel max bandwidth threshold** field of the Gateway uplink configuration. For more information, see Configuring an MPLS, Metro-Ethernet, or an INET Uplink.

The VPNC assigns a bandwidth contract with the tunnel to control the tunnel traffic based on traffic priority. Traffic in the high priority queue is handled first, followed by the low priority queue. Therefore, the management-plane traffic or the traffic marked as high in any session-based policy takes precedence over the rest of the traffic.

The following figure illustrates a scenario where the Gateways at both ends of a tunnel negotiate the bandwidth each other can ingest.

Figure 185 *Tunnel Bandwidth Negotiation*



Configuring Uplink Interfaces on Branch Gateways

To configure uplink interfaces on Branch Gateways, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete one of the following steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Go to **WAN** > **Uplink**. The **Uplink** configuration page opens.
4. To enable data compression, select the **Compression** check box.
5. Select any one of the following load balancing modes:
   - **Round Robin**—To equally distribute traffic among all active uplinks on a round robin basis. By default, Branch Gateway uses the round robin mode for balancing load across uplinks.
   - **Session Count**—To balance traffic among the uplinks based on the number of sessions managed by each link, so that the load for each active uplink stays within 5% of the other active uplinks. For example, if there are two active uplinks with the **Weight** parameter defined as 10 and 20, the active uplink with a weight of 20 will have more sessions assigned.
   - **Uplink utilization**—To distribute traffic between active WAN uplinks based on the utilization % of each active WAN uplink. Uplink utilization considers the link speed to calculate the utilization and allows a maximum percentage of bandwidth threshold to be defined. When the bandwidth threshold exceeds, the WAN uplink is no-longer considered for session allocation.
6. To calculate the available bandwidth for the uplinks, select the **Bandwidth Estimation** check box. The periodic computation of the actual available Internet bandwidth in both directions helps administrators ensure better control of application performance at the branch even when the bandwidth keeps changing over the internet. When the bandwidth estimation feature is enabled, the available bandwidth is measured by synthesizing traffic and calculating an average for a specific time duration. To view the average bandwidth estimated for your sites, see the WAN Health—Site dashboard.
7. To add an uplink, click **+** in the **Uplink VLANs** table and enter the following values to define an uplink VLAN for an uplink interface on the Branch Gateway:

- **Link Type**—Select any one of the following types of uplink:
  - **MPLS**—MPLS network
  - **INET**—Internet
  - **LTE**—4G cellular network
  - **Metro-Ethernet**—Ethernet network in a metropolitan area

Configuring an MPLS, Metro-Ethernet, or an INET Uplink

To configure an MPLS, or a Metro-Ethernet, or an INET uplink, select the uplink type from the drop-down list, and enter details for the parameters provided in the following table:

Table 246: *MPLS, Metro-Ethernet, or an INET Uplink Configuration Parameters*

Parameter	Description
Link Name	Specify the name of the uplink.
Interface VLAN ID	Specify the VLAN ID that you want to assign to the uplink.
Operation state	Use this check box to disable or re-enable the uplink. By default, uplinks are enabled.
Use only as backup link	By default, all uplinks operate as active uplinks. If you want to use the uplink in the standby mode, select this check box.
Bandwidth Percentage	Use this field to configure bandwidth percentage for uplink utilization. This field is available only for the **Uplink utilization** load balancing mode.
Speed	You can configure a custom value for uplink speed to optimize performance. The allowed range of values is 1–10000 Mbps. If not set, the WAN uplink speed defaults to auto-negotiated port speed for INET, MPLS, and Metro-Ethernet. Based on the speed and bandwidth threshold allowed for an uplink, Branch Gateways assign session traffic.
Weight	For Round Robin and Session Count load balancing modes, you can define a value for **Weight** within a range of 1–100. By default, this is set to 10. In an active-active uplink scenario, an uplink with a higher weight is assigned more session traffic than an uplink with a lower weight.
Tunnel max bandwidth threshold	To limit the amount of traffic transmitted from a Branch Gateway or a VPNC, configure the maximum transmit rate based on the WAN uplink bandwidth. For example, if the bandwidth of a WAN uplink is 15 Mbps and you want to limit the traffic transmission to 1.5 Mbps, you must configure the maximum bandwidth threshold as 10%. To apply the tunnel limits, a tunnel renegotiation followed by a tunnel flap is triggered on the Branch Gateway. **NOTE:** The maximum bandwidth threshold is applied on the VPNCs during the next tunnel rekey.

Configuring an LTE Uplink

To configure an LTE uplink, select **LTE** from the drop-down list, and enter details for the parameters provided in the following table:

Table 247: *LTE Uplink Configuration Parameters*

Parameter	Description
Link Name	Specify the name of the uplink.
Connection type	Specify one of the following connection types: ■ Wired ■ USB ■ Internal By default, **USB** is selected. **NOTE:** For a 9004-LTE Branch Gateway, the default connection type is **Internal**.
Interface VLAN ID	The VLAN ID assignment is not configurable for 4G LTE USB and Internal uplinks. By default, VLAN ID 4095 is assigned to the 4G LTE USB and Internal uplinks.
Low frequency probe	This is a global configuration for all LTE connections. Use this check box to enable less-frequent health check probing on the LTE uplink. LTE uplinks normally have lower bandwidth compared to wired uplinks, therefore you may want to enable less frequent probing on the LTE uplinks. When Low frequency probe is enabled, health check probes are sent every 15 seconds with a burst size of 2 packets for all LTE uplink interfaces configured on the Branch Gateway.
Use only as backup link	By default, all uplinks operate as active uplinks. If you want to use the uplink in the standby mode, select this check box.
Bandwidth Percentage	Use this field to configure bandwidth percentage for uplink utilization. This field is available only for the **Uplink utilization** load balancing mode.
Speed	You can configure a custom value for uplink speed to optimize performance. The allowed range of values is 1–10000 Mbps. If not set, the WAN uplink speed defaults to100 Mbps for LTE. Based on the speed and bandwidth threshold allowed for an uplink, Branch Gateways assign session traffic.
Weight	For Round Robin and Session Count load balancing modes, you can define a value for **Weight** within a range of 1–100. By default, this is set to 10. In an active-active uplink scenario, an uplink with a higher weight is assigned more session traffic than an uplink with a lower weight.
If you have selected **Internal** as the Connection Type, enter details for the following parameters:	
Active SIM slot	Select SIM 1 or SIM 2 as the active uplink.
Access point name (APN)	Enter the name of the Access Point to which the uplink connects.
Public land mobile network (PLMN)	A PLMN ID is a six digit ID which is a combination of Mobile Country Code and Mobile Network Code. Each service provider has their own PLMN code. This field allows you to restrict roaming. Select **Auto** or **Manual** for the PLMN mode. If you have selected **Manual**, enter the PLMN ID in the text box. By default, PLMN is on **Auto** mode.

Parameter	Description
Mode	Select one of the following network modes: ■ **Auto**—This mode keeps both 3G and 4G LTE options open and switches based on availability. ■ **4G LTE—**Connects to the 4G LTE cellular network and takes the default frequency band. ■ **3G—**Connects to the 3G cellular network and takes the default frequency band. ■ **Custom**—If you want to select one of the supported frequency bands for 3G and 4G LTE, select Custom. The following fields are displayed: ■ **3g band selection**—Select the desired 3G band from the drop-down list. ■ **4g LTE band selection**—Select the desired 4G LTE band from the drop-down list. **NOTE:** The frequency bands are specific to the internal modem and not the SIM. You will experience an interim disruption in the cellular connectivity when a frequency band is configured. The connection is established only if the frequency band is supported in your region.
Data Usage Tracking	Turn on the toggle switch to start tracking your data usage. If this field is enabled, the options to configure data usage limit and the Billing cycle are displayed.
Data usage alert limit	Enter the data limit in megabytes (Range – 1 to 65535 MB) to be used per month. Configure an alert in the **Alerts & Events** page for the alert to be generated when the data usage crosses the specified limit.
Monthly Billing start date	Select the day of the month on which the billing cycle begins.

8. Click **Save Settings**.

Configuring Uplink Interfaces on VPNCs

The SD-WAN Orchestrator requires uplink interfaces to be configured on both Branch Gateways and VPNCs for tunnel orchestration. For more information on configuration recommendations, see Configuring Overlay Network Using SD-WAN Orchestrator.

To configure uplink interfaces on VPNCs, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway complete one of the following steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **WAN** > **Uplink**.
4. To add an uplink VLAN, click **+** in the **Uplink VLANs** table.
5. Configure the following parameters:
   - **Link Type**—Select any one of the following uplink types:
     - **MPLS**—For the MPLS traffic
     - **INET**—For the Internet traffic
   - **Link Name**—Enter a name for the uplink interface.
     - For MPLS uplinks—The link name must match the link name configured for the MPLS uplink interface on Branch Gateways.
     - For INET uplinks—The link name need not be the same as the MPLS uplink name configured on Branch Gateways.
   - **Interface VLAN ID**—Enter the VLAN ID that you want to assign to the uplink interface.
   - **Private IP**—If **MPLS** is selected as the uplink type, enter a private IP address.

     By default, the IP address of the VLAN interface is used as the private IP address for both MPLS and INET uplinks. Private IP address for INET uplinks cannot be modified or overwritten.
   - **Public IP**—This field is available only for INET uplinks. Ensure that you define a public IP address that corresponds to the firewall NAT translation of the private IP address.
6. Click **Save Settings**.

Viewing Uplink Configuration

To view the current configurations of an uplink, use the `show uplink` command. For more information about the command, see The CLI Bank.

Managing 9004-LTE Branch Gateway

Aruba Central supports the 9004-LTE Branch Gateway model that comes with a default SD-WAN image. The recommended software version for 9004-LTE Gateway is ArubaOS 8.5.0.0-2.1.0.0.

The 9004-LTE Gateway comes with an inbuilt LTE modem. This integrated modem enhances performance in comparison to a dongle that needs to be connected to a USB port. This model provides a more efficient radio network, latency reduction, and improved mobility. The 9004-LTE Gateway has the capability of dual SIM and single radio.

Configuring Uplink Interfaces on a 9004-LTE Branch Gateway

1. To configure a Branch Gateway group or a Branch Gateway, complete one of the following steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Go to **WAN** > **Uplink**. The **Uplink** configuration page opens.
4. To add an uplink, click **+** in the **Uplink VLANs** table and select **LTE** from the **Link type** drop-down list.

   For detailed information, see Configuring an LTE Uplink.

The following table contains the new fields that need to be configured for 9004-LTE Gateway along with the existing fields:

Table 248: *Configuring an LTE Uplink on a 9004-LTE Gateway*

Parameter	Description
Link Name	Specify the name of the uplink.
Connection type	Specify one of the following connection types: ■ Wired ■ USB ■ Internal **NOTE:** For a 9004-LTE Branch Gateway, the default connection type is **Internal**.
Interface VLAN ID	The VLAN ID assignment is not configurable for 4G LTE USB and Internal uplinks. By default, VLAN ID 4095 is assigned to the 4G LTE USB and Internal uplinks.

Parameter	Description
Low frequency probe	This is a global configuration for all LTE connections. Use this check box to enable less-frequent health check probing on the LTE uplink. LTE uplinks normally have lower bandwidth compared to wired uplinks, therefore you may want to enable less frequent probing on the LTE uplinks. When Low frequency probe is enabled, health check probes are sent every 15 seconds with a burst size of 2 packets for all LTE uplink interfaces configured on the Branch Gateway.
Use only as backup link	By default, all uplinks operate as active uplinks. If you want to use the uplink in the standby mode, select this check box.
Bandwidth Percentage	Use this field to configure bandwidth percentage for uplink utilization. This field is available only for the **Uplink utilization** load balancing mode.
Speed	You can configure a custom value for uplink speed to optimize performance. The allowed range of values is 1–10000 Mbps. If not set, the WAN uplink speed defaults to 100 Mbps for LTE. Based on the speed and bandwidth threshold allowed for an uplink, Branch Gateways assign session traffic.
Weight	For Round Robin and Session Count load balancing modes, you can define a value for **Weight** within a range of 1–100. By default, this is set to 10. In an active-active uplink scenario, an uplink with a higher weight is assigned more session traffic than an uplink with a lower weight.
If you have selected **Internal** as the Connection Type, enter details for the following parameters:	
Active SIM slot	Select SIM 1 or SIM 2 as the active uplink.
Access point name (APN)	Enter the name of the Access Point to which the uplink connects.
Public land mobile network (PLMN)	A PLMN ID is a six digit ID which is a combination of Mobile Country Code and Mobile Network Code. Each service provider has their own PLMN code. This field allows you to restrict roaming. Select **Auto** or **Manual** for the PLMN mode. If you have selected **Manual**, enter the PLMN ID in the text box. By default, PLMN is on **Auto** mode.
Mode	Select one of the following network modes: ■ **Auto**—This mode keeps both 3G and 4G LTE options open and switches based on availability. ■ **4G LTE—**Connects to the 4G LTE cellular network and takes the default frequency band. ■ **3G—**Connects to the 3G cellular network and takes the default frequency band. ■ **Custom**—If you want to select one of the supported frequency bands for 3G and 4G LTE, select Custom. The following fields are displayed: ◦ **3g band selection**—Select the desired 3G band from the drop-down list. ◦ **4g LTE band selection**—Select the desired 4G LTE band from the drop-down list. **NOTE:** The frequency bands are specific to the internal modem and not the SIM. You will experience an interim disruption in the cellular connectivity when a frequency band is configured. The connection is established only if the frequency band is supported in your region.
Data Usage Tracking	Turn on the toggle switch to start tracking your data usage. If this field is enabled, the options to configure data usage limit and the Billing cycle are displayed.
Data usage alert limit	Enter the data limit in megabytes (Range – 1 to 65535 MB) to be used per month. Configure an alert in the **Alerts & Events** page for the alert to be generated when the data usage crosses the specified limit.

Parameter	Description
Monthly Billing start date	Select the day of the month on which the billing cycle begins.

Viewing the 9004-LTE Gateway Details

To view 9004-LTE Gateway device details, complete the following steps:

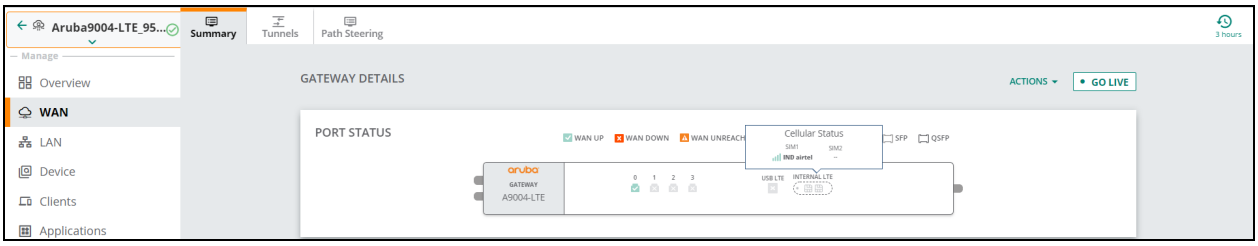
1. In the **Network Operations** app, use the filter to select a 9004-LTE Branch Gateway.
2. Under **Manage**, go to **Overview** > **Summary**. The **Gateway Details** page is displayed.

New fields that pertain to 9004-LTE Gateway have been introduced in the **WAN** and **Overview** tabs.

WAN Tab

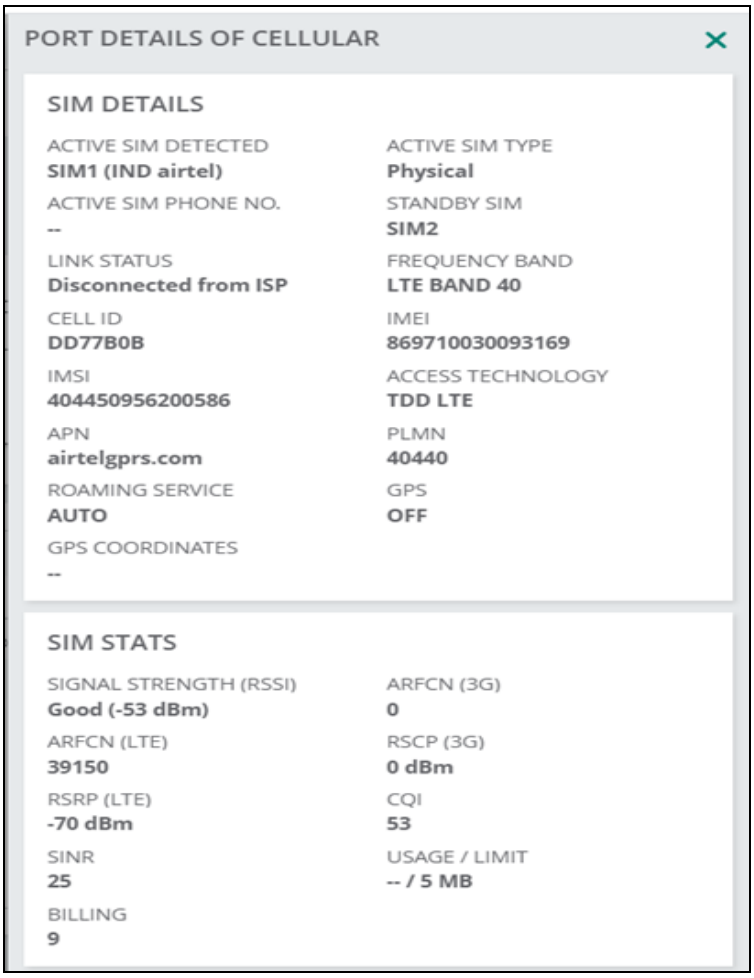
For a 9004-LTE Gateway, the faceplate displays the LTE uplink details. When you hover over **Internal LTE**, you can view details about the active SIM, the name of the service provider, and the signal strength as illustrated in the image:

Figure 186 *LTE Gateway Details*



You can click on the active SIM to view the port details of cellular:

Figure 187 *Cellular Port Details*



For more information, see Gateway > WAN > Summary.

Overview Tab

The following attributes are added exclusively for 9004-LTE Gateway model:

- **4G/LTE Modem Type**—Displays the LTE connection type as **Internal** if it is an internal modem. Displays the name of the vendor if it is an external modem.
- **4G/LTE Modem Status**—Displays the modem connectivity status. A green check-mark icon indicates that the modem is connected. A red circular icon indicates that the modem is disconnected. If the modem type is Internal, this field also displays the name of the service
- provider and the signal strength along with the modem status. Hover over the information icon to view details about the active SIM, the IMEI number, and the phone number. If the modem type is external, this field displays only the modem connection status.

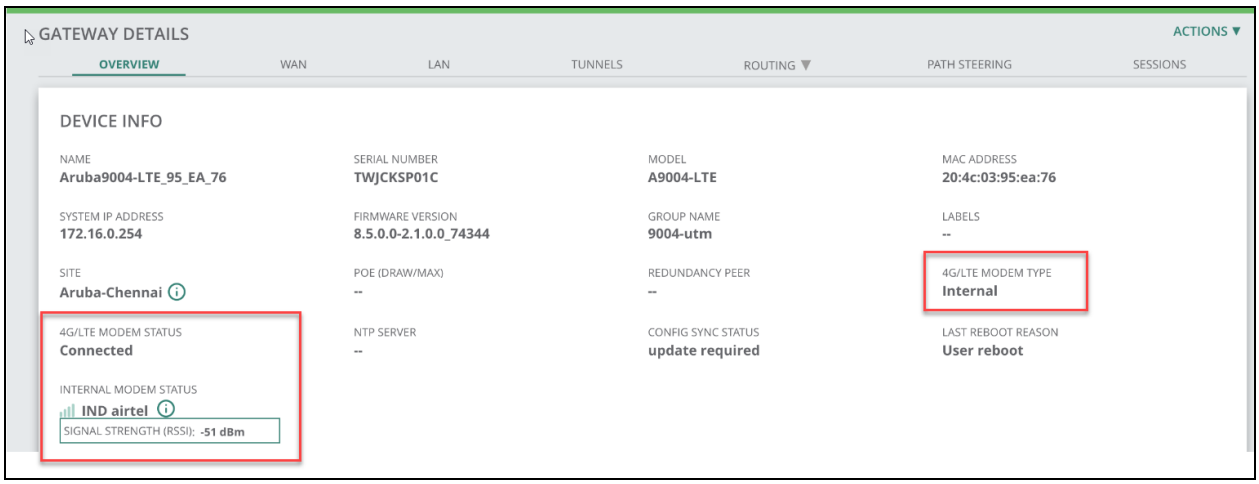
  You can view the signal strength classification based on the RSSI value provided in the following table:

Table 249: *Signal Strength Classification*

Signal Strength	Value	Representation
Good	> –65 dBm	All four bars are shaded green
Average	> –80 dBm	From the left, first 2 or 3 bars are shaded green
Poor	< –80 dBm	From the left, only one bar is shaded green

The following image displays the device information of a 9004-LTE Gateway:

Figure 188 *Device Info - 9004-LTE Gateway*



Configuring WAN Health Check

The WAN Health Check sends probes to measure WAN availability and latency on selected uplinks. Based on probe response, Gateways continue to use the primary uplink, or fail over to a backup link.

As health check monitoring is critical for forwarding the Internet traffic, ensure that the health check feature is enabled on all Branch Gateway groups. When the health check feature is enabled, the probes are sent through the underlay at regular intervals to verify if the Internet is reachable over the uplink interfaces configured on Gateways. Based on the probe response, the uplink interface is marked as unavailable for the underlay traffic.

When the health check is enabled on a Branch Gateway, it sends five UDP or ICMP probes to a host every 10 seconds. The tunnel health is determined based on the probes received at the host:

1. If a probe is lost, then five probes are sent every two seconds to the host.
2. If a probe is lost in the first two seconds, then the aggressive mode is enabled by default and 25 probes are sent every two seconds for the next 10 seconds.
3. If the probes do not reach the destination, then the tunnel is torn down hence achieving faster tunnel age-out with minimum packet loss.

When probes are not lost, The Branch Gateway goes back to send five probes every 10 seconds per uplink.

Enabling WAN Health Check Probes

To enable WAN health check and configure probe settings, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **WAN** > **Health Check**.
3. Select the **Health Check** check box and configure the parameters described in the following table:

Table 250: *WAN Health Check Settings—Advanced Mode*

Parameter	Description
Remote Host IP/FQDN	Remote host to which the Branch Gateways can send the health check probes. As part of the SD-WAN solution, Aruba Central provides a globally redundant path quality monitoring service for WAN health checks by default. Ensure that you use the **pqm.arubanetworks.com** FQDN as the probe responder, so that Aruba Central uses this host address to check the health of WAN uplinks configured on Branch Gateways. Branch Gateways with ArubaOS 8.4.0.0-1.0.6.0 or later software versions can probe up to four IP addresses that are obtained after resolving the health check FQDN. In the earlier releases, Branch Gateways could send probes to only one IP address obtained after resolving the health check FQDN. **NOTE:** The Branch Gateways running the ArubaOS 8.4.0.0-1.0.6.0 or later software versions can install host routes to any DNS servers that are learned or configured using the uplink interfaces. This enhancement ensures that the DNS queries are routed through the appropriate uplink interfaces irrespective of the default routes. However, Branch Gateways do not support installing host routes on the MPLS uplink.
Probe Mode	Probe modes to use for connectivity checks. The following probe modes are available: ▪ **Ping**—Sends ICMP probes to measure latency and packet loss. ▪ **UDP**—Sends UDP Probes through UDP port 4500 to measure latency, packet loss and jitter. Latency is calculated based on the Round-Trip Time (RTT) of ping responses.

Table 250: *WAN Health Check Settings—Advanced Mode*

Parameter	Description
Probe Interval (sec)	Probe interval for sending probes. The default probe interval is 10 seconds. The allowed range of values is 2–3600 seconds.
Packet Burst Per Probe	Number of probes to be sent during the probe interval. To change the default value of 5 probes, enter a new value within a range of 1–16.
Probe Retries	The number of times the Branch Gateway must attempt to resend a probe. You can set any value withing a range of 1-255. The default value is 3.
Jitter Measurement	For the **UDP** probe mode, you can enable this check box to measure jitters on the uplink interface.

4. Click **Save Settings**.

Monitoring WAN Health

If you have configured uplink interfaces and enabled health check, the dashboard on the **Overview** > **Gateways** page displays WAN availability, usage, and compression details.

Configuring WAN Interface Bandwidth Priorities

The SD-Branch devices support configuring WAN scheduler profiles to ensure that all traffic types are allowed a minimum bandwidth. The WAN scheduler profiles also allow you to define priorities per traffic class to ensure that critical and delay-sensitive applications such as voice and video are assigned a higher priority and more bandwidth. Each WAN interface can have a scheduler profile that supports four queues with different priority levels. When you use session ACLs to define traffic policies on the Branch Gateway, you can use the scheduler profile to automatically associate different priority levels assigned by these policies to a scheduler profile queue.

For information on creating a traffic policy that assigns 802.1p priority levels to a specific application or application type, see Creating a Firewall Policy for Network Services.

Creating a WAN Scheduler Profile

To enable WLAN interface bandwidth priorities using WAN Scheduler, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Go to **WAN** > **WAN Scheduler**.
4. Click **+** below the **WAN Scheduler Profiles** table to define a new scheduler profile.
   a. In the **Profile name** field, enter a profile name.
   b. In the **Priority** fields, enter one or more 802.1p priority levels (0–7) for each queue type. Each of the seven priority levels must be supported by one of the four queues.
   c. For each queue, click the **Scheduler Discipline** drop-down list and select one of the following discipline types:
      - **Strict priority**—The queue service is based exclusively on the priority of the queue, where the lower-priority queues are not serviced until the higher-priority queue is clear. With this option, the highest-level priority is guaranteed as much bandwidth as possible, but there can be phases where the second, third, and fourth priority queues may receive little or no bandwidth.
      - **Deficit Round Robin (DRR) Weight**: The queue is assigned a percentage of available bandwidth. If you selected the **DRR Weight** option, you must enter the percentage of bandwidth that should be made available to the traffic in the selected queue.

You can define both strict priority and DRR Weight discipline types for a single scheduler profile. If you configure both strict priority and DRR weighted queues, the strict priority queues should be specified in a sequential order, followed by the DRR weighted queues. For example, if you want to specify two strict priority queues and two DRR weighted queues, configure queues 0 and 1 with the strict priority type, and then configure queues 2 and 3 with a DRR priority type. Do not alternate between strict priority and DRR weighted queues.

Table 251 displays sample Class of Service values for each queue of a WAN scheduler profile.

Table 251: *Sample CoS Values for WAN Scheduler profile*

Queue	Priority	Scheduler Discipline
Queue 0	6 7	Strict Priority
Queue 1	4 5	Strict Priority
Queue 2	2 3	Strict Priority
Queue 3	0 1	Strict Priority

1. To assign the scheduler profile to a cellular or Gigabit Ethernet port interface, click **+** in the **Assignments** area and configure the following parameters:

- Select the **Port** option and from the **Ports** drop-down list, select an interface. In the **Transmit Rate** field, enter the maximum transmit rate in Mbps for the selected interface.
- Click the **Cellular** option. In the **Transmit Rate** field, enter the maximum transmit rate in Mbps for the selected interface. The allowed range of values is 1–500 Mbps.

2. Create a firewall session policy that assigns a priority level to an application or application group. For details, see Creating a Firewall Policy for Network Services.

SD-WAN Overlay Tunnel and Route Orchestration

To simplify branch deployments, the Aruba SD-Branch solution provides support to the SD-WAN Orchestrator service for automatically setting up IPsec tunnels between the Branch Gateways and VPNCs provisioned in an Aruba Central account.

The SD-WAN Orchestrator supports the following functions:

- Tunnel Orchestration—The SD-WAN Orchestrator automates tunnel configuration between the branch and hub sites. The service can be enabled globally or for individual groups in Aruba Central.
- Route Orchestration—The SD-WAN Orchestrator automates the route advertisement and redistribution process by routing information learnt from each connected branch in a dynamic way.
- Overlay Tunnel and Route Monitoring—The SD-WAN Orchestrator service also includes a dashboard that displays detailed information about the orchestrated tunnels and routes.

The tunnel and route orchestrations run on the Gateway Foundation license. If the gateway's license expires or if the gateway is unlicensed, the tunnel and route orchestrations continue to work without impacting the network.

For more information on SD-WAN Orchestrator, see the following topics:

- Configuring Overlay Network Using SD-WAN Orchestrator
- Advertising Overlay Routes
- Monitoring SD-WAN Overlay Tunnels and RoutesThe Aruba SD-WAN solution provides support to configure SD-WAN Overlay network manually and automatically. To view information about the tunnels and routes configured for individual Branch Gateway, go to the Tunnels and Routing tab in the gateway monitoring dashboard. For more information, see Gateway > WAN > Tunnels and Gateway > Overview > Routing.The monitoring features of SD-WAN Overlay run on the Gateway Foundation license that is auto-assigned to the gateway device. Aruba Central provides a separate dashboard to monitor the status of tunnels and routes. See the following sections for more information:Overlay Tunnel Orchestrator in Map ViewOverlay Tunnel Orchestrator in Grid ViewOverlay Route Orchestrator in Map ViewOverlay Route Orchestrator in Grid View

Configuring Overlay Network Using SD-WAN Orchestrator

The Aruba SD-Branch solution supports overlay networks based on the hub and spoke, hub mesh, and branch mesh models. Administrators can use the SD-WAN Orchestrator for automatic configuration of IPsec tunnels between Branch Gateways and VPNCs (VPNCs). The SD-WAN Orchestrator supports IPsec tunnel between Aruba Gateways provisioned in an Aruba Central account.

The SD-WAN Orchestrator can be enabled either globally or on individual device groups. When enabled, the SD-WAN Orchestrator automatically builds an overlay network based on the data center preference you configure for the device groups in Aruba Central.

Prerequisites

Before you begin, ensure that your deployment topology meets the following prerequisites:

- Aruba Gateways are onboarded to and are managed by Aruba Central.
- Aruba Gateways are provisioned as part of **Branch Gateway** and **VPNC** groups in Aruba Central.
- Access to Central FQDNs must be allowed for device communication when SD-WAN Orchestrator service is enabled for an Aruba Central account.
- Aruba Gateways are upgraded to ArubaOS 8.4.0.0-1.0.5.1 or later software version.
- The overlay IPsec tunnels are initiated by Branch Gateways and terminated on a VPNC or another Branch Gateway using NAT traversal, therefore ensure that UDP 4500 port is permitted.

Configuration Steps

The following configuration steps are required for tunnel and route orchestration on Aruba Gateways:

- Configure uplinks for tunnel orchestration.
- Set data center preference.
- Configure global settings.
- Enable group orchestration.
- Configure network segment.
- Associate an overlay network segment.
- Configure aggregate overlay routes.
- Redistribute overlay routes. For information on redistributing overlay routes, see Advertising Overlay Routes.

Additional Documents

Aruba SD-WAN Orchestrator

Configuring Uplinks for Tunnel Orchestration

For tunnel orchestration, uplink configuration is required on both Branch Gateways and VPNCs. The SD-WAN Orchestrator requires:

- An appropriate pair of uplinks to bring up IPsec tunnels between Branch Gateways and VPNCs
- An algorithm to determine the tunnels orchestrated between Branch Gateways and VPNCs.

For tunnel orchestration, the following configuration is required on the uplink interfaces:

- For **MPLS** uplinks:
  - Link Name—The link name configured on the MPLS uplink interface of a VPNC must match the link name of the MPLS uplink interface configured on Branch Gateways.
  - Private IP address—By default, the IP address of the VLAN interface is used as the private IP address for uplink interfaces on the VPNCs. The private IP address can be modified.
- For **INET** uplinks:
  - Link Name—Link name matching is not mandatory. However, the SD-WAN Orchestrator will try to find the INET link with the same name; for example, if the INET uplink is named **att_inet**, the SD-WAN Orchestrator tries to establish tunnels to **att_inet**. Even if there is no matching INET link, the SD-WAN Orchestrator can establish IPsec tunnels between Branch Gateways and VPNCs with first available INET uplink.

- Public IP address—You must configure a public IP address that corresponds to the firewall NAT translation of the private IP address for the uplink interfaces on VPNCs.
- Private IP address—By default, the IP address of the VLAN interface is used as the private IP address for INET uplink interfaces on the VPNCs. Private IP address for INET uplinks cannot be modified or overwritten.

For more information on how to configure uplinks on Gateways, see Configuring Uplinks.

Setting Data Center Preference

If there are multiple data centers in the network, you can set a preferred data center for the Branch Gateways for IPsec tunnel configuration and route preference.

To configure data center preference, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options
5. Click **VPN** > **SD-WAN Overlay**.
6. Select **Orchestrated** for the **Overlay mode** from drop down options and enable the Orchestrated mode.
7. Click **DC Preference**.
8. To add the hub details, click **+** and select the hub group and VPNC(s). If the hub site has multiple VPNCs, you can configure a primary and secondary VPNC for the Branch Gateways.
9. Click **Save Settings**.

Data Center preference also determines the cost of the corresponding routes. A different cost based on the order of configuration is assigned to the advertised routes. This means that Data Center 1 with a primary preference automatically gets a lower cost assigned than the secondary VPNC. This cost is applied to the subnets that are redistributed into overlay (and subsequently into Data Center) as well as the opposite direction (the Data Center subnets are being redistributed through the VPNC and are advertised to the branch).

Configuring Global Settings

To configure tunnels and routes using the SD-WAN Orchestrator, complete the following steps:

- Configure timers and best path computation.
- Configure Dynamic Backup Route Advertisement (DBRA).

Configuring Timers and Best Path Computation

To configure tunnels and routes using the SD-WAN Orchestrator, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Network Services** > **SD-WAN Overlay**.
3. Click the **Config** icon to display the **SDWAN Overlay** configuration dashboard.

4. Click **Global Settings** tab and configure the following timers:
   - **Graceful Restart timer**—Sets the timer for keeping the tunnel and route state on the device when it loses connectivity to cloud.
   - **Tunnel rekey timer**—Sets a timer for Branch Gateway and VPNCs to exchange keys for IPsec tunnel. For more information, see Cloud Survivability.

By default, the SD-WAN Orchestrator service is enabled. When you shut down the service, tunnel and routing service is disabled and the SD-WAN overlay network is impacted. Aruba recommends that you use this option in case of emergency or when guided by the Aruba SD-WAN support team.

5. Enable **Dynamic data center path computation** to allow the Overlay Route Orchestrator to use the best path computation using the route attributes, selecting the next hops for the data center routes accordingly with the transported route attributes.

By default, the Overlay Route Orchestrator uses the configured Data Center preference for the next hop selection while announcing data center routes to the branches.

Configuring Dynamic Backup Route Advertisement

Dynamic Backup Route Advertisement (DBRA) is used to control advertisement of routes to the backup data center, if required. This feature decides whether or not to advertise the routes; however, it does not have control over the number of routes or which routes need to be advertised from the segment. DBRA is enabled per segment. When DBRA is enabled, the Overlay Route Orchestrator (ORO) advertises the routes from the segment only to the primary VPNC for that segment. This restricts the secondary VPNC from advertising any DBRA-segment routes to the core router. ORO follows the priority rule and selectively advertises the DBRA segment routes to the secondary VPNC when the primary VPNC fails, and sequentially to the tertiary VPNC if the secondary VPNC also fails.

For example, if vpnc1-dc1 and vpnc1-dc2 hubs are subscribed to a segment named Orange, then the routes are not advertised to vpnc1-dc2 as long as a tunnel to vpnc1-dc1 hub exists.

To configure DBRA, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Network Services**.
3. Click the **Config** icon. The **Network Services** configuration page is displayed.
4. Click the **SDWAN Overlay** tab. Then, click the **Config** icon.

   The **SDWAN Overlay** configuration page is displayed.
5. Click **Global Settings**.
6. Click **Show Dynamic Backup Route Advertisement (DBRA)** and configure the following parameters:
   - **Preemption**—Select this check box to advertise routes back to the primary VPNC and withdraw from the secondary VPNC, if connectivity to the primary VPNC restores. Otherwise, lower preference VPNC continues to receive the routes until connectivity to theprimary preference VPNC is maintained. By default, this field is not selected.
   - **Hold time**—Enter the wait time for the Overlay Route Orchestrator (ORO) before reacting to a tunnel down or up event (that is, advertising or withdrawal of routes). The default value is 30 seconds.

- **Randomize time**—Enter the randomize-time which the ORO adds to the hold-time to further reduce the churn in network when tunnels go down or up. The default value is 30 seconds.

Enabling Group Orchestration

To enable SD-WAN Orchestrator for the groups deployed in your account, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Network Services**.
3. Click the **Config** icon. The **Network Services** configuration page is displayed.
4. Click the **SDWAN Overlay** tab. Then, click the **Config** icon.
   The **SDWAN Overlay** configuration page is displayed.
5. Click **Group Orchestration** tab.
6. Select the groups for which you want to enable this service.
7. Click **Enable**.

Configuring Network Segments

To add an overlay network segment in the global dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage,** click **Network Services**.
3. Click the **Config** icon to display the **SDWAN Overlay** configuration dashboard.
4. Click the **Network Segments** tab. The **Network Segments** configuration page is displayed.
5. To add a network segment, click **+** in the **Networks Segments** table.
6. Provide a name to the new network segment, and click **Save Settings**. The newly added segment appears in the **Network Segments** table.
7. Click **Save Settings**.

Associating an Overlay Network Segment

To configure an overlay network configuration, complete the following steps:

1. In the **Network Operations** app, do either of the following:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing Branch Gateways or VPNCs.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
   - To configure a Branch Gateway, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Gateways**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **VPN** > **Network Segments**. The **Network Segments** configuration page is displayed.
4. All the Network Segments created under Network Services dashboard are displayed in the device or group **Network Segments** tab.
5. Click the segment for which you want to associate VLANs.
6. Select the **VLANs** from the drop-down list.
7. Click **OK**.

Configuring Branch Aggregate Routes

To configure branch aggregate routes using the SD-WAN Orchestrator, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Network Services** > **SD-WAN Overlay**.
3. Click the **Config** icon to display the **SDWAN Overlay** configuration dashboard.
4. Navigate to **Route Aggregates** > **Branch Aggregate**.
5. Click **+** and configure the following parameters:
   a. From the **Select Segment** drop-down menu, select a segment.
   b. To enable dynamic backup routes, enable the check box for **Dynamic backup route advertisement**.
   c. In the **Branch Aggregate Routes** table, click **+** and enter the IP summary range allocated to branch offices and respective Netmask. The IP summary range will be advertised with corresponding hubs as next hops to all the branches. Aruba recommends that you define a summary IP range to reduce the routing table size of the Branch Gateways.

Aggregating Routes from VPNCs in the Data Center

To aggregate route prefixes for all VPNCs routes in a data center, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **VPN** > **SD-WAN Overlay**.
6. Select **Orchestrated** for the **Overlay mode**.
7. Click **DC Aggregate Routes**.
8. Enter a summary IP range for the prefixes in the data center. This summary will be advertised with corresponding hubs as the next hops to all the branches. Aruba recommends that you configure a summary IP range to reduce the routing table size of the Branch Gateways
9. If you want to allow branch to branch traffic through the VPNC hub, select the **Allow branch-to-branch** check box. Enabling this option will make the VPNC hub a transit site and allow branch-to-branch traffic.
10. Click **Save Changes**.

Cloud Survivability

Configured tunnels have a definite expiry time, the common default expiry time is 24 hours. During rekeying, if the cloud connection fails, the tunnel keys expire. The expiration of authentication keys causes the tunnels to go offline, resulting in network traffic disruption.

Cloud Survivability mitigates the loss of a tunnel or the IPSec traffic between Aruba devices. These devices have IPsec tunnels which are orchestrated by SD-WAN Tunnel Orchestration and have a finite key expiry time. If the cloud connection fails for any reason, the devices remain connected through either LAN or WAN connections. This feature is available from ArubaOS 8.5.0.0-2.1.0.0 onward.

Devices can also re-establish IPSec tunnels between them based on tunnel configurations which are received from SD-WAN Tunnel Orchestration using legacy IKE/IPSec tunnel establishment. When cloud connectivity failure is detected during the rekeying process, the tunnels seamlessly switch over to legacy IPSec tunnels.

Cloud Survivability is triggered when:

- Devices on both sides of the tunnel have no connectivity to the Overlay Tunnel Orchestration.
- Overlay Tunnel Orchestration pushes new keys to the Branch Gateway or VPNC, but the Branch Gateway or VPNC did not receive the new keys.
- Overlay Tunnel Orchestration does not push a new key to the Branch Gateway or VPNC.
- The Branch Gateway or VPNC is unable to bring up the tunnel using the Overlay Tunnel Orchestration keys received.

A maximum of 6000 tunnels per VPNC is supported. The number of supported tunnels also depends on the gateway model.

While monitoring the tunnels, when the tunnels move to a survivability mode the tunnel type is categorized as **Orch-Srv**. The tunnel status is displayed in the Tunnels monitoring page. For more information, see the Gateway > WAN > Tunnels.

For more information about orchestrated configuration of IPsec tunnels, see Configuring Overlay Network Using SD-WAN Orchestrator.

Advertising Overlay Routes

To simplify routing and allow SD-Branch deployments to build scalable and secure VPNs on demand, the Aruba SD-Branch solution supports the SD-WAN Orchestrator for centralized orchestration of tunnels and routes. The SD-WAN Orchestrator automates the route configuration process and distributes routing information learnt from each connected branch in a dynamic way as per the routing segmentation requirements.

Branch Gateways and VPNCs in an SD-WAN topology, use the Overlay Agent Protocol (OAP) to automatically build the SD-WAN overlay topology. The OAP allows advertising local routes to the SD-WAN Orchestrator in Aruba Central.

The route orchestration service learns the following attributes in the routes advertised by the peer devices:

- IP address of the device from which the routes were received.
- IP address of the LAN side router from which the routes originated.
- The WAN service over which the routes are distributed.
- The site from where the route originated.
- Number of preferred data centers.

- Source protocol from which the routes originate.
- Metric and cost assigned to the routes.

Configuring Route Maps

Route maps allow you to configure a filtering criteria by defining a set of rules or match statements with a permit or deny condition. A route map includes a series match statements to determine if a route matches the criteria defined in the statement and then apply the permit or deny rule accordingly. You can also configure an additional set of parameters to adjust the attributes and metrics for routes that match the criteria defined in the match statement.

Important Points to Note

The following list includes some of the important points to consider when configuring a route map:

- A route map includes name, sequence number, permit or deny rule, the match and set statements. The match statements determine the route or the traffic to which the rule must be applied, whereas the set statements allow you configure attributes or adjust metrics for the route that matches the criteria defined in the match statement.
- The route map rules are applied sequentially; that is, based on the sequence number defined for each entry.
- The route map can use a prefix list in the match statement to apply the allow or deny rule. For more information on prefix lists, see Configuring a Prefix List.

Creating a Route Map

To create a route map:

1. To configure a gateway group or gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Go to **Routing** > **Overlay Routing**.
4. To add a route map, click the **+** icon in the **Route Maps** table. The **Create New Route Map** panel

opens.

5. Configure the following parameters as per your network requirements:

Table 252: *Route Map Configuration Parameters*

Parameter	Description
Name	Enter a name for the route map.
Sequence Number	Enter a sequence number for the route map. Sequence numbers allow route maps to be executed in an order. If you are configuring multiple match clauses or statements, ensure that you define a sequence number to uniquely identify each match statement.
Action	Configure a **permit** or **deny** rule for the match condition.
Match	Configure the match condition for the routes that have a destination network. The match statements define a set of conditions for determining if the route redistribution must be allowed or denied. To add a match statement, click the **+** icon in the **Match** table. You can set match **Type** to any of the options listed here: ■ **IP address** ■ **Next-hop IP address** ■ **Community** ■ **Interface VLAN** ■ **OSPF route tag** If you have selected the **IP address** or **Next-hop IP** address for match type, you can assign a prefix list to a match statement. If you have selected **Community** for match type, use one of the following options to define the community string. ■ **as:nn**—The community string in the AS:NN format, where AS refers to the Autonomous System number and NN refers to the network number. The valid range of values is 0-65535. ■ **community-val**—The Community Value string allows you to specify a community value. The valid range of values is 1–4294967295. ■ **well-known community**—A well-known community. Allows you to configure one of the following options: ◦ **Internet**—Advertises subnets to all neighboring devices. ◦ **No-Export**—Does not advertise prefix to any neighboring device. ◦ **No-Advertise**—Does not advertise subnets to neighboring devices. ◦ **Local-AS**—Prevents sending packets outside the local autonomous system. ■ **community list**—Allows you to select a community list configured on the Gateway. If you have selected **Interface VLAN** for match type, enter the interface VLANS separated by comma. You can enter up to 10 Interface VLANs. The value you enter must be between 1 to 4095. To know how to configure VLANs, see Configuring VLANs on Aruba Gateways. If you have selected **OSPF route tag** for match type, a match tag condition is added. You need to enter the tag names separated by comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.
Set	Configure a set of rules or attributes to apply to the overlay route that matches the conditions defined in a match statement. To add a set attribute, click the **+** icon in the **Set** table and configure the following attributes as per your requirement: ■ **as-path-prepend**—Prepends AS numbers through which the packets have traversed. You can apply the AS path prepending criteria to determine the best path. ◦ **AS number**— Enter any valid AS number between 1–65535. ■ **last-as**—Prepends the last AS number to the AS path. The valid range of values is 1–10.

Parameter	Description
	■ **community**—Sets a community string as an attribute in the routes. Community strings add additional information to the prefixes advertised to neighboring devices. You can set one of the following types of community string: ◦ **as:nn**—The community string in the AS:NN format, where AS refers to the Autonomous System number and NN refers to the network number. The valid range of values is 0-65535. ◦ **community-val**—The community Value string. The valid range of values is 1–4294967295. ◦ **well-known community**—A well-known community. You can configure one of the following options: • **Internet**—Advertises subnets to all neighbors. • **No-Export**—Does not advertise prefix to any neighbor. • **No-Advertise**—Does not advertise subnets to neighbors. • **Local-AS**—Prevents sending packets outside the local autonomous system. ■ **Community list**—Allows you to select a community list configured on the Gateway. ■ **ip next-hop**—Sets a next-hop IPv4 address as an attribute in the routes. ■ **local-preference**—Sets a preference value to the routes for determining the best AS path. When the neighboring device receives multiple routes to the same destination network, the route with the highest local preference value takes precedence. The valid range of values for local preference is 0–4294967295. ■ **metric**—Sets a metric value for determining the preferred path into an Autonomous System. You can define a metric value between 0–4294967295. When a metric value in a route matches this value, the route is advertised. ■ **origin**—Sets the origin of the route. The following options are available: ◦ **incomplete** (EGP)—To specify that the route is originated from exterior routing protocol. ◦ **igp**—To specify that the route is originated from interior routing protocol. ■ **OSPF route tag**—Sets the OSPF route tag information. You can set a value between 0–4294967295. ■ **OSPf route-type**—Sets the external OSPF route type. Configure one of the following options: ◦ **External Type-1**—To redistribute routes as External type 1 which applies both external cost to the destination and the cost to reach the boundary router in an Autonomous System. ◦ **External Type-2**—To redistribute routes as External type 2 and apply only the external cost to the destination.

Configuring a Prefix List

A prefix list allows routing systems to determine which routes must be accepted when they peer with other networks. A prefix list includes IP prefixes with a match criteria that allows or denies route redistribution. Prefix lists contain one or more ordered entries which are processed sequentially.

Prefix lists can be used as a match criteria for applying route map rules on network subnets. For example, if you want to prevent a route for 10.0.0.0/24 from being redistributed, you can define a rule to match the prefix and add it as a match criterion in the Overlay redistribution route map. For more information, see Configuring Route Maps.

To create a prefix list:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Go to **Routing** > **Overlay Routing** page, click **Prefix List**.
4. Click the **+** icon in the **Prefix Rules** table.
5. Enter a name for the prefix rule.
6. Enter a sequence number.
7. Select the action to perform when the traffic matches the condition defined in the prefix rule.
8. Enter a network address to which you want to apply the prefix rule.
9. Enter the subnet mask of the network.
10. If you want to define a prefix length parameter and use it as a match criteria for applying rules, enter an appropriate value for the optional **LE** and **GE** operators. The allowed range of values is 1–32.

    If the **LE** parameter is configured, the prefix rules are applied only if the subnets are equal to or smaller than the value specified for LE. Similarly, if the **GE** parameter is configured, the prefix rules are applied only if the subnets are equal to or greater than the value specified for GE. If either **LE** or **GE** parameter is not configured, the prefix rule is applied only to those subnets that match the exact address or subnet mask configured in the rule.

Redistributing Overlay Routes

Redistribution rules allow you to enable advertising of routing information from the connected, static, OSPF, and BGP interfaces into overlay routing. Routing information from other sources is not automatically redistributed into overlay routing, but need to be configured for each source protocol locally on each Gateway.

From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch gateways can apply route filters to the connected routes, which are aggregated, when redistributing to the SD-WAN Overlay. The route map applied to redistribution is also applied to aggregated and non-aggregated routes.

To redistribute routes as overlay routes:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Go to **Routing** > **Overlay Routing**.
4. Click **Redistribution Routes**.
5. To add a redistribution rule, click **+** under the **Redistribution Rules** table.
6. From the **Source Protocol** drop-down list, select a source type. The following options are available:
   - **Static**—To redistribute IP static routes.
   - **IKE Overlay**—To redistribute branch routes advertised by the Branch Gateways after establishing an IPsec tunnel with the VPNC at the hub site.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site. If you have selected **Connected**, select the VLAN interfaces to which the Gateway is connected.
   - **OSPF**—To redistribute routes learnt from the OSPF neighbors. If you have selected **OSPF**, select the OSPF path type in the **Filter** column. The following options are available:
     - **Intra Area**—To redistribute routes to same area from which they originated.
     - **Inter Area**—To redistribute routes to another area in the OSPF domain.
     - **External Type–1**—To redistribute as routes as External type 1 which applies both external cost to the destination and the cost to reach the boundary router in an Autonomous System.
     - **External Type–2**—To redistribute routes as External type 2 and apply only the external cost to the destination.
   - **IAP-VPN Overlay**—Routes learnt from micro-branch deployments with Instant APs.
   - **BGP**—To redistribute routes using BGP.

From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch Gateways are capable of redistributing a route to null into SD-WAN Overlay (OAP).

1. Set a **Filter** for the selected protocol.
2. Associate an existing **Route Map** with the **Source Protocols** if required. The route map association is applicable only for available routes.
3. For connected routes, you can enable the **Auto Aggregate** option to summarize routes.

Configuring Administrative Distance

Administrative distance is one of the main criteria to determine a preferred route when there are multiple paths to the same destination. The route with the lower administrative distance takes precedence for route redistribution.

To configure administrative distance:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. On the **Routing** > **Overlay Routing** page, click **Advanced**.
4. Define a route preference value for the following parameters:
   - **SDWAN overlay distance**—Enter a value within the range of 1–255. Default value is 90.
   - **IKE overlay distance**—Enter a value within the range of 1–255. Default value is 70.
   - **IAP-VPN overlay distance**—Enter a value within the range of 1–255. Default value is 60.

Viewing Overlay Routes in the Route Table

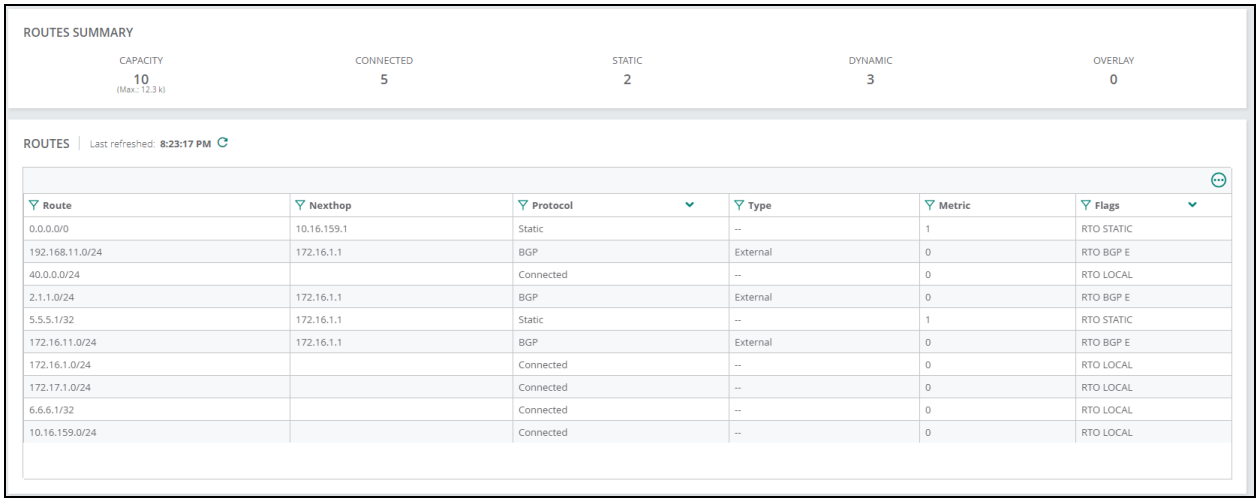
To view a Gateway group or Gateway route table complete either one of these steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one Branch Gateway.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the List view.
3. Click a gateway under **Device Name**.
   The dashboard context for the specific gateway is displayed.

4. Under **Manage**, click **Overview** > **Routing** > **Route Table**.

   A complete list of routes advertised by the Gateway is displayed.

5. From the **Protocol** drop-down list, select **Overlay** to view the Overlay routes.



Troubleshooting Overlay Configuration Issues

1. To troubleshoot Overlay configuration issues in a gateway group or a gateway device, complete either one of these steps:
   - To troubleshoot a Gateway group:
     a. In the **Network Operations** app, set the filter to a **Group** containing at least one Branch Gateway.

        The dashboard context for a group is displayed.
   - To troubleshoot a gateway:
     a. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

        The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.
4. Under **Analyze**, click **Tools**. The **Tools** page for troubleshooting devices opens.
5. Ensure the **Device Type** is set to Gateway and the Gateway device you want to troubleshoot is listed under **Available Devices**.
6. From **Categories**, select **Network**.
7. Select the commands that you want to use from the **Commands** list and add to the **Selected Commands**.
8. Click **Run**.
9. Verify the command output and resolve configuration errors if any.
10. Go to monitoring dashboard, verify the configuration status, and monitor the routes.
11. If the issue persists, contact Aruba Technical Support.

Monitoring SD-WAN Overlay Tunnels and Routes

The Aruba SD-WAN solution provides support to configure SD-WAN Overlay network manually and automatically. To view information about the tunnels and routes configured for individual Branch Gateway, go to the **Tunnels** and **Routing** tab in the gateway monitoring dashboard. For more information, see Gateway > WAN > Tunnels and Gateway > Overview > Routing.

The monitoring features of **SD-WAN Overlay** run on the Gateway Foundation license that is auto-assigned to the gateway device.

Aruba Central provides a separate dashboard to monitor the status of tunnels and routes.

See the following sections for more information:

- Overlay Tunnel Orchestrator in Map View
- Overlay Tunnel Orchestrator in Grid View
- Overlay Route Orchestrator in Map View
- Overlay Route Orchestrator in Grid View

Overlay Tunnel Orchestrator in Map View

The **Map** view is a pictorial representation of the geographical locations of SD-Branch deployment sites. The topology consists of the hub and spoke, hub mesh network between VPNCs, and the branch mesh network between the gateways. For information about how to create hub mesh and branch mesh topologies, see Configuring the SD-WAN Hub Mesh Topology.

- **VPNC groups**—When a VPNC group is selected, the map view displays its data centers and the number of VPNCs in each data center. If the selected group has a hub mesh topology, the tunnel network between data centers is also displayed.
- **Branch groups**—When a Branch group is selected, the default map view displays its Branch Gateways and data centers. A site or host name must be specified to view the tunnel network between branches.

The following topics are discussed in this section:

- Navigating to the Map View
- Overlay Tunnel Orchestrator Topology

Navigating to the Map View

To view the orchestration topology details in map view:

1. In the **Network Operations** app, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Network Services > SD-WAN Overlay**.
   The **SD-WAN Overlay** page is displayed in the **List** view. This is the default view. The page consists of two tabs:
   - **Tunnel**—Consists of the **Overlay Tunnel Orchestrator Topology** pane with the **Map** and **Grid** tabs.
   - **Route**—Consists of the **Overlay Route Orchestrator Topology** pane with the **Map** and **Grid** tabs.

3. Click **Map**.

   The orchestration details are displayed in a diagrammatic representation on map. The following tabs are present:

   - **VPNC groups**—Consists of VPNC groups details.
   - **Branch groups**—Consists of Branch groups details.

     The contextual summary table appears only when a VPNC group or a Branch group is selected.

Overlay Tunnel Orchestrator Topology

You can view the **Overlay Tunnel Orchestrator Topology** details as follows:

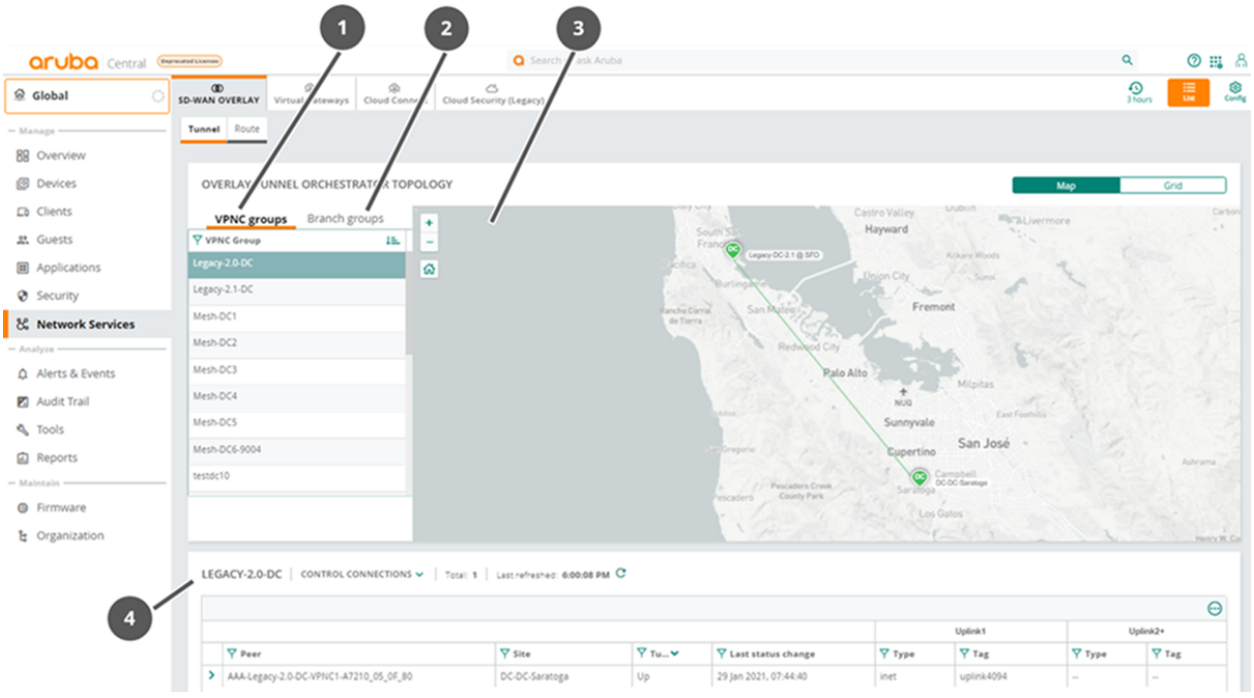
- Map View—A pictorial representation of the geographical location of SD-Branch deployment sites.
- Grid View—The topology information for each branch group in a tabular format.

Map View

The **Map** view consists of the following sections:

- VPNC Groups Filter
- Branch Groups Filter
- Map View
- Contextual Summary Table

Figure 189 *Overlay Tunnel Orchestrator in Map View*



The following table explains the interface elements of the map view.

Table 253: *User Interface Elements*

Number	UI Element	Description
1	**VPNC** Groups Filter	Displays the list of VPNC groups present in the network. VPNC

Number	UI Element	Description
		groups are configured in a hub mesh topology.
2	**Branch Groups Filter**	Displays the list of branch groups present in the network. Branch groups are configured in a branch mesh topology.
3	**Map View**	Displays data centers as pins and mesh links as bars (lines). Selecting a group depicts the location of the deployment site and details of the data center preference configured for the branch devices. The map also indicates if the VPNCis set as the primary VPNC for the Branch Gateways in the group. Search Options: ■ The  icon allows you to search a particular branch group. ■ The  and  icons allow you to sort the branch group names in ascending or descending order.
4	**Contextual Summary Table**	Displays information corresponding to the selected item (branch group or data center or tunnel). For example, if you have selected a VPNC group, the map displays the geographical location of the data centers and the summary table displays the **Peer**, **Site**, **Type**, **Tunnel State**, **Uptime**, **Last Status Change**, **Tunnels orchestrated**, and **Last Reset Reason** information. Every uplink in the orchestration displays **Type**, **Tag**, **Public IP**, and **Private IP** columns.

By default, the map view displays all the data centers of the SD-WAN overlay connected via a mesh link. Select a VPNC group or Branch group to view details specific to it.

VPNC Group—Map View Elements

The following features aid in reading the Overlay Tunnel Orchestration Topology in map view for a VPNC group.

Figure 190 *Viewing Options for VPNC Group*

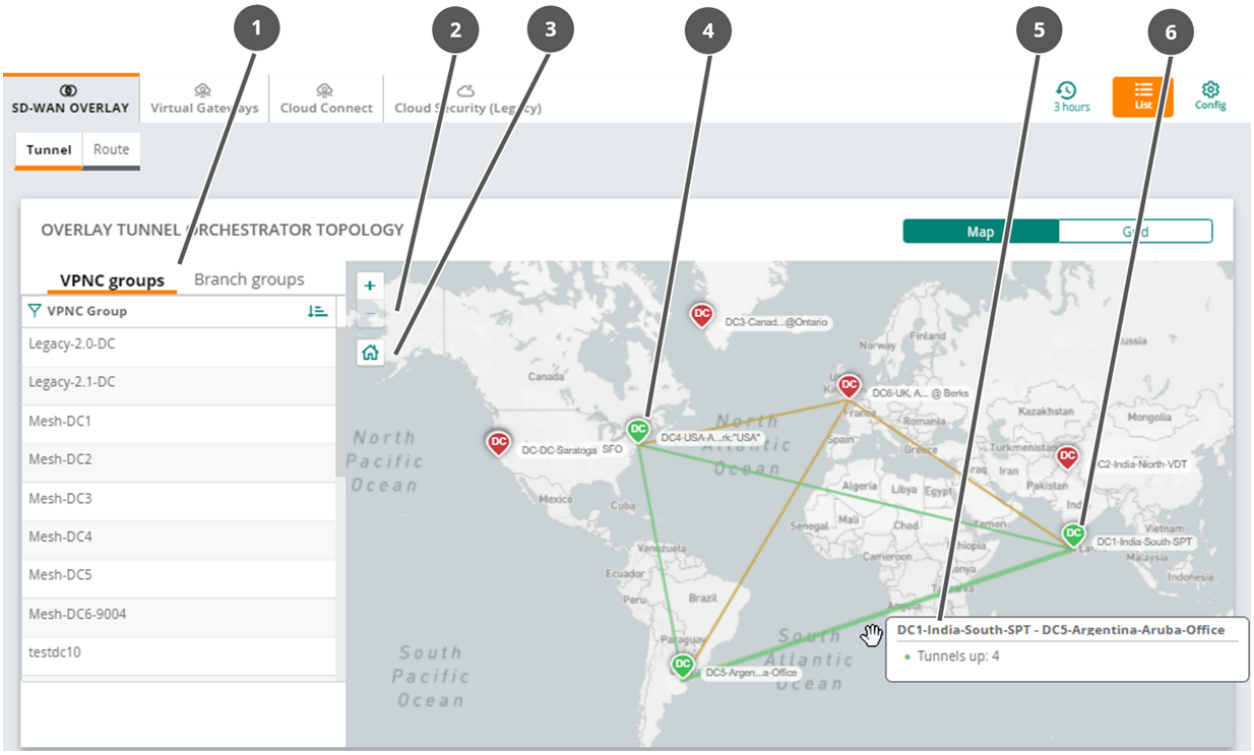


Figure 191 *Viewing Options for Branch Group*

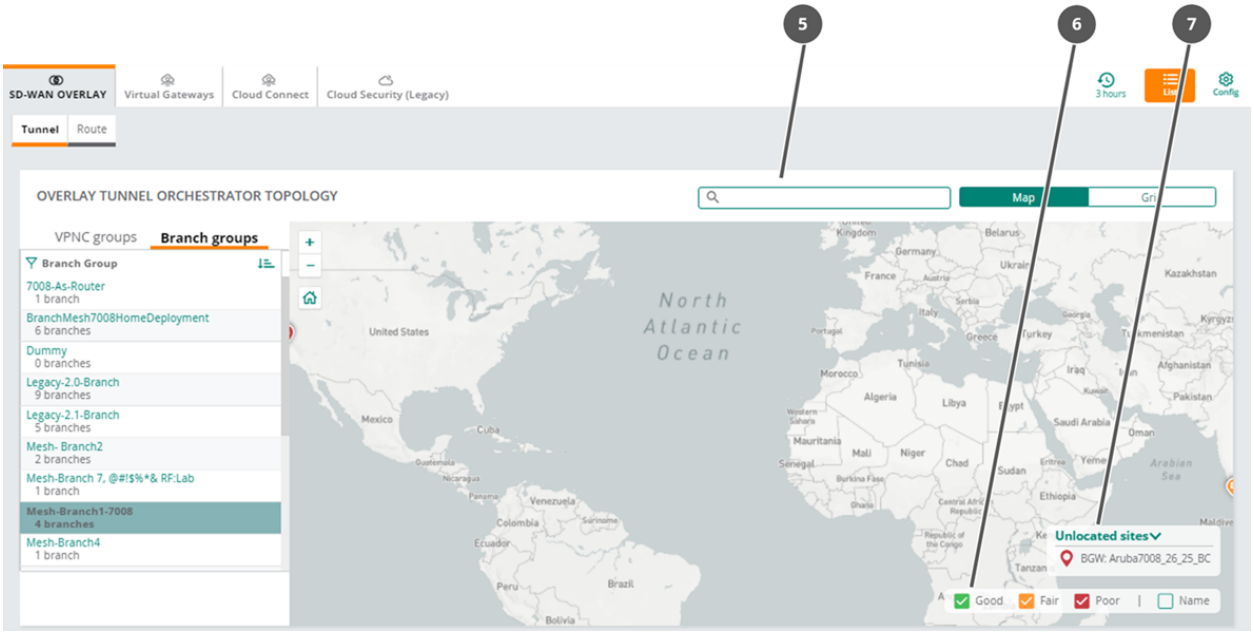
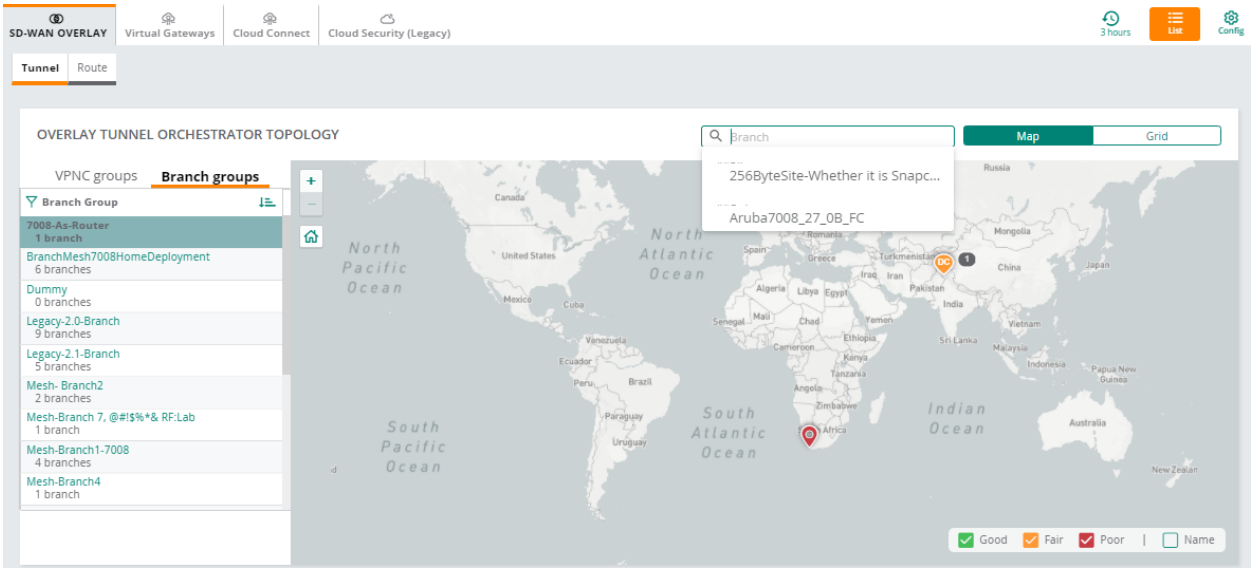


Figure 192 *Branch Group Mesh Topology of the Site*



The following table explains how to read the elements in the map view.

Table 254: *VPNC Group and Branch Group Map View Elements*

Number	UI Element	Description
1	**Branch Group Filter**	To view the branch group topology in the map, select a branch group from the **Branch Group** filter. The data centers (—pin) appear on the map. If the branch group is configured with hub-mesh topology, you can see mesh links (—bar) between the data centers.
2	**Zoom Buttons**	▪ Click **+** to zoom in. ▪ Click **-** to zoom out.
3	**Home Icon**	Click the Home icon to reset the map view.
4	**Data Center Pin**	Hover over the data center to view the data center name and its VPNCs.

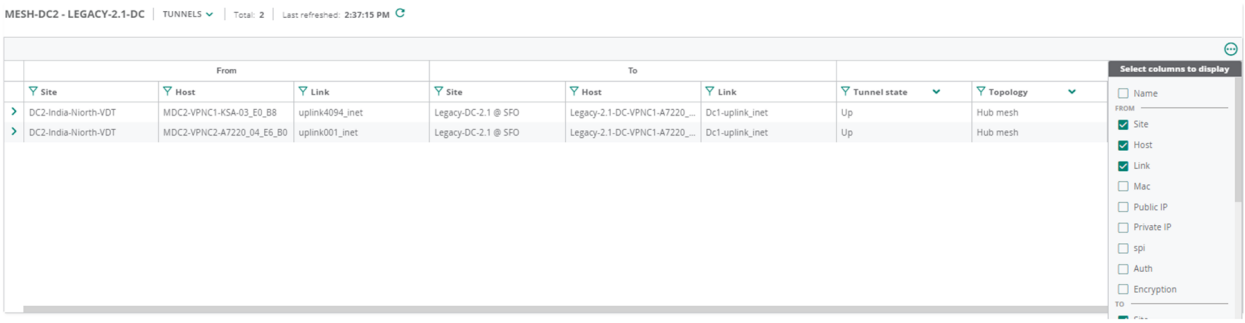
Number	UI Element	Description
5	**Tunnel lines**	When you select a branch group with mesh topology, there are tunnels formed between the data centers and branches. The tunnels are indicated by lines between the gateways.
	Tunnel Details	Hover over the tunnel link  to view the number of active tunnels between the data centers. **NOTE:** Ensure to click the mesh link (bar) only when you see the hand pointer icon.
	Source and Destination Details	To view the source and destination site details of a tunnel, click the tunnel link. A pop-up window appears displaying the list of tunnels between the data centers and its corresponding information. The columns present in the pop-up window are: ■ **Name**—Name of the tunnel. ■ **From and To**—The **From** and **To** site, hosts and links that connect the tunnel. ■ **Tunnel State**—Current status of the tunnel. ■ **Next Rekey**—Time stamp for the next rekey. **NOTE:** ■ Expand the drop-down to view details about the devices in the source and the destination such as the link type, their MAC and IP addresses and so on. ■ Click the **Ellipses** icon  to display more columns in the table. See the *Tunnel Details Pop-Up* topic for more information.
6	**Tunnel/Data Center Status**	The status of the tunnel and data center is indicated by colors. ■ **Green**—Indicates active tunnels or data centers. ■ **Red**—Indicates inactive tunnels or data centers. ■ **Yellow**— Indicates one or more tunnels that are down.
7	**Search Box**	Use this option to view the tunnel links between the branch groups based on the selected site or host. To view the mesh representation for a site or host, select the branch group and specify the site name or host name in the search box. The available sites and hosts for the selected branch group appear in the auto-suggest box. The mesh links appear for the selected site or host. Zoom in on the map view to view all the mesh topologies for the selected site or host.
8	**Unallocated Sites**	Displays the Branch Gateways that are not assigned to a site. ■ Click the number to view the device details. ■ Click the down arrow to expand the pane. **NOTE:** The **Unallocated Sites** drop-down appears only for Branch Groups, which has SD-WAN Branch Gateways that are not associated with any sites.

Number	UI Element	Description
9	**Status Filter**	Select or clear the options to view the pins on the map. ■ **Good**—Select this option to view the Branch Gateways that are active. ■ **Fair**—Select this option to view the Branch Gateways that are partially active. ■ **Poor**—Select this option to view the Branch Gateways that are not active. ■ **Name**—Select this option to display the Branch Gateways name over the pin on the map.

Tunnel Details Pop-Up

In the map view for the **Overlay Tunnel Orchestrator Topology**, click the tunnel link to display the tunnel details pop-up window.

Figure 193 *Pop-up—Tunnel Details*



Contextual Summary Table

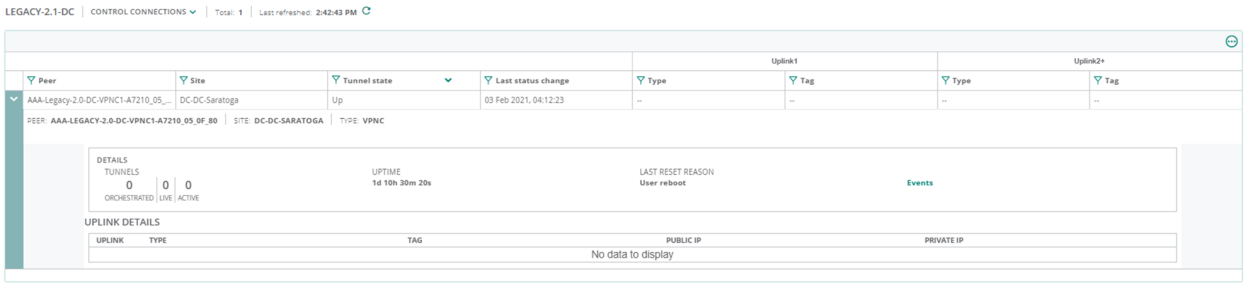
To view tunnel information for each group and the devices in a group, select the VPNC group or branch group in the **Map** or **Grid** view. The tunnel details for gateways deployed in selected group is displayed. The details displayed in the summary table are contextual to the selected item in the **Map** or **Grid**. If you select the group, the values in the columns correspond to the group. Similarly, if you select the data center or tunnel, the respective values are displayed.

By default, the **Control Connections** option is selected and the following details are displayed for each Branch Gateway in VPNC group or branch group:

- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **Peer**—The list of peer devices with which the tunnel is established.
- **Site**—The physical location of the hub site with which the tunnel is established.
- **Type**—The type of the site. Indicates if the tunnel request is triggered from the hub or branch site.
- **Tunnel State**—The current status of the tunnel.
- **Uptime**—The uptime of the tunnel.
- **Last Status Change**—The time stamp of the last status change.
- **Tunnels orchestrated**—Displays the number of tunnels orchestrated, number of live tunnels and the number of active tunnels.

- **Last Reset Reason**—The reason that triggered the last reboot.
- **Uplink**—Displays the uplink number.
  - **Tag**—VLAN tag associated with the tunnel.
  - **Type**—Uplink type associated with the tunnel.
  - **Private IP**—Private IP address associated with the tunnel.
  - **Public IP**—Public IP address associated with the tunnel.

Figure 194 *Overlay Tunnel Orchestrator—Tunnel Details*

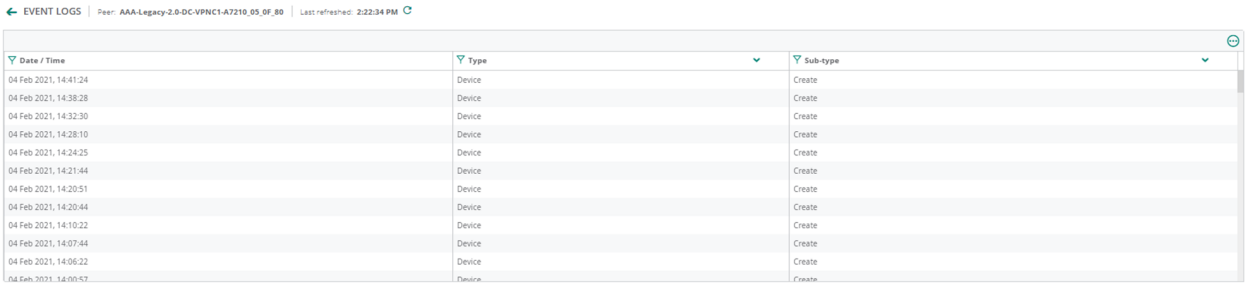


Expand the device to view the peer device details and the link to **Events** log:

Events—The link to the table that lists the events recorded. Click **Events** to open the **Event Logs** table.

- **Date/Time**—The timestamp of the event.
- **Severity**—Specifies whether the event is **Invalid**, or a **Warning**, or an **Alert** or a **Notice** based on the severity of the event.
- **Type**—Specifies the type of event.
  - **Invalid**—An invalid event.
  - **Config**—A configuration event.
  - **Tunnel**—Tunnel related events.
  - **Device**—A device related event such as a gateway going down.
- **Sub Type**—Specifies the sub type of the event.
  - **Invalid**—Invalid event type.
  - **Create**—New tunnel configuration is created.
  - **Noop**—No operation (noop) performed.
  - **KeyCollision**—Recalculated key of the tunnel, because computed Security Parameter Index (SPI) exists in the device.
  - **Rekey**—Tunnel is rekeyed.
  - **ConfigUpdate**—Tunnel configuration is updated.
  - **Restart**—Tunnel is restarted from the Bringup or Down state after the retry attempts.
  - **Delete**—Tunnel configuration is deleted.
  - **Up**—Device is operationally UP.
  - **Down**—Device is operationally Down.
  - **Bringup**—Tunnel key is sent to bring up the device if it is not yet Up or Down.
  - **Resync**—Device tries to resync.
- **Description**—A brief description of the event.

Figure 195 *Overlay Tunnel Orchestrator Event logs*

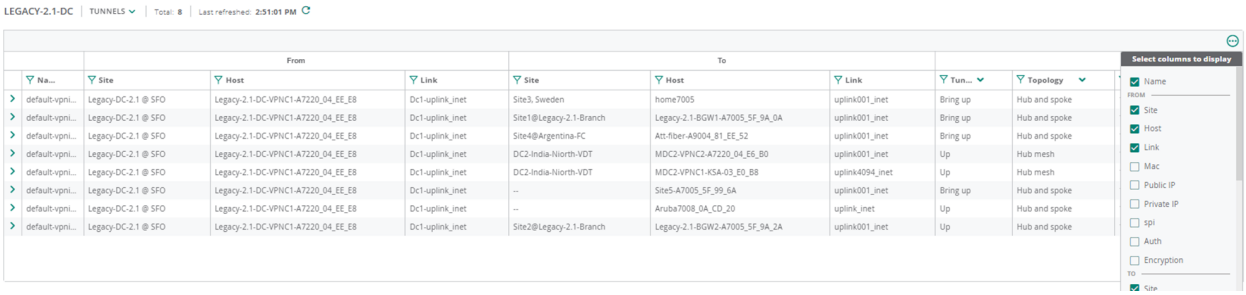


In the contextual summary table, select **Tunnels** from the drop-down. The list of tunnels is displayed with the following details:

Click the **Ellipses** icon to display more columns in the table.

- **Name**—Name of the tunnel.
- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **From and To**—The following columns are available:
  - **Site**—The source or destination site name.
  - **Host**—Source or destination host name.
  - **Link**—Source or destination uplink used by the tunnel.
  - **MAC**—Source or destination MAC address.
  - **Public IP**—Source or destination public IP address.
  - **Private IP**—Source or destination private IP address.
  - **SPI**—Source or destination Serial Peripheral Interface (SPI).
  - **Auth**—Source or destination authentication information.
  - **Encryption**—Source or destination encryption information.
- **Tunnel State**—Current status of the tunnel, which could be **Up**, **Down**, **Bring up**, **Inactive**, or **Unknown**.
- **Topology**—Type of topology, which could be **Hub and spoke**, **Hub mesh**, **Branch mesh**, or **unknown**.
- **Next Rekey**—Time stamp for the next rekey.

Figure 196 *Overlay Tunnel Orchestrator—Tunnels*



Overlay Tunnel Orchestrator in Grid View

The **Grid** view provides the topology information for each VPNC group and Branch group in a tabular format. The topology consists of the hub and spoke, hub mesh network between VPNCs, and the branch

mesh network between the gateways. For information about how to create hub mesh and branch mesh topologies, see Configuring the SD-WAN Hub Mesh Topology and Branch Mesh Topology in SD-Branch .

- **VPNC groups**—When VPNC group tab is selected, the table displays the data center name and the mesh topology to which it belongs.
- **Branch groups**—When Branch group tab is selected, the table and contextual summary table panes are displayed. The Branch group table displays the Branch Group, DC Preference, Site, Preferred VPNC, Latitude, and Longitude details. The contextual summary table displays details for the selected branch group.

The following topics are discussed in this section:

- Navigating to the Grid View
- Overlay Tunnel Orchestrator Topology

Navigating to the Grid View

To view the orchestration topology details in a grid:

1. In the **Network Operations** app, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Network Services > SD-WAN Overlay**.
   The **SD-WAN Overlay** page is displayed in the **List** view. This is the default view. The page consists of two tabs:
   - **Tunnel**—Consists of the **Overlay Tunnel Orchestrator Topology** pane with the **Map** and **Grid** tabs.
   - **Route**—Consists of the **Overlay Route Orchestrator Topology** pane with the **Map** and **Grid** tabs.
3. Click **Grid**.
   The orchestration details are displayed in a tabular format. The following tabs are present:
   - **VPNC groups**—Consists of VPNC groups table.
   - **Branch groups**—Consists of Branch groups table.
     The contextual summary table appears only when a VPNC group or a Branch group is selected.

Overlay Tunnel Orchestrator Topology

You can view the **Overlay Tunnel Orchestrator Topology** details as follows:

- Map View—A pictorial representation of the geographical location of SD-Branch deployment sites.
- Grid View—The topology information for each branch group in a tabular format.

Grid View

The **Grid** view displays the following tabs:

- VPNC Groups
- Branch Groups
- Contextual Summary Table

VPNC Groups

The **VPNC Groups** tab consists of the data center name and the mesh topology to which it belongs. The contextual summary table appears when you select a group.

The **VPNC Groups** table details are as follows:

- **Name**—The data center name.
- **Hub Mesh**—The mesh topology to which the data center is associated.

Branch Groups

The **Branch Groups** tab consists of the Branch groups table. The contextual summary table appears when you select a group.

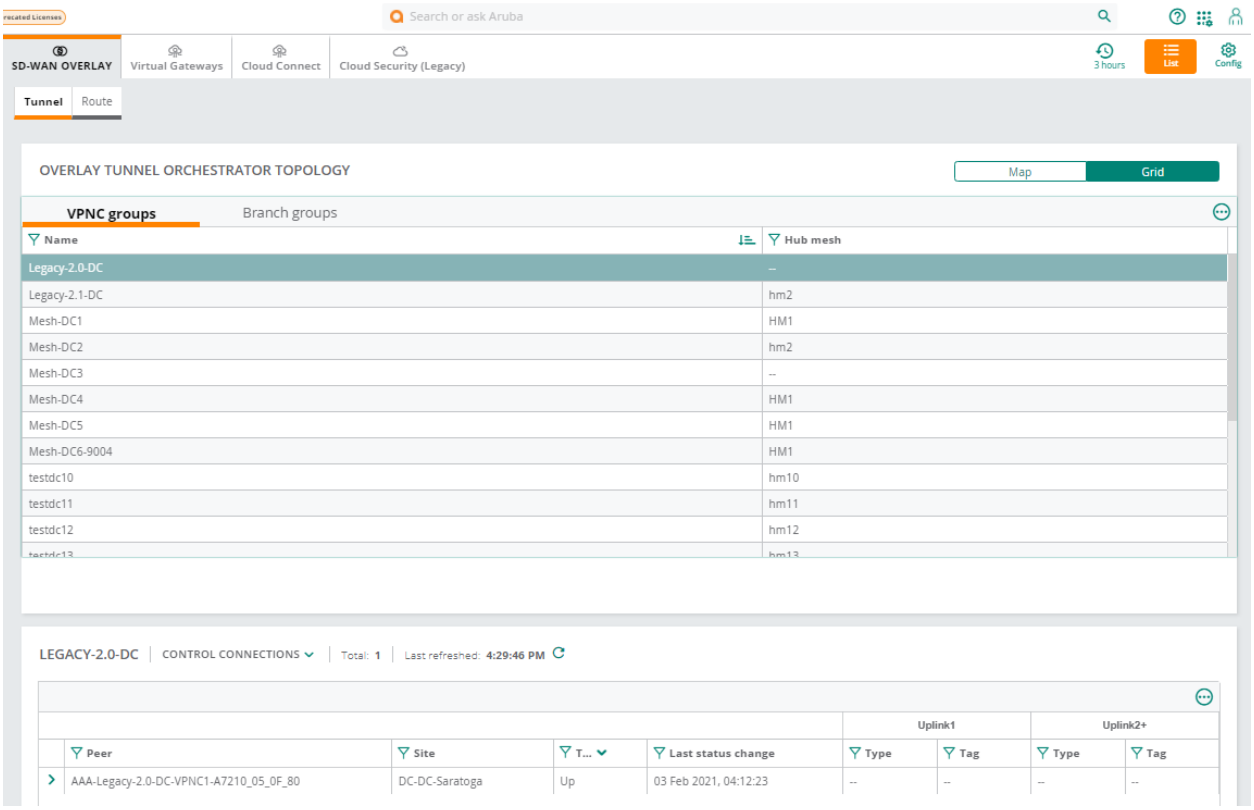
The **Branch Groups** table details are as follows:

NOTE

The search box is available only for the **Branch groups** in **Map** and **Grid** views. Use this option to view information about the required tunnel links between the branch groups based on the selected site.

- **Branch Group**—The name of the device group in which the Aruba Gateways are provisioned.
- **DC Preference**—The data center preference order configured for the branch devices.
- **Site**—The physical location of the SD-Branch site.
- **Preferred VPNC**—The preferred hub sites.
- **Latitude**—The latitude of the SD-Branch topology.
- **Longitude**—The longitude of the SD-Branch topology.

Figure 197 *Overlay Tunnel Orchestrator in Grid View*



Contextual Summary Table

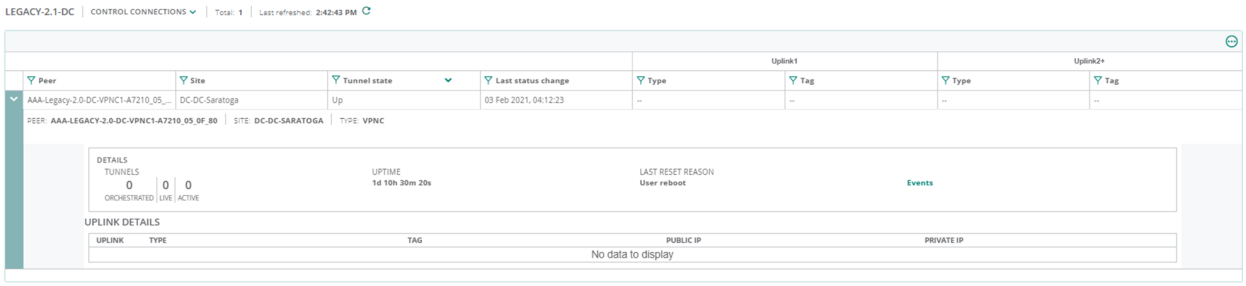
To view tunnel information for each group and the devices in a group, select the VPNC group or branch group in the **Map** or **Grid** view. The tunnel details for gateways deployed in selected group is displayed. The details displayed in the summary table are contextual to the selected item in the **Map** or **Grid**. If you select

the group, the values in the columns correspond to the group. Similarly, if you select the data center or tunnel, the respective values are displayed.

By default, the **Control Connections** option is selected and the following details are displayed for each Branch Gateway in VPNC group or branch group:

- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **Peer**—The list of peer devices with which the tunnel is established.
- **Site**—The physical location of the hub site with which the tunnel is established.
- **Type**—The type of the site. Indicates if the tunnel request is triggered from the hub or branch site.
- **Tunnel State**—The current status of the tunnel.
- **Uptime**—The uptime of the tunnel.
- **Last Status Change**—The time stamp of the last status change.
- **Tunnels orchestrated**—Displays the number of tunnels orchestrated, number of live tunnels and the number of active tunnels.
- **Last Reset Reason**—The reason that triggered the last reboot.
- **Uplink**—Displays the uplink number.
  - **Tag**—VLAN tag associated with the tunnel.
  - **Type**—Uplink type associated with the tunnel.
  - **Private IP**—Private IP address associated with the tunnel.
  - **Public IP**—Public IP address associated with the tunnel.

Figure 198 *Overlay Tunnel Orchestrator—Tunnel Details*



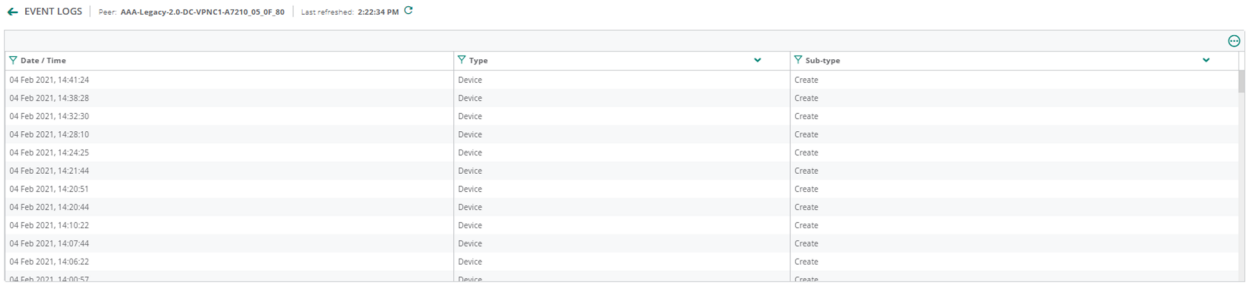
Expand the device to view the peer device details and the link to **Events** log:

Events—The link to the table that lists the events recorded. Click **Events** to open the **Event Logs** table.

- **Date/Time**—The timestamp of the event.
- **Severity**—Specifies whether the event is **Invalid**, or a **Warning**, or an **Alert** or a **Notice** based on the severity of the event.
- **Type**—Specifies the type of event.
  - **Invalid**—An invalid event.
  - **Config**—A configuration event.
  - **Tunnel**—Tunnel related events.
  - **Device**—A device related event such as a gateway going down.

- **Sub Type**—Specifies the sub type of the event.
  - **Invalid**—Invalid event type.
  - **Create**—New tunnel configuration is created.
  - **Noop**—No operation (noop) performed.
  - **KeyCollision**—Recalculated key of the tunnel, because computed Security Parameter Index (SPI) exists in the device.
  - **Rekey**—Tunnel is rekeyed.
  - **ConfigUpdate**—Tunnel configuration is updated.
  - **Restart**—Tunnel is restarted from the Bringup or Down state after the retry attempts.
  - **Delete**—Tunnel configuration is deleted.
  - **Up**—Device is operationally UP.
  - **Down**—Device is operationally Down.
  - **Bringup**—Tunnel key is sent to bring up the device if it is not yet Up or Down.
  - **Resync**—Device tries to resync.
- **Description**—A brief description of the event.

Figure 199 *Overlay Tunnel Orchestrator Event logs*



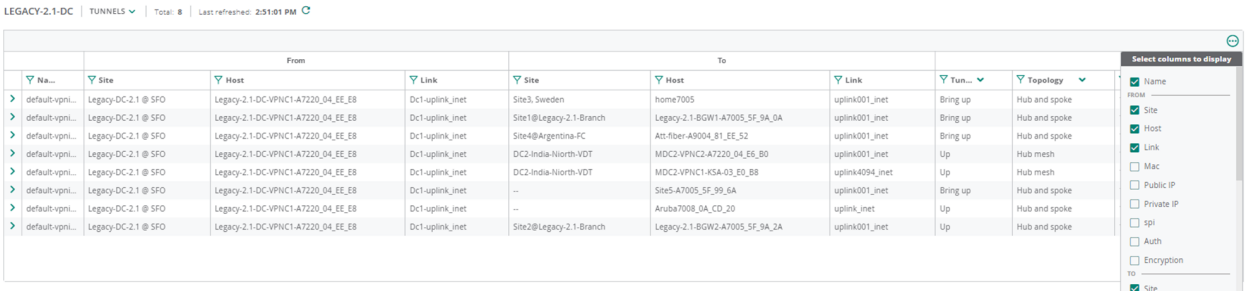
In the contextual summary table, select **Tunnels** from the drop-down. The list of tunnels is displayed with the following details:

Click the **Ellipses** icon to display more columns in the table.

- **Name**—Name of the tunnel.
- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **From and To**—The following columns are available:
  - **Site**—The source or destination site name.
  - **Host**—Source or destination host name.
  - **Link**—Source or destination uplink used by the tunnel.
  - **MAC**—Source or destination MAC address.
  - **Public IP**—Source or destination public IP address.
  - **Private IP**—Source or destination private IP address.
  - **SPI**—Source or destination Serial Peripheral Interface (SPI).
  - **Auth**—Source or destination authentication information.
  - **Encryption**—Source or destination encryption information.

- **Tunnel State**—Current status of the tunnel, which could be **Up**, **Down**, **Bring up**, **Inactive**, or **Unknown**.
- **Topology**—Type of topology, which could be **Hub and spoke**, **Hub mesh**, **Branch mesh**, or **unknown**.
- **Next Rekey**—Time stamp for the next rekey.

Figure 200 *Overlay Tunnel Orchestrator—Tunnels*



Overlay Route Orchestrator in Map View

The **Map** view is a pictorial representation of the geographical locations of SD-Branch deployment sites. The topology consists of the hub and spoke, hub mesh network between VPNCs, and the branch mesh network between the gateways. For information about how to create hub mesh and branch mesh topologies, see Configuring the SD-WAN Hub Mesh Topology.

- **VPNC groups**—When a VPNC group is selected, the map view displays its data centers and the number of VPNCs in each data center. If the selected group has a hub mesh topology, the tunnel network between data centers is also displayed.
- **Branch groups**—When a Branch group is selected, the default map view displays its Branch Gateways and data centers. A site or host name must be specified to view the tunnel network between branches.

The following topics are discussed in this section:

Navigating to the Map View

To view the orchestration topology details in map view:

1. In the **Network Operations** app, set the filter to **Global**.

   The global dashboard is displayed.
2. Under **Manage**, click **Network Services > SD-WAN Overlay**.

   The **SD-WAN Overlay** page is displayed in the **List** view. This is the default view. The page consists of two tabs:
   - **Tunnel**—Consists of the **Overlay Tunnel Orchestrator Topology** pane with the **Map** and **Grid** tabs.
   - **Route**—Consists of the **Overlay Route Orchestrator Topology** pane with the **Map** and **Grid** tabs.
3. Click **Map**.

   The orchestration details are displayed in a diagrammatic representation on map. The following tabs are present:

- **VPNC groups**—Consists of VPNC groups details.
- **Branch groups**—Consists of Branch groups details.

  The contextual summary table appears only when a VPNC group or a Branch group is selected.

Overlay Route Orchestrator Topology

You can view the **Overlay Route Orchestrator Topology** details as follows:

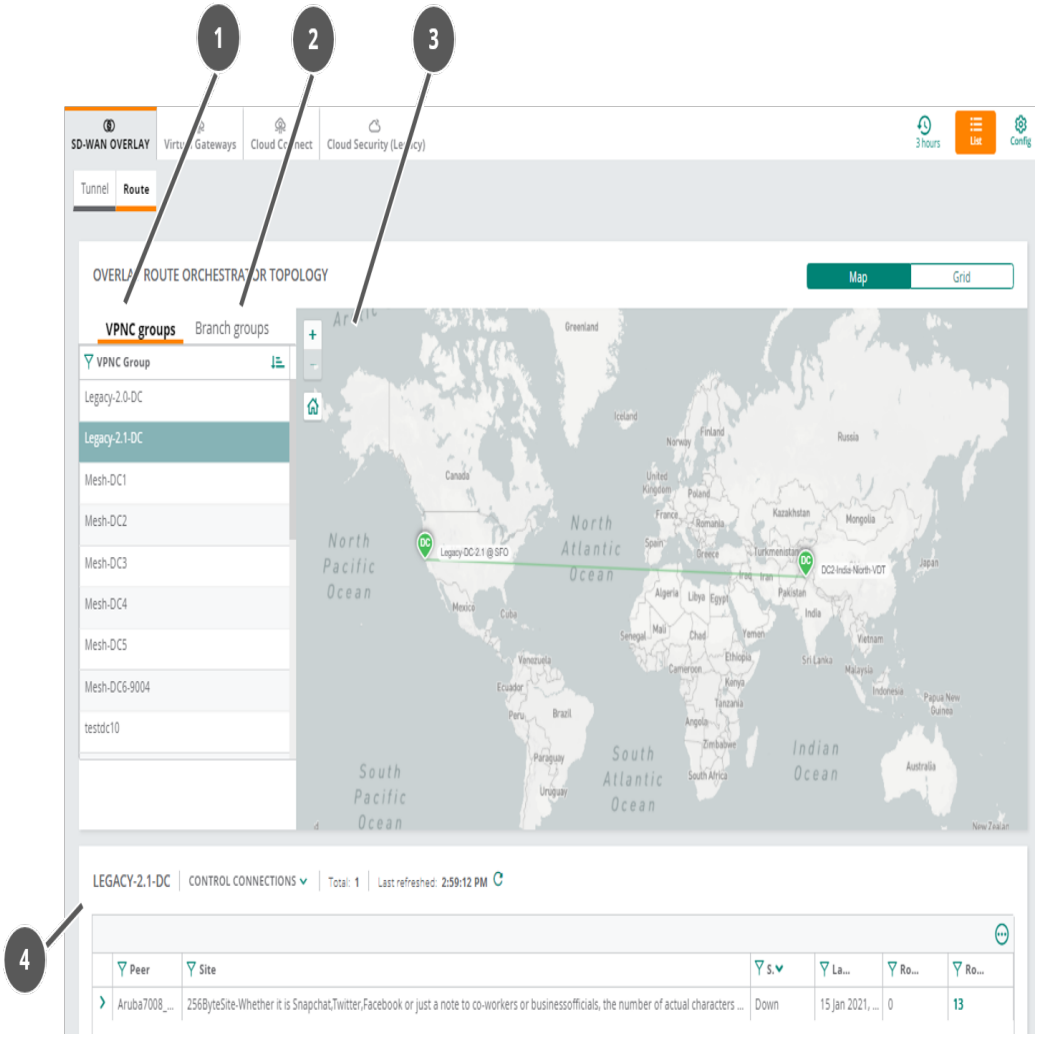
- Map View—A pictorial representation of the geographical location of SD-Branch deployment sites with hub mesh or branch mesh topologies.
- Grid View—The topology information for VPNC groups and branch groups in a tabular format.

Map View

The **Map** view consists of the following sections:

- VPNC Groups Filter
- Branch Groups Filter
- Map View
- Contextual Summary Table

Figure 201 *Overlay Route Orchestrator in Map View*



The following table explains the interface elements of the map view.

Table 255: *User Interface Elements*

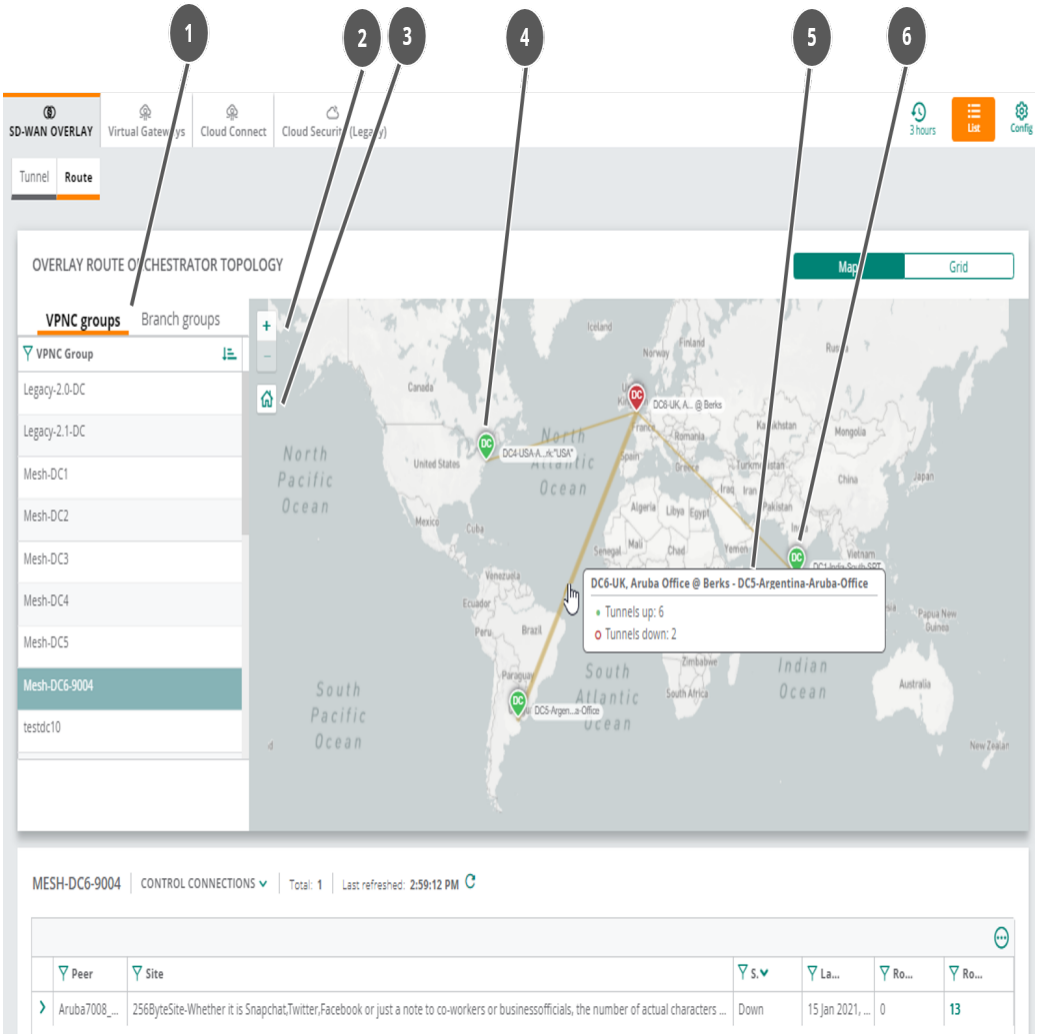
Number	UI Element	Description
1	**VPNC** Groups Filter	Displays the list of VPNC groups present in the network. VPNC groups are configured in a hub mesh topology.
2	**Branch Groups Filter**	Displays the list of branch groups present in the network. Branch groups are configured in a branch mesh topology.
3	**Map View**	Displays data centers as pins and mesh links as bars (lines). Selecting a group depicts the location of the deployment site and details of the data center preference configured for the branch devices. The map also indicates if the VPNCis set as the primary VPNC for the Branch Gateways in the group. Search Options: ■ The icon allows you to search a particular branch group. ■ The and icons allow you to sort the branch group names in ascending or descending order.
4	**Contextual Summary Table**	Displays information corresponding to the selected item (branch group or data center or tunnel). For example, if you have selected a VPNC group, the map displays the geographical location of the data centers and the summary table displays the **Peer**, **Site**, **Type**, **Tunnel State**, **Uptime**, **Last Status Change**, **Tunnels orchestrated**, and **Last Reset Reason** information. Every uplink in the orchestration displays **Type**, **Tag**, **Public IP**, and **Private IP** columns.

By default, the map view displays all the data centers of the SD-WAN overlay connected through a mesh link. Select a VPNC group or Branch group to view details specific to it.

VPNC Group—Map View Elements

The following features aid in reading the Overlay Route Orchestration Topology in the map view for a VPNC group.

Figure 202 *VPNC Group Viewing Options*



Branch group—Map View Elements

Figure 203 *Branch Group Viewing Options*

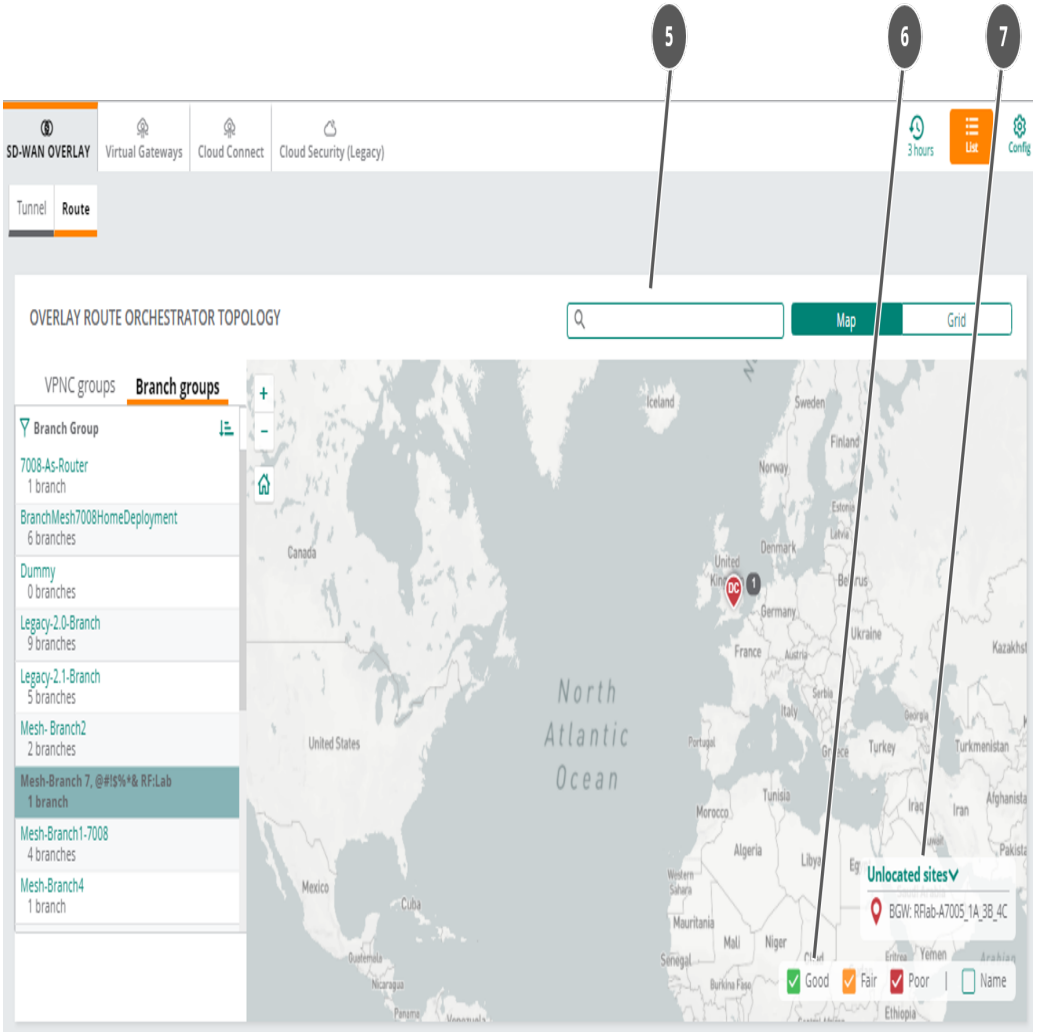
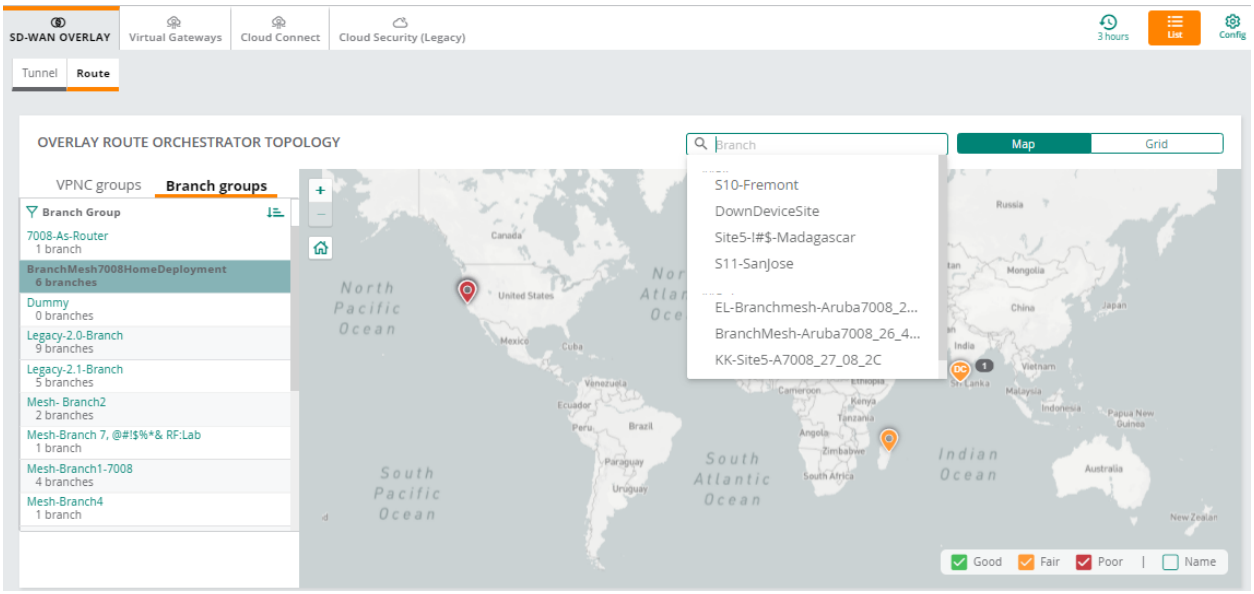


Figure 204 *Branch Group Mesh*



The following table explains how to read the elements in the map view.

Table 256: *VPNC Group and Branch Group Map View Elements*

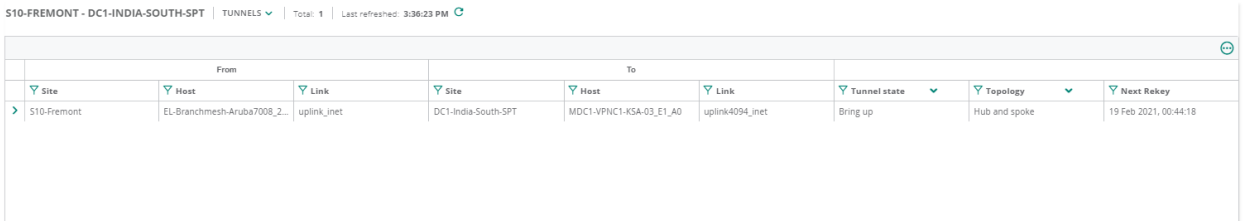
Number	UI Element	Description
1	**Branch Group Filter**	To view the branch group topology in the map, select a branch group from the **Branch Group** filter. The data centers (—pin) appear on the map. If the branch group is configured with hub-mesh topology, you can see mesh links (—bar) between the data centers.
2	**Zoom Buttons**	▪ Click **+** to zoom in. ▪ Click **-** to zoom out.
3	**Home Icon**	Click the Home icon to reset the map view.
4	**Data Center Pin**	Hover over the data center to view the data center name and its VPNCs.
5	**Tunnel lines**	When you select a branch group with mesh topology, there are tunnels formed between the data centers and branches. The tunnels are indicated by lines between the gateways.
	Tunnel Details	Hover over the tunnel link to view the number of active tunnels between the data centers. **NOTE:** Ensure to click the mesh link (bar) only when you see the hand pointer icon.
	Source and Destination Details	To view the source and destination site details of a tunnel, click the tunnel link. A pop-up window appears displaying the list of tunnels between the data centers and its corresponding information. The columns present in the pop-up window are: ▪ **Name**—Name of the tunnel. ▪ **From and To**—The **From** and **To** site, hosts and links that connect the tunnel. ▪ **Tunnel State**—Current status of the tunnel. ▪ **Next Rekey**—Time stamp for the next rekey. **NOTE:** ▪ Expand the drop-down to view details about the devices in the source and the destination such as the link type, their MAC and IP addresses and so on. ▪ Click the **Ellipses** icon to display more columns in the table. See the *Tunnel Details Pop-Up* topic for more information.
6	**Tunnel/Data Center Status**	The status of the tunnel and data center is indicated by colors. ▪ **Green**—Indicates active tunnels or data centers. ▪ **Red**—Indicates inactive tunnels or data centers. ▪ **Yellow**— Indicates one or more tunnels that are down.

Number	UI Element	Description
7	**Search Box**	Use this option to view the tunnel links between the branch groups based on the selected site or host. To view the mesh representation for a site or host, select the branch group and specify the site name or host name in the search box. The available sites and hosts for the selected branch group appear in the auto-suggest box. The mesh links appear for the selected site or host. Zoom in on the map view to view all the mesh topologies for the selected site or host.
8	**Unallocated Sites**	Displays the Branch Gateways that are not assigned to a site. ■ Click the number to view the device details. ■ Click the down arrow to expand the pane. **NOTE:** The **Unallocated Sites** drop-down appears only for Branch Groups, which has SD-WAN Branch Gateways that are not associated with any sites.
9	**Status Filter**	Select or clear the options to view the pins on the map. ■ **Good**—Select this option to view the Branch Gateways that are active. ■ **Fair**—Select this option to view the Branch Gateways that are partially active. ■ **Poor**—Select this option to view the Branch Gateways that are not active. ■ **Name**—Select this option to display the Branch Gateways name over the pin on the map.

Tunnel Details Pop-Up

In the map view for the **Overlay Route Orchestrator Topology**, click the tunnel link to display the tunnel details pop-up window.

Figure 205 *Pop-up—Tunnel Details*



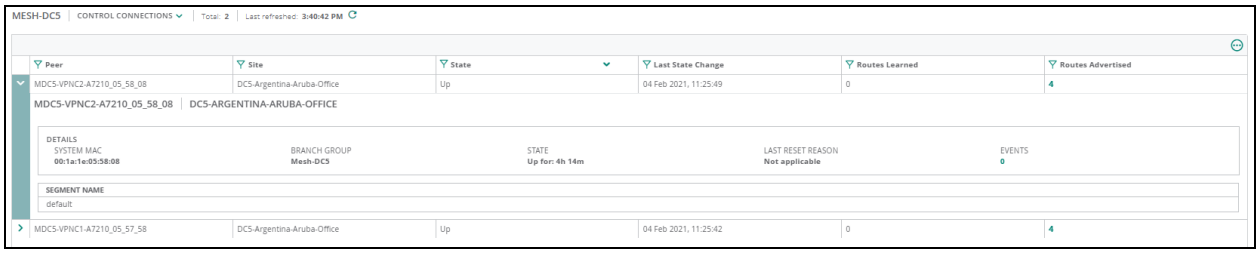
Contextual Summary Table

To view the overlay route for each group and the devices in a group, select the VPNC group or Branch group in the **Map** or **Grid** view. The route details for gateways corresponding to the selected VPNC group or Branch group is displayed in the bottom of the page. The details displayed in the summary table are contextual to the selected item in the **Map** or **Grid**. If you select the group, the values in the columns correspond to the group. Similarly, if you select the data center or tunnel, the respective values are displayed.

By default, the **Control Connections** option is selected and the following details are displayed for each Branch Gateway in a group:

- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **Peer**—The list of peer Branch Gateway devices that exchanged routes.
- **Site**—The physical location of the SD-Branch site.
- **State**—The state of the connection, which could be **Up**, **Down**, **Bring up**, **Inactive**, or **Unknown**.
- **Last State Change**—The time stamp of the last state change.

Figure 206 *Overlay Route Orchestrator Device Details*

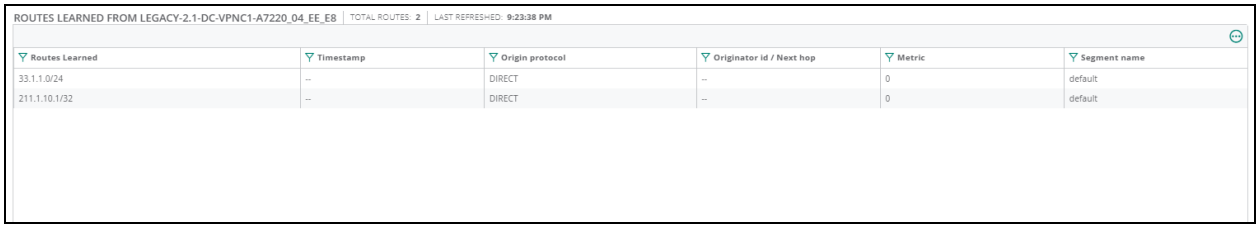


- **Routes Learned**—The number of routes that are learned from other peer devices. Click the number to view the details of the routes learned from the device.

  The Routes Learned table displays the following:

  - **Routes Learned**—Displays the route.
  - **Timestamp**—Displays the time.
  - **Origin Protocol**—Displays the originating protocol.
  - **Originator ID/Nexthop**—Displays the originator ID or nexthop information.
  - **Metric**—Displays the metric value of the route.
  - **Segment Name**—Displays the segment associated to the route.

Figure 207 *Details of the Routes Learned*



- **Routes Advertised**—The number of advertised routes. Click the number to view the details of the routes advertised by the device

  The Routes Advertised table displays the following:

  - **Routes Advertised**—Displays the route.
  - **Timestamp**—Displays the time.
  - **Nexthop**—Displays information about the next hop.
  - **Origin Protocol**—Displays the originating protocol.
  - **Cost**—Displays cost associated with the route.
  - **Link type**—Displays type of the link which could be **Unknown**, **Branch**, or **Hub**.
  - **Segment Name**—Displays the segment associated for the route.

- **Origin Type**—Displays the origin of route which could be **Unknown**, **Branch, Data Center**, **Branch Aggregate**, or **Data Center Aggregate**.
- **Origin Site**—Displays the originating site.

Figure 208 *Details of the Routes Advertised*

- **System MAC**—The MAC address of Branch Gateway.
- **Branch Group**—The group to which the device is assigned.
- **Duration**—The uptime or downtime of the Branch Gateway.
- **Last Reset Reason**—The reason that triggered the last reboot.

Expand the device to view the peer device details and the link to **Events** log:

Events—The link to the table that lists the events recorded. Click **Events** to open the **Event Logs** table.

- **Date/Time**—The timestamp of the event.
- **Severity** —Specifies whether the event is a **Warning**, an **Alert**, or a **Notice** based on the severity of the event.
- **Type**—Specifies the type of event
  - **Config**—Configuration specific event.
  - **Route**—Route specific event.
  - **Device**—Device specific event.
- **Sub Type—**Specifies the **Sub Type** of the event. It could be one of the following.
  - **Connection**—Connection specific event.
  - **Tunnel**—Tunnel specific event.
  - **Route**—Route specific event.
  - **Config**—Configuration specific event.
  - **Customer**—Customer specific event.
- **Description**—A brief description of the event.

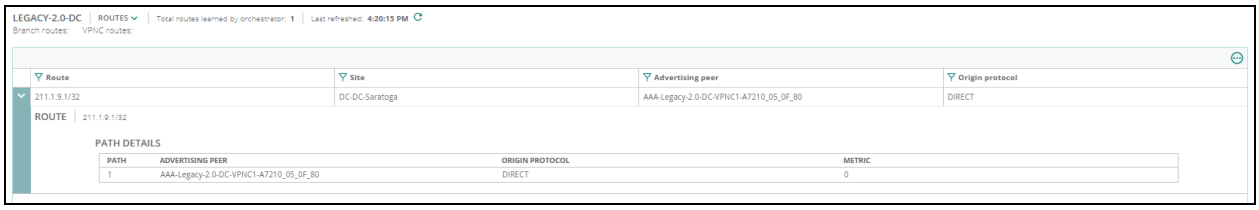
Figure 209 *Overlay Route Orchestrator Event Logs*

In the contextual summary table, select **Routes** in the drop-down. The following details are displayed:

- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **Route**—The route advertised.

- **Site** —The data center or the hub site that originated the routes.
- **Advertising Peer**—The peer device that advertised the route.
- **Origin Protocol**—The routing protocol that originated the route.
- **Metric**—The cost associated with the route
- **Segment Name**—Displays the segment associated to the route.

Figure 210 *Overlay Route Orchestrator Route Details*



Overlay Route Orchestrator in Grid View

The **Grid** view provides the topology information for each VPNC group and Branch group in a tabular format. The topology consists of the hub and spoke, hub mesh network between VPNCs, and the branch mesh network between the gateways. For information about how to create hub mesh and branch mesh topologies, see Configuring the SD-WAN Hub Mesh Topology and Branch Mesh Topology in SD-Branch .

- **VPNC groups**—When VPNC group tab is selected, the table displays the data center name and the mesh topology to which it belongs.
- **Branch groups**—When Branch group tab is selected, the table and contextual summary table panes are displayed. The Branch group table displays the Branch Group, DC Preference, Site, Preferred VPNC, Latitude, and Longitude details. The contextual summary table displays details for the selected branch group.

The following topics are discussed in this section:

- Navigating to the Grid View
- Overlay Route Orchestrator Topology

Navigating to the Grid View

To view the orchestration topology details in a grid:

1. In the **Network Operations** app, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Network Services > SD-WAN Overlay**.
   The **SD-WAN Overlay** page is displayed in the **List** view. This is the default view. The page consists of two tabs:
   - **Tunnel**—Consists of the **Overlay Tunnel Orchestrator Topology** pane with the **Map** and **Grid** tabs.
   - **Route**—Consists of the **Overlay Route Orchestrator Topology** pane with the **Map** and **Grid** tabs.
3. Click **Grid**.
   The orchestration details are displayed in a tabular format. The following tabs are present:

- **VPNC groups**—Consists of VPNC groups table.
- **Branch groups**—Consists of Branch groups table.

  The contextual summary table appears only when a VPNC group or a Branch group is selected.

Overlay Route Orchestrator Topology

You can view the **Overlay Route Orchestrator Topology** details as follows:

- Map View—A pictorial representation of the geographical location of SD-Branch deployment sites.
- Grid View—The topology information for each branch group in a tabular format.

Grid View

The **Grid** view consists of the following sections:

- VPNC Groups
- Branch Groups
- Contextual Summary Table

VPNC Groups

The **VPNC Groups** tab consists of the data center name and the mesh topology to which it belongs.

- **Name**—The data center name.
- **Hub Mesh**—The hub mesh topology to which the data center is associated.

Branch Groups

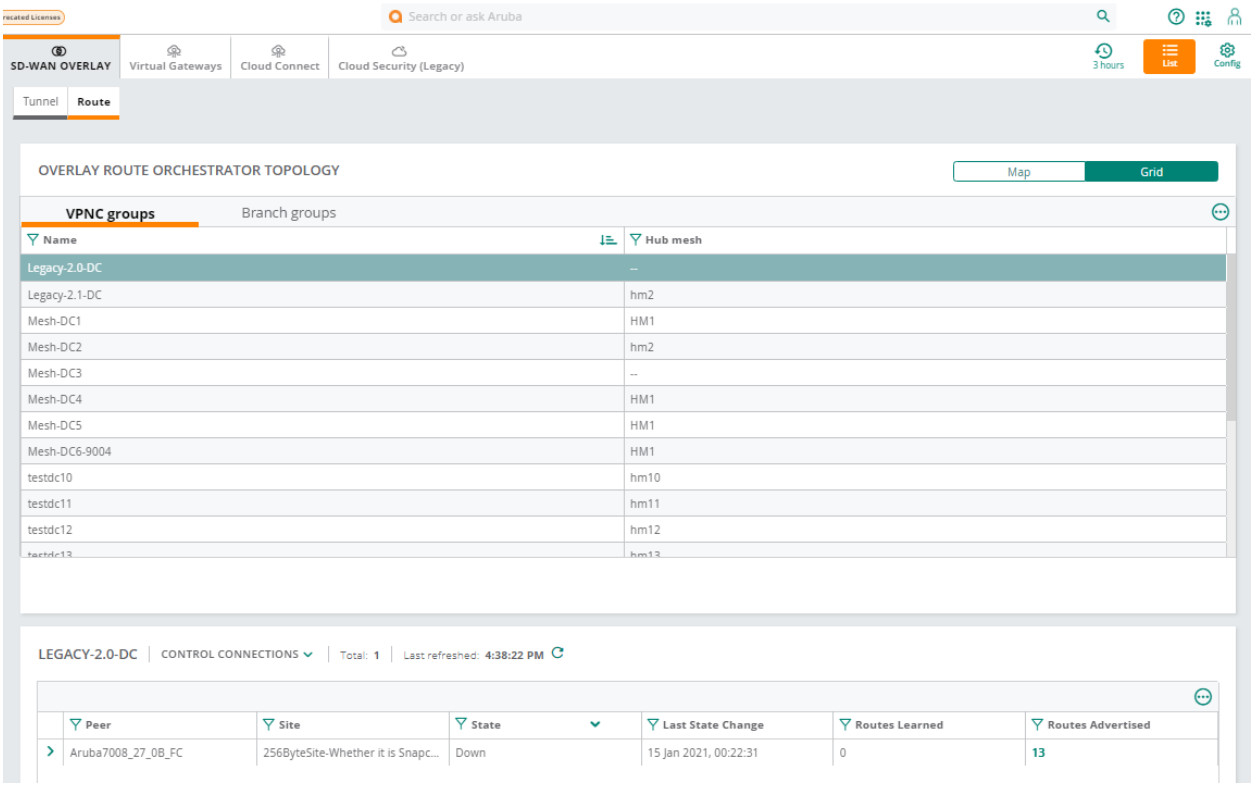
The **Branch Groups** tab consists of the Branch groups table and contextual summary table.

The Branch groups table details are as follows:

The search box is available only for the **Branch groups** in **Map** and **Grid** views. Use this option to view information about the required tunnel links between the branch groups based on the selected site.

- **Branch Group**—The name of the device group in which the Aruba Gateways are provisioned.
- **DC Preference**—The data center preference order configured for the branch devices.
- **Site**—The physical location of the SD-Branch site.
- **Preferred VPNC**—The preferred hub sites.
- **Latitude**—The latitude of the SD-Branch topology.
- **Longitude**—The longitude of the SD-Branch topology.

Figure 211 *Overlay Route Orchestrator in Grid View*



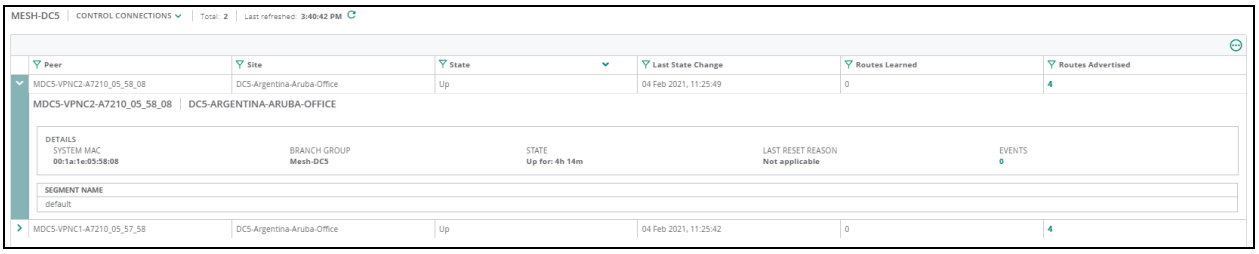
Contextual Summary Table

To view the overlay route for each group and the devices in a group, select the VPNC group or Branch group in the **Map** or **Grid** view. The route details for gateways corresponding to the selected VPNC group or Branch group is displayed in the bottom of the page. The details displayed in the summary table are contextual to the selected item in the **Map** or **Grid**. If you select the group, the values in the columns correspond to the group. Similarly, if you select the data center or tunnel, the respective values are displayed.

By default, the **Control Connections** option is selected and the following details are displayed for each Branch Gateway in a group:

- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **Peer**—The list of peer Branch Gateway devices that exchanged routes.
- **Site**—The physical location of the SD-Branch site.
- **State**—The state of the connection, which could be **Up**, **Down**, **Bring up**, **Inactive**, or **Unknown**.
- **Last State Change**—The time stamp of the last state change.

Figure 212 *Overlay Route Orchestrator Device Details*

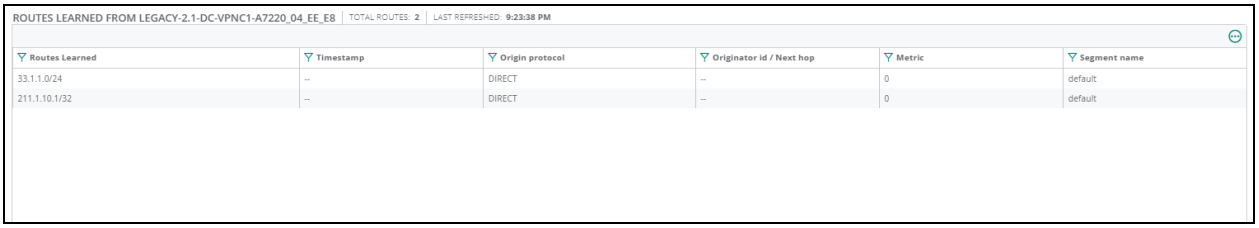


- **Routes Learned**—The number of routes that are learned from other peer devices. Click the number to view the details of the routes learned from the device.

  The Routes Learned table displays the following:

  - **Routes Learned**—Displays the route.
  - **Timestamp**—Displays the time.
  - **Origin Protocol**—Displays the originating protocol.
  - **Originator ID/Nexthop**—Displays the originator ID or nexthop information.
  - **Metric**—Displays the metric value of the route.
  - **Segment Name**—Displays the segment associated to the route.

Figure 213 *Details of the Routes Learned*



- **Routes Advertised**—The number of advertised routes. Click the number to view the details of the routes advertised by the device

  The Routes Advertised table displays the following:

  - **Routes Advertised**—Displays the route.
  - **Timestamp**—Displays the time.
  - **Nexthop**—Displays information about the next hop.
  - **Origin Protocol**—Displays the originating protocol.
  - **Cost**—Displays cost associated with the route.
  - **Link type**—Displays type of the link which could be **Unknown**, **Branch**, or **Hub**.
  - **Segment Name**—Displays the segment associated for the route.
  - **Origin Type**—Displays the origin of route which could be **Unknown**, **Branch, Data Center**, **Branch Aggregate**, or **Data Center Aggregate**.
  - **Origin Site**—Displays the originating site.

Figure 214 *Details of the Routes Advertised*

- **System MAC**—The MAC address of Branch Gateway.
- **Branch Group**—The group to which the device is assigned.
- **Duration**—The uptime or downtime of the Branch Gateway.
- **Last Reset Reason**—The reason that triggered the last reboot.

Expand the device to view the peer device details and the link to **Events** log:

Events—The link to the table that lists the events recorded. Click **Events** to open the **Event Logs** table.

- **Date/Time**—The timestamp of the event.
- **Severity** —Specifies whether the event is a **Warning**, an **Alert**, or a **Notice** based on the severity of the event.
- **Type**—Specifies the type of event
  - **Config**—Configuration specific event.
  - **Route**—Route specific event.
  - **Device**—Device specific event.
- **Sub Type—**Specifies the **Sub Type** of the event. It could be one of the following.
  - **Connection**—Connection specific event.
  - **Tunnel**—Tunnel specific event.
  - **Route**—Route specific event.
  - **Config**—Configuration specific event.
  - **Customer**—Customer specific event.
- **Description**—A brief description of the event.

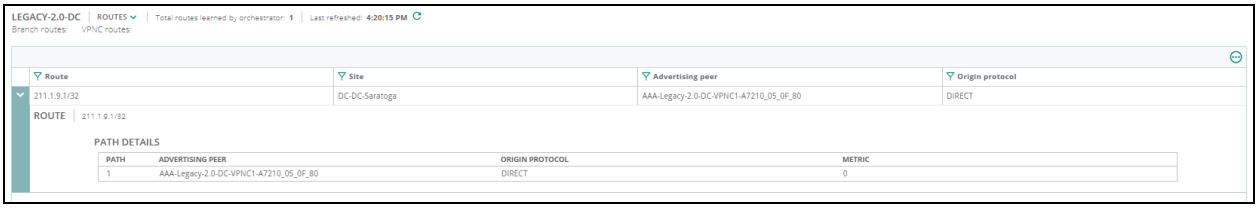
Figure 215 *Overlay Route Orchestrator Event Logs*

In the contextual summary table, select **Routes** in the drop-down. The following details are displayed:

- **Total**—The total number of control connections established.
- **Last Refreshed**—Indicates when the last refresh was completed. Click the refresh icon to display the latest information.
- **Route**—The route advertised.
- **Site** —The data center or the hub site that originated the routes.
- **Advertising Peer**—The peer device that advertised the route.
- **Origin Protocol**—The routing protocol that originated the route.

- **Metric**—The cost associated with the route
- **Segment Name**—Displays the segment associated to the route.

Figure 216 *Overlay Route Orchestrator Route Details*



Configuring the SD-Branch Overlay Network

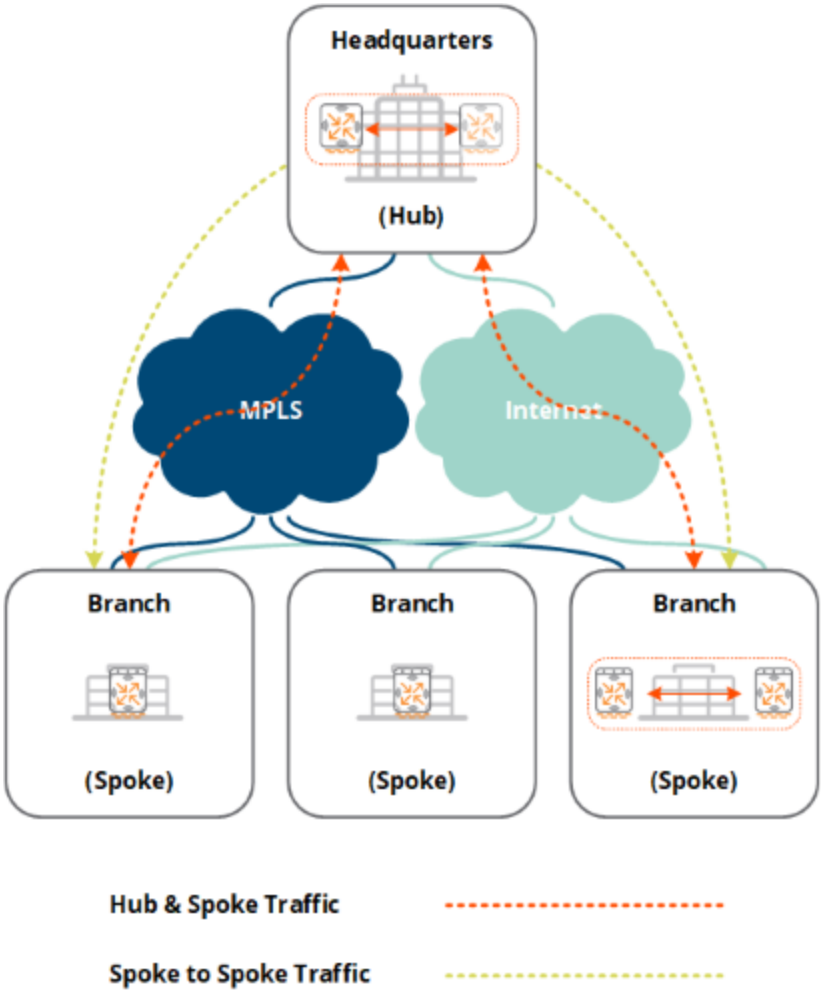
The Aruba SD-Branch solution supports the hub and spoke topology and uses IPsec tunnels between the branch and the hub sites to build an SD-Branch overlay network. Hub sites are typically the corporate headquarters or data centers that include one or more Gateways operating as VPNCs, while branch sites or spokes include one or more Branch Gateways. The overlay network securely transports traffic forwarded between the hub and branch sites.

The SD-Branch deployment includes at least one hub site with one or more VPNCs that terminate IPsec-based VPN tunnels initiated from the Branch Gateways. Based on the deployment size and redundancy requirements, you can deploy one or more VPNCs at each hub site.

Overriding port-based tunnel client VLAN on the controller is supported only for untagged VLANs configured on the port-based tunneling switch port. It is not supported when both untagged and tagged VLANs are configured on the port-based tunneling switch port.

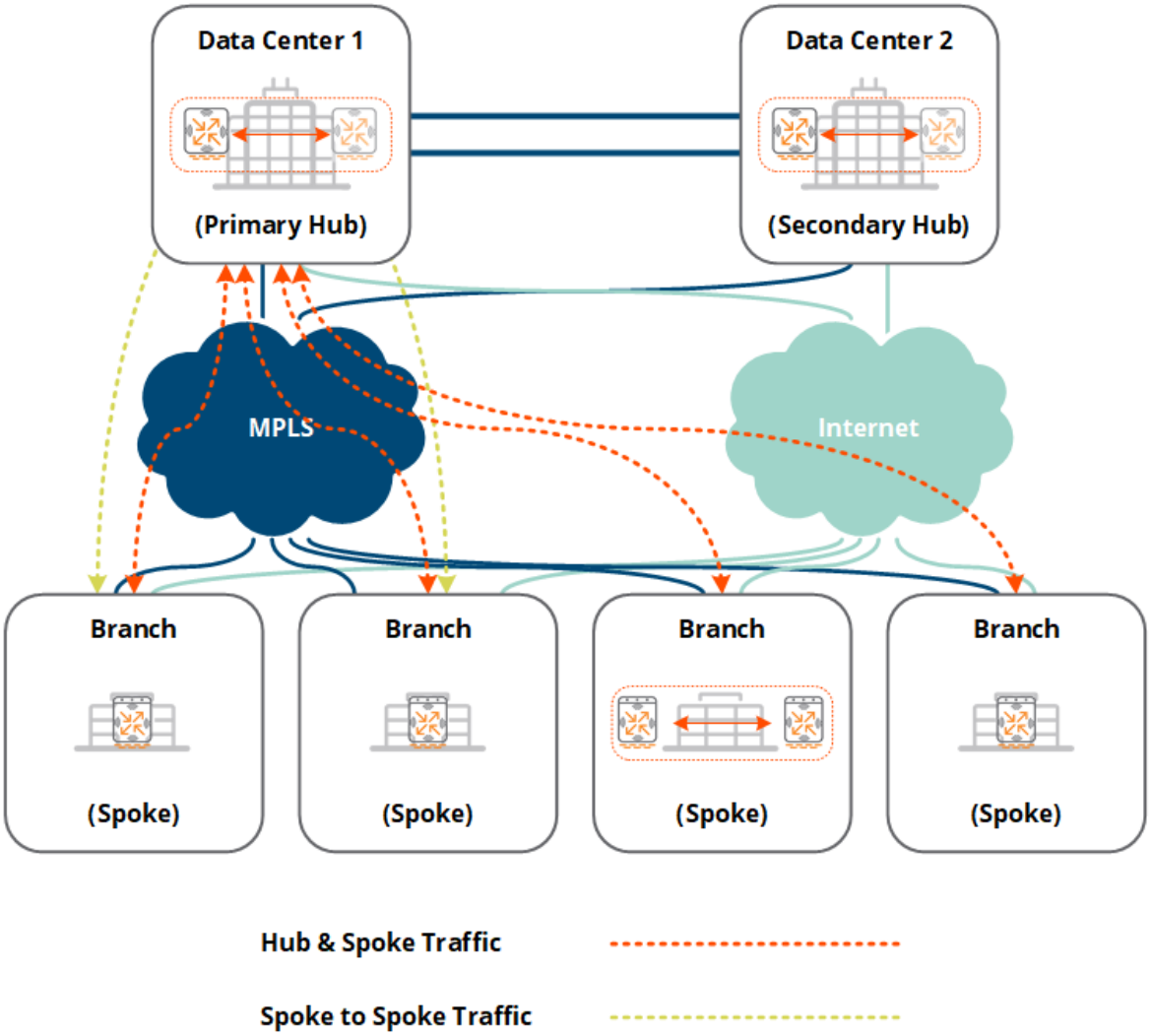
The following figure illustrates the hub and spoke topology with a single hub site:

Figure 217 *Hub and Spoke Topology: Single Hub Site*



Large deployments may include additional hub sites to provide redundancy in the event of a primary hub site failure. The most common deployment consists of a primary and secondary hub, each with two redundant VPNCs, as shown in the following figure:

Figure 218 *Hub and Spoke Topology: Dual Hub Sites*



Configuration Recommendations

The Aruba SD-Branch overlay network based on the hub and spoke architecture requires the administrators to configure Gateways using the Aruba Central management interface. Administrators can either manually set up the Gateways for establishing VPN tunnels or use the tunnel orchestrator service in Aruba Central to enable Gateways to automatically establish VPN tunnels. When the VPN hub is set and the Branch Gateways are configured as spokes, Aruba Gateways authenticate using the built-in TPM certificates and automatically establish an overlay tunnel. Administrators can also upload custom certificates for authentication.

Important Points to Note

- The overlay IPsec VPN tunnels are initiated by Branch Gateways and terminated on a VPNC in a hub site using NAT traversal. For NAT traversal, the UDP 4500 port must be enabled.
- The VPN tunnels over MPLS based WANs typically terminate on a VPNC using a VLAN interface assigned a private IPv4 address.
- Internet-based WAN services can either be directly terminated on a VPNC using a public IPv4 or private IPv4 address assigned by the VLAN interface.

- Using the Aruba Central management interface, you can enable automatic allowlisting of Branch Gateways or manually add the list of hub sites on Branch Gateways.

Configuring Overlay Tunnels Automatically

The Aruba SD-Branch Solution supports the SD-Branch overlay orchestration service that automates the overlay tunnel and route configuration process. For more information on SD-WAN Overlay orchestration service, see SD-WAN Overlay Tunnel and Route Orchestration .

Manually Configuring Hub and Spoke VPN

To configure a hub and spoke topology for the SD-Branch overlay network, complete the following steps:

- Allowlisting Gateways Manually
- Enabling Automatic Allowlisting on Branch Gateways
- Advertising Branch Subnets to Hub Sites

Enabling Automatic Allowlisting of Gateways

In a hub and spoke VPN topology, where remote branches connect to the VPNC, newer branches are added in a staggered way. Each time a Branch Gateway is added, the branch information needs to be populated in the VPNC to allowlist the branch device. With large-scale deployments, this method can be error prone and cumbersome. The automatic allowlisting feature automates the process of allowing branch devices to connect to VPNCs and thus eliminates the need for configuring each device at the headend.

Using Aruba Central as a single management entity for Gateways, administrators can enable automatic allowlisting and define a passphrase for secure transmission of VPN traffic. The automatic allowlisting serves as a global configuration that enables all VPNCs to terminate tunnels initiated by the Branch Gateways provisioned in Aruba Central.

Automatic allowlisting configuration is required on both Branch Gateways and VPNC. Ensure that you enable this feature on both Branch Gateway and VPNC groups.

Enabling Automatic Allowlisting of Branch Gateway on a VPNC

To allowlist a Branch Gateway automatically on a VPNC, complete the following steps:

1. In the **Network Operations** app, select a group in which VPNCs are provisioned.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **VPN** > **SD-WAN Overlay**.
6. Select the **Overlay mode** as **Manual**.
7. Click **Automatically Allowlist Branch Gateways**.
8. Enter a passphrase for VPN peer authentication. Ensure that the same passphrase is configured on the Branch Gateways.

9. Select any of the following encryption methods from the **Encryption** drop-down list:
   - **Factory Cert**—To use the built-in TPM certificate for mutual authentication.\
   - **Custom Cert**—To use custom certificates for mutual authentication. If you want to use custom certificates, ensure that the CA and Server certificates are uploaded to the certificate inventory on Aruba Central. For more information, see Certificates.
10. To apply a route ACL to the IPsec session, select an ACL from the **Route ACL** drop-down.
11. To apply a session ACL, select an ACL from the **Session ACL** drop-down.
12. If you want to assign overlapping uplink IP addresses across the branches, enable the **Uplink IP addresses overlap across branches** feature and then enter the IP address range configured for the branch pool.
13. Click **Save Changes**.

Enabling Automatic Allowlisting on Branch Gateways

To enable Branch Gateways to automatically connect to VPNCs, complete the following steps::

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **VPN** > **SD-WAN Overlay**.
7. Select the **Overlay mode** as **Manual**.
8. Click **Automatically Allowlist Branch Gateways**.
9. Enter a passphrase for VPN peer authentication. Ensure that the same passphrase is configured on the Branch Gateways.
10. Select any of the following encryption methods from the **Encryption** drop-down list:
    - **Factory Cert**—To use the built-in TPM certificate for mutual authentication.
    - **Custom Cert**—To use custom certificates for mutual authentication. If you want to use custom certificates, ensure that the CA and Server certificates are uploaded to the certificate inventory on Aruba Central. For more information, see Certificates.
11. To apply a route ACL to the IPsec session, select an ACL from the **Route ACL** drop-down.
12. To apply a session ACL, select an ACL from the **Session ACL** drop-down.
13. If you want to assign overlapping uplink IP addresses across the branches, enable the **Uplink IP addresses overlap across branches** feature and then enter the IP address range configured for the branch pool.
14. Click **Save Changes**.
15. Select a group in which the Branch Gateway is provisioned.
16. Click **VPN** > **SD-WAN Overlay**.
17. Click **Connect automatically to VPNC**.

18. Enter the VPN peer authentication passphrase. The passphrase must be the same as the one configured on the VPNC for automatic allowlisting.
19. If required, advertise branch VLANs to all hubs.
20. Click **Save Settings**.

Allowlisting Gateways Manually

To manually allowlist Gateways, administrators must manually add the VPNCs as hubs in Branch Gateways and add the Branch Gateways to the VPNC database.

Adding a VPN Endpoint on Branch Gateways

To manually add a VPN endpoint on Branch Gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **VPN** > **SD-WAN Overlay**.
7. Click **VPN** > **SD-WAN Overlay**.
8. Click **+** from the **Hubs** table and add the following information:
   - **Primary VPNC**—Enter the MAC address of the primary VPNC.
   - **Backup VPNC**—If you have a backup VPNC deployed at your site, enter the MAC address of the backup VPNC.
   - **IP Address**—Enter the IP address of the VPNC.
   - **Source VLAN**—If you have more than one VPNC, enter the VLAN of WAN uplink VLAN interface of the Branch Gateway on which the VPN tunnel must initiate.
9. Select any of the following encryption methods from the **Encryption** drop-down list:
   - **Factory Cert**—To use the built-in TPM certificate for mutual authentication.
   - **Custom Cert**—To use custom certificates for mutual authentication. If you want to use custom certificates, ensure that the CA and Server certificates are uploaded to the certificate inventory on Aruba Central. For more information, see Certificates.
10. If required, advertise branch VLANs to all hubs.
11. Click **Save Settings**.

Adding Branch Gateways on VPNCs

To manually add Branch Gateways on VPNCs, complete the following steps:

1. In the **Network Operations** app, select a group in which the VPNCs are provisioned.
2. Under **Manage**, click **Devices** > **Gateways**.

3. Click the settings 

icon. The Gateway dashboard is displayed.
4. Click **VPN** > **SD-WAN Overlay**.
5. Click **+** from the **Branch Gateway Table** to add the MAC address of the Branch Gateways:
   - **MAC ADDRESS**—Enter the MAC address of the Branch Gateway.
   - **ENCRYPTION**—Select any of the following encryption methods from the **Encryption** drop-down list:
     - **Factory Cert**—To use the built-in TPM certificate for mutual authentication.
     - **Custom Cert**—To use custom certificates for mutual authentication. If you want to use custom certificates, ensure that the CA and Server certificates are uploaded to the certificate inventory on Aruba Central. For more information, see Certificates.
6. Click **Advanced** and configure the following parameters as per your requirements:
   - If you want to bring down the IPsec tunnel when the peer routes are lost on the LAN interface of the VPNC, select the **LAN health check** check box.
   - To apply a route ACL to the IPsec session, select an ACL from the **Route ACL** drop-down.
   - To apply a session ACL, select an ACL from the **Session ACL** drop-down.
   - If you want to assign overlapping uplink IP addresses across the branches, enable the **Uplink IP addresses overlap across branches** and then enter the IP address range configured for the branch pool.
7. Click **Save Changes**.

Advertising Branch Subnets to Hub Sites

Aruba recommends that you configure Branch Gateways to advertise branch networks to the hub sites in which the VPNCs are deployed. When this feature is enabled, Aruba devices use IKEv2 extensions to dynamically learn branch routes without the need for static routes configuration. The learned IKEv2 routes are typically redistributed to neighboring routers through OSPF or BGP.

To advertise branch subnets, complete the following steps:

1. In the **Network Operations** app, select a group in which VPNCs are provisioned.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **VPN** > **SD-WAN Overlay**.
6. Ensure that the **Overlay mode** is set to **Manual**.
7. Click **+** from the **Hubs** table and add the following information:
   - **Primary VPNC**—Enter the MAC address of the primary VPNC.
   - **Backup VPNC**—If you have a backup VPNC deployed at your site, enter the MAC address of the backup VPNC.
   - **Source VLAN**—If you have more than one VPNC, enter the VLAN of WAN uplink VLAN interface of the Branch Gateway on which the VPN tunnel must initiate.

8. Select any of the following encryption methods from the **Encryption** drop-down list:
   - **Factory Cert**—To use the built-in TPM certificate for mutual authentication.
   - **Custom Cert**—To use custom certificates for mutual authentication. If you want to use custom certificates, ensure that the CA and Server certificates are uploaded to the certificate inventory on Aruba Central. For more information, see Certificates.
9. If required, advertise branch VLANs to all hubs.
10. Click **Save Settings**.
11. Click **VPN** > **SD-WAN Overlay**.
12. To advertise branch subnets to all hubs:
    a. Turn on the **Advertise branch VLANs to all hubs** toggle switch.
    b. Select the VLANs to advertise. Ensure that you select only those VLANs that are required for device communication through the overlay network. For example, management or user VLAN.
13. To advertise a set of VLANs to a specific VPNC on the hub site, enter a list of VLANs in the **VLANs Advertised to this Hub** field in the **Hubs** table.
14. To optimize the number of routes advertised to the VPNCs on the hub site, turn on the **Summarize routes** toggle switch.
15. Click **Save Settings**.

Monitoring VPN Tunnels

To monitor the VPN Tunnel status, complete the following steps:

1. In the **Network Operations** app, select the Gateway for which you want to monitor the tunnels.
2. Under **Manage**, click **Overview** > **Tunnel**.

Configuring the SD-WAN Hub Mesh Topology

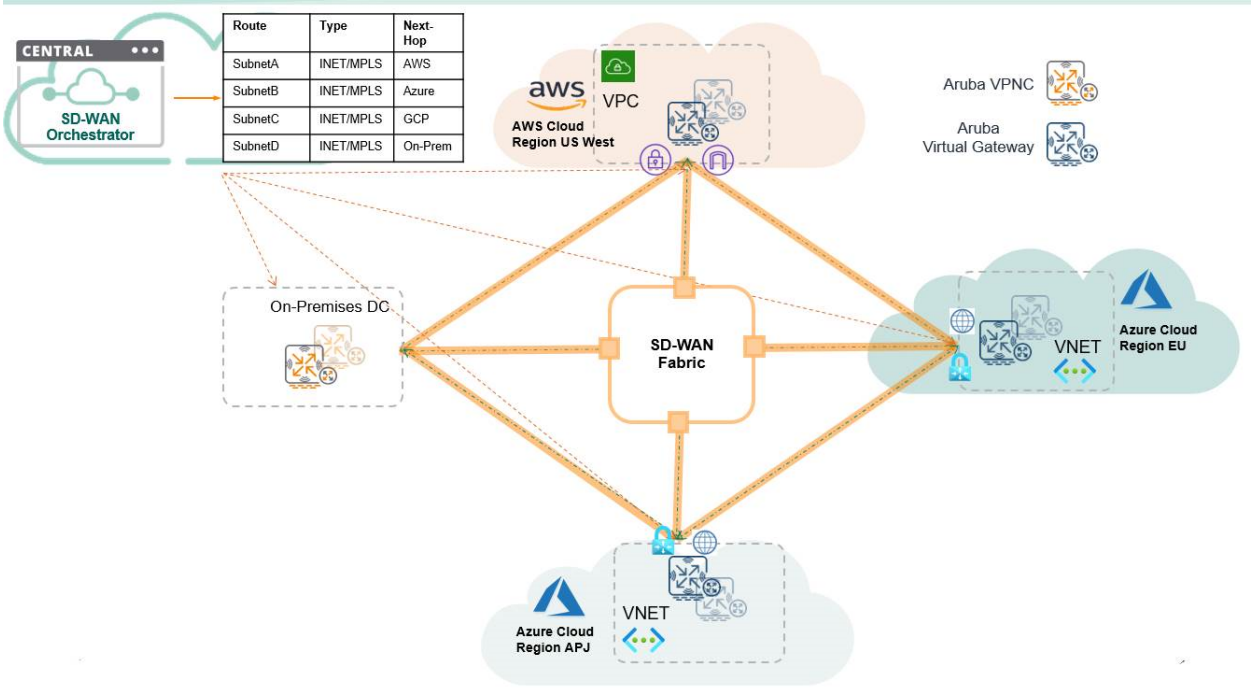
The Aruba SD-Branch solution supports the hub mesh topology that uses overlay tunnels to connect a hub site with one or more hub sites and build an SD-WAN mesh topology. A hub site is a headquarter or data center that includes one or more Gateways operating as VPNC.

When a mesh topology is configured between two or more hub groups, mesh links are formed between the VPNCs of selected hub groups creating an overlay network that securely transports traffic between the VPNCs of selected hub groups. These mesh links are displayed in the maps view of Overlay Tunnel Orchestrator. For more information, see Route and Tunnel pages.

The SD-Branch deployment includes at least one hub group with one or more VPNCs that terminate IPsec-based VPN tunnels initiated from the Branch Gateways. Based on the deployment size and redundancy requirements, you can deploy one or more VPNCs at each hub group.

The following figure illustrates the hub mesh topology between two hub groups:

Figure 219 *Hub Mesh Topology*



Configuration Recommendations

The Aruba SD-WAN hub mesh topology requires to manage the Branch Gateways through Aruba Central.

For optimal routing using hub mesh topology, it is strongly recommended to enable the Dynamic Data Center Path Computation. For more information, see Configuring Overlay Network Using SD-WAN Orchestrator.

Important Points to Note

- Hub mesh is established between data center groups, not between hubs belonging to the same group. Data center hubs bellowing to same group are expected to be connected via data center routing protocol.
- You can configure up to eight hub groups in a mesh topology.
- A hub group can be configured in one mesh topology only.

Configuring Hub Mesh Topology

To configure a hub mesh topology, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Network Services** > **SD-WAN Overlay**.
3. Click the **Config** icon.

   The configuration page is displayed.
4. Under **Topology** tab, click **Hub Mesh**.

   The **Hub Mesh Topology** configuration page is displayed.
5. To add a hub mesh topology, click **+**.
6. Provide a name for the new topology under **Create Hub Mesh Topology**.

7. Select the groups to be included in the hub mesh topology.

   You can add a minimum of two and a maximum of eight groups.
8. Click **Save Settings**.
9. To delete a mesh topology, select the respective hub mesh topology listed under the **Hub Mesh** tab and click the delete icon.
10. To confirm deletion, click **Yes**.

Branch Mesh Topology in SD-Branch

Branch mesh topology configuration is supported in this release as an Early-Access feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

The Aruba SD-Branch branch mesh topology configuration allows Branch Gateways to establish secure overlay tunnels with Branch Gateways those are part of a same group or different group. When a branch mesh topology is configured between two or more Branch Gateways, a branch mesh link is established to securely transport traffic between the Branch Gateways. The branch mesh link is a point-to-point link that allows traffic to flow from one Branch Gateway to another based on the subnets advertised by the destination Branch Gateway to the cloud orchestrator. Note that a destination Branch Gateway in a branch mesh topology never acts as a transit gateway. It is not necessary for Branch Gateways to be part of a same group to form a branch mesh tunnel. The Branch Gateways can be part of a same group or different group, and each Branch Gateway establishes a point-to-point secure tunnel with the other Branch Gateways which are part of the same branch mesh topology. The branch mesh links are displayed in the SD-WAN overlay map view of Overlay Tunnel Orchestrator. For more information, see Route and Tunnel pages. To form a branch mesh topology, following mechanisms are involved:

- The Overlay Tunnel Orchestrator (OTO) provides the tunnel specifications to the selected branch gateways based on the topology. When two branch gateways are selected, the OTO picks one branch gateway as the tunnel initiator and the other branch gateway as the tunnel responder and forms an IPsec tunnel between them over their uplinks. Initiator and responder role depends on the serial number of the device. The device with lower serial number from a pair of devices is picked as the initiator.
- The Overlay Route Orchestrator (ORO) sends the routes to selected branch gateways. ORO advertises originating branch gateway with lowest cost and data center VPNC with higher cost. Branch-to-branch path is preferred when the IPsec tunnel is up.
- To establish branch mesh tunnels between the two branch gateways, the Branch Gateways at both ends of the tunnel query the STUN server through their uplinks to learn the public IP and external facing post-NAT port.

  The STUN server's response to each message contains the post-NATed public IP information as seen by the STUN server. This IP could be different on all uplinks. The STUN protocol keeps the external-facing post-NAT port open and maintains the current mapping until the branch mesh tunnels using this port come up, ensuring that the port mapping does not expire on the NAT devices.

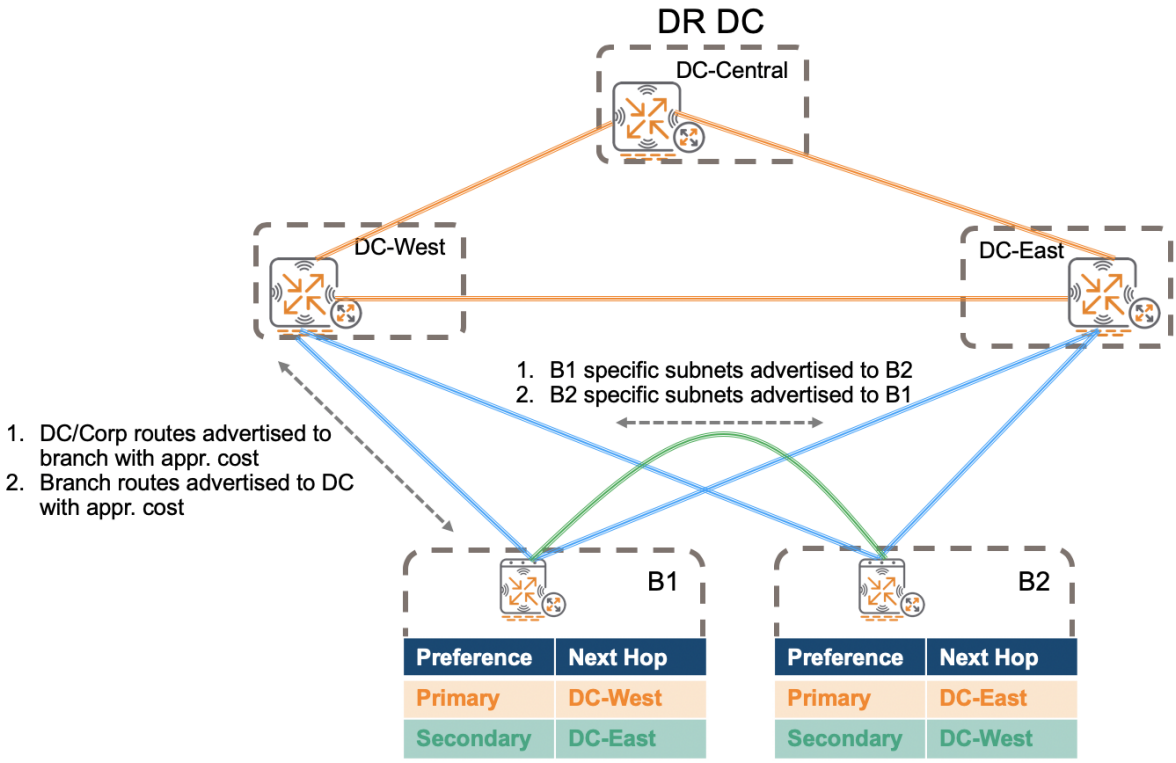
The following uplink data for the branch gateways is exchanged with OTO through the uplink AMON message so that OTO can bring up branch mesh tunnels:

- Private Uplink IP
- Source Port used by STUN for public IP discovery
- Public IP
- External facing post-NAT port discovered by STUN

When Branch-HA and branch mesh topologies intersect, the Branch Gateway is restricted from mistaking a branch mesh tunnel with a Branch-HA peer and does not set up IPsec tunnels between the Branch-HA peers.

The following figure illustrates a branch mesh topology between two Branch Groups:

Figure 220 *Branch Mesh Topology*



Configuration Recommendations

The Aruba SD-WAN branch mesh topology requires to manage the Branch Gateways through Aruba Central.

Important Points to Note

- Every branch group requires to be connected to a hub or data center (DC).
- Every branch group must have DC preference configured to participate in branch mesh topologies.
- You can configure up to 64 Branch Gateways in a branch mesh topology.
- You can configure up to 256 branch mesh topologies.
- A Branch Gateway can be part of multiple branch mesh topologies.

Configuring Branch Mesh Topology

To configure a branch mesh topology, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Network Services** > **SD-WAN Overlay**.
3. Click the **Config** icon.
   The configuration page is displayed.
4. Under **Topology** tab, click **Branch Mesh**.The **Branch Mesh Topology** configuration page is

displayed.

5. To add a branch mesh topology, click **+**.
6. Provide a name for the new topology under **Create Branch Mesh Topology**.
7. Click the drop-down under **Available Devices** and select a Branch Group.

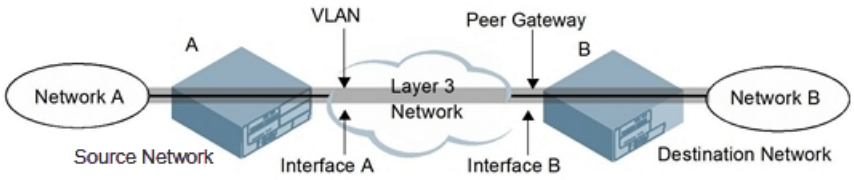
   The available Branch Gateways in the selected Branch Group are displayed.
8. Select one or more Branch Gateways from the Branch Group.
9. Click **Add>** for one or more Branch Gateways or **Add All>** to add all Branch Gateways. The selected Branch Gateways are displayed under **Selected Devices**.
10. Click **Save Settings**.
11. To delete a branch mesh topology, select the respective mesh topology under the **Branch Mesh** tab and click the delete icon.
12. To confirm deletion, click **Yes**.

Configuring Site-to-Site VPN

A site-to-site VPN allows the branch sites to establish secure connections with one another over a public network, for example, the internet. A site-to-site VPN allows users from different locations to access network resources hosted within the corporate network.

Figure 221 illustrates the site-to-site VPN topology in which a tunnel connects Network A to Network B across the internet.

Figure 221 *Site-to-Site VPN Configuration Components*



As shown in Figure 221, the following parameters must be configured to set up a site-to-site VPN tunnel on a Branch Gateway A:

- The source network (Network A).
- The destination network (Network B).
- The VLAN on which Branch Gateway A's interface to the layer 3 network is located (Interface A in Figure 221).
- The peer gateway, which is the IP address of Branch Gateway B's interface to the layer 3 network (Interface B in Figure 221).

NOTE

For the site-to-site VPN, you must configure VPN settings on Branch Gateways deployed at both the local and remote sites.

Site-to-site VPNs allow sites in different locations to securely communicate with one another over a layer 3 network such as the internet.

Aruba Gateways support the following IKE SA authentication methods for site-to-site VPNs:

- Pre-shared key—The same IKE shared secret must be configured on both the local and remote sites. The MAC address of the VPNC should be added as the peer MAC address in the Branch Gateway to establish

the IKE/IPsec tunnel with the VPNC.

- Suite-B cryptographic algorithms—Branch Gateways support Suite-B cryptographic algorithms when the Advanced Cryptography license is installed.
- Digital certificates—You can configure an RSA or ECDSA server certificate and a CA certificate for each site-to-site VPN IPsec map configuration. If you use certificate-based authentication, the peer must be identified by its certificate subject name, distinguished name (for deployments using IKEv2), or peer's IP address (for IKEv1).

Configuring IPsec Map for Site-to-Site VPNs

To configure IPsec map parameters for a site-to-site VPN, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **VPN** > **Site to Site**.
7. In the **IPsec Maps** section, click **+** to open the **New Ipsec Map** section.
8. Configure the required parameters as described in Table 257.
9. Save the changes.

Table 257: *IPsec Map Parameters*

Parameter	Description
Name	Enter a name for the VPN connection.
Enabled	Select the check box.
Priority	Enter a priority level for the IPsec map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next highest-priority map until a match is found.
Source network type	Select one of the following options to identify the source, the local VPN network connected to the Branch Gateway: ■ **IP Address**—The source is identified by an IP address. ◦ **Source network** —If you selected **IP Address**, you must enter the IP address of the source network. ◦ **Source subnet mask**—Enter the netmask for the source network. ■ **VLAN**—The source is identified by a VLAN ID. ◦ **VLAN**—If you selected the VLAN ID for the source network type, you must specify the VLAN ID from the drop-down list. ■ **Any**—The source can be any network.

Table 257: *IPsec Map Parameters*

Parameter	Description
Destination network type	Select one of the following options to identify the destination, the remote network to which the local network communicates: ■ **IP Address**—The destination is identified by an IP address. ◦ **Destination network** —If you selected **IP Address**, you must enter the IP address of the destination network. ◦ **Destination subnet mask**—Enter the netmask for the destination network. ■ **Any**—The destination can be any network.
IKE version	Select **v1** to configure the VPN for IKEv1, or **v2** for IKEv2. For more information on configuring an IKE policy, see Configuring IKE Policies.
IKE policy	(Optional) Click the **Policies** drop-down list and select a predefined or custom IKE policy to apply to the IPsec map.
Transforms	Add one or more transform sets to be used by the IPsec map. Click **+** and select an existing transform set or create a new one. Then click **Apply** to add that transform set to the IPsec map. If you selected **Add new transform** enter the follwoing details: ■ **Name**—Enter a name for the transform. ■ **Encryption**—Select the encryption level from the drop-down list. ■ **Hash**—Select the hash key fromthe drop down list.
Remote peer addressing	Select one of the following options: ■ **Static**—For site-to-site VPNs with peers that have static IP address. ■ **Dynamic**—For site-to-site VPNs with dynamically addressed peers.
Peer gateway type	The peer gateway type can be one of the following values: ■ **IP address**—If you selected this option, then specify an IP address in the **Peer gateway IPv4** field. ■ **FQDN**—If you selected this option then specify a value in the **Destination gateway FQDN** field.
Destination gateway	This field is applicable only if you selected **Dynamic** in the **Remote peer addressing** field. Select one of the following options: ■ **Initiator**—Select this if the dynamically addressed switch is the initiator of IKE Aggressive-mode for site-to-site VPNs. ■ **Responder**— Select this option if the dynamically addressed switch is the *responder* for IKE Aggressive-mode.
Source FQDN	Enter an FQDN for the Branch Gateway if the Branch Gateway is defined as a dynamically addressed responder, ■ **All Peers** Select this option to make the Branch Gateway a responder for all VPN peers. ■ **Per Peer Id** Select this option to make the Branch Gateway a responder for one specific initiator. Specify the **FQDN id** of the specific initiator to which the Branch Gateway acts a responder.

Table 257: *IPsec Map Parameters*

Parameter	Description
VLAN	Select the **VLAN** containing the interface of the Branch Gateway that connects to the layer 3 network. This determines the source IP address used to initiate IKE. If you selected **0** or **None**, the default is the VLAN of the Branch Gateway's IP address . **NOTE:** This field is not applicable if you have enabled **Load balance**.
Authentication method	Select one of the following authentication options: ■ **PSK**—Select this option for PSK authentication: ◦ **Representation type**—Select either **Text-based** or **Hex-based**. ◦ **IKE shared secret**—Enter a shared secret value. This authentication type is generally required in IPsec maps for a VPN with dynamically addressed peers, but can also be used for a static site-to-site VPN. ◦ **Retype shared secret**—Retype the shared secret value. ■ **Custom Certificate**—Select this option for certificate authentication: ◦ **Server certificate**—For certificate authentication, select the server certificates previously imported into the Branch Gateway. ◦ **CA certificate**— Select the CA certificates previously imported into the Branch Gateway. ◦ **Peer certificate subject name**—Enter the **peer certificate subject name**.

10. Click **Show Advanced Options** to view the parameters listed in the following table:

Table 258: *IPsec Map Parameters*

Parameter	Description
SA lifetime (seconds)	The specified value (in seconds) defines the lifetime of the IPsec security association. The default value is 7200 seconds. The allowed range is 300–86,400 seconds.
SA lifetime (kb)	The specified value (in kilobytes) defines the lifetime of the IPsec security association. The allowed range is 1000–1,000,000,000 kilobytes.
Trusted tunnel	Select the **Trusted tunnel** check box if the traffic between the networks is trusted. If you do not select this, then the traffic between the networks is untrusted.
Enforce NATT	Select the check box to enforce UDP 4500 for IKE and IPsec. This option is disabled by default.
Pre-connect	Select the **Pre-connect** check box to establish the VPN connection, even if there is no traffic being sent from the local network. If you do not select this, the VPN connection is established only when traffic is sent from the local network to the remote network.
IP compression	This option appears only if you selected **v2** as **IKE version**. IKEv2 site-to-site VPNs between VPNCs and Branch Gateways support traffic compression between those devices. Set **IP compression** to **Enabled** to enable compression for traffic in the site-to-site tunnel.

Table 258: *IPsec Map Parameters*

Parameter	Description
	Enabling this feature reduces the size of data frames transmitted over a site-to-site VPN between 7200 Series or 7000 Series controllers using IKEv2 authentication. IP compression can reduce the time required to transmit the frame across the network. When this hardware-based compression feature is enabled, the quality of unencrypted traffic (such as Lync or Voice traffic) is not compromised by increased latency or decreased throughput. IP compression is disabled by default. **NOTE:** This feature is only supported in an IPv4 network using IKEv2. This feature cannot be enabled on a 7205controller or on a site-to-site VPN that is established using IKEv1.
Factory certificate authentication	Select the check box to enable the Factory certificate authentication. **NOTE:** This option is applicable only if you selected **v2** as **IKE version**.
Inbound Route ACL	Select the inbound route ACL from the drop-down list. **NOTE:** This option is applicable only if you selected **v2** as **IKE version**.
PFS	If you enable **PFS** mode, new session keys are not derived from previously used session keys. Therefore, if a key is compromised, that compromised key does not affect any previous session keys. PFS mode is disabled by default. To enable this feature, click the **PFS** drop-down list and select one of the following PFS modes: ▪ **group1**—768-bit Diffie–Hellman prime modulus group ▪ **group2**—1024-bit Diffie–Hellman prime modulus group ▪ **group 14**—2048-bit Diffie–Hellman prime modulus group ▪ **group19**—256-bit random Diffie–Hellman ECP modulus group ▪ **group20**—384-bit random Diffie–Hellman ECP modulus group
Force tunnel mode	Select the check box to enforce tunnel mode. This option is disabled by default.

Enabling Dead Peer Detection

DPD is enabled by default on the Branch Gateway for site-to-site VPNs. DPD, as described in RFC 3706, uses IPsec traffic patterns to minimize the number of IKE messages required to determine the liveliness of an IKE peer.

Configuring Dead Peer Detection Parameters

To enable Dead Peer Detection, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group with branch gateways.
2. Go to **Manage** > **Devices** > **Gateways**, click the configuration 

icon. The gateway configuration page is displayed.
3. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
4. Click **VPN** > **DPD**.

5. Click **DPD** toggle switch to enable or disable the feature.
6. Enter the idle timeout, retry timeout, retry attempts, and Tunnel MTU in the respective fields.
7. Save the changes.

Configuring Site-to-Site VPN with GRE Tunnel

Site-to-site tunnel with GRE can be used to setup connections between Branch Gateways and their Enterprise headend. In site-to-site tunnel configuration, the VPN traffic is encapsulated using before entering the IPsec tunnels. Site-to-site tunnel configuration is required when VPNC at the data center is a non-Aruba device.

To set up a site-to-site VPN with GRE tunnel, complete the following tasks:

1. Configure a site-to-site VPN—For more information, see Configuring Site-to-Site VPN.
2. Configure GRE tunnel—For more information, see Configuring Layer 2 GRE Tunnels and Configuring Layer 3 GRE Tunnels.
3. Route the IPsec traffic into the GRE tunnel—For more information, see Directing Traffic into the GRE Tunnel.

Configuring GRE Tunnels

The headend gateway supports GRE tunnels between Branch Gateways and other network devices that support GRE tunnels.

To configuring a site-to-site VPN with GRE Tunnel, complete the following tasks:

- Configuring Layer 2 GRE Tunnels
- Configuring Layer 3 GRE Tunnels
- Configuring Tunnel Keepalives
- GRE Tunnel Groups
- Directing Traffic into the GRE Tunnel

Directing Traffic into the GRE Tunnel

You can direct traffic into a GRE tunnel by configuring a Static route, which directs traffic to the IP address of the tunnel, or a firewall policy (session-based ACL), that redirects traffic to the specified tunnel ID.

Configuring Static Routes

You can configure a static route that specifies the IP address of a tunnel as the next hop for traffic for a specific destination. See Configuring Static IP Routes for detailed information on how to configure a static route.

While redirecting traffic into a layer 3 GRE tunnel via a static route, be sure to use the tunnel IP address of the source Branch Gateway as the next hop, instead of providing the tunnel IP address of the destination Branch Gateway.

Configuring a Firewall Policy Rule

You can configure a firewall policy rule to redirect selected traffic into a GRE tunnel.

Traffic redirected by a firewall policy rule is not forwarded to a tunnel that is down (for more information on how GRE tunnel status is determined, see Configuring Tunnel Keepalives).

To configure a firewall policy for directing traffic into a GRE tunnel using session based ACLs, see Creating a Firewall Policy for Network Services.

1. Click **Submit**.
2. Click **Pending Changes**.
3. In the **Pending Changes** window, select the check box and click **Deploy changes**.

GRE Tunnel Groups

Branch Gateways support redundancy of GRE tunnels for both layer 2 and layer 3 GRE tunnels. This feature enables automatic redirection of the user traffic to a standby tunnel when the primary tunnel goes down.

A tunnel group is identified by a name or number. You can add multiple tunnels to a tunnel group. The order of the tunnels defined in the tunnel-group configuration specifies their standby precedence. The first member of the tunnel-group is the *primary tunnel*.

A GRE tunnel group combines two tunnels created on a Branch Gateway, where one tunnel is active and the other tunnel is the standby. Traffic forwarding can occur on the active tunnel, and the standby tunnel can become active once the active tunnel is down. When the first tunnel fails, the second tunnel carries the traffic. The third tunnel in the tunnel-group takes over if the second tunnel also fails. In the meantime, if the first tunnel comes up, it becomes the most eligible standby tunnel.

You can also enable or disable preemption as part of the tunnel-group configuration. Preemption is enabled by default. This **preemptive-failover** option automatically redirects the traffic whenever it detects an active tunnel with a higher precedence in the tunnel group. When preemption is disabled, the traffic gets redirected to a higher precedence tunnel only when the tunnel carrying the traffic fails.

When creating a tunnel group, remember the following points:

- When a tunnel is added to the tunnel group, the tunnel is used for data traffic only if it is the active tunnel in the group.
- Standby tunnels do not carry any data traffic. However, all tunnels in the group continue to send and receive keepalive packets.
- Only one type of tunnel can be placed into a tunnel group—either layer 2 or layer 3. That is, you cannot have a tunnel group consisting of both layer 2 and layer 3 tunnels.
- The default value of tunnel group type is layer 3.
- All tunnels in a layer 2 tunnel group must be tunneling the same VLAN.
- A layer 2 tunnel can only be part of one tunnel group.
- The Branch Gateway layer 2 tunnel-group is not interoperable with other vendors. You must set up layer 2 tunnel groups between Aruba devices only.

Configuring Tunnel Groups

To configure a layer 2 or layer 3 GRE tunnel group, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. In the **Interface** tab, click **+** in the **Tunnel Group** table.
4. Specify a name for the tunnel group in the **Tunnel Group Name** field.
5. In the **Tunnel Group Members** text box, click **+** to add one or more tunnel IDs.
6. Select the IDs and click **OK**.
7. To enable preemption, select the **Enable Preemptive-Failover Mode** check box. This option is enabled by default.
8. In the **Mode** section, identify the tunnel group type as a layer 2 or layer 3 group.
9. Click **Save Settings**.

Configuring Tunnel Keepalives

The headend gateway determines the status of a GRE tunnel by sending periodic keepalive frames on the layer 2 or layer 3 GRE tunnel. When you enable tunnel keepalives and the keepalives fail repeatedly, the tunnel is considered down.

If you configure a firewall policy rule to redirect traffic to the tunnel, traffic is not forwarded to the tunnel until it is up. When the tunnel comes up or goes down, an SNMP trap and logging message is generated. The remote endpoint of the tunnel does not need to support the keepalive mechanism.

The headend gateway sends keepalive frames at 60-second intervals by default and retries keepalives up to three times before the tunnel is considered down. You can change the default values of the intervals:

- For the **interval**, specify a value between 1 and 86400 seconds.
- For the **retries**, specify a value between 0 and 1024.
- To interoperate with Cisco network devices, select the **Cisco compatible** check box. This option is applicable only for layer 3 GRE tunnels.

To configure keepalives (Heartbeats), complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.

4. Under **Manage**, Click **Device**.

   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. To enable tunnel keepalives, select **Enable keepalive** and configure the following Keepalive options.
   - (Optional) To interoperate with Cisco network devices, select the **Cisco compatible** check box. This option is not applicable for layer 2 GRE tunnels.
   - Specify a value for **Heartbeat interval (secs)**.

     The default value is 10 seconds.
7. Specify a value for **Heartbeat retries**.

   The default value is 3 retries.
8. Click **Save Settings.**

Configuring Layer 3 GRE Tunnels

The headend gateway supports GRE tunnels between Branch Gateways and other network devices that support GRE tunnels.

Layer 3 GRE Tunnels

The benefit of layer 3 GRE tunnels is that broadcasts are not flooded through the tunnel, so there is less wasted bandwidth and less load on the Branch Gateway. The forwarding method for a layer 3 GRE tunnel is routing.

IPv6 encapsulated in IPv4 and IPv4 encapsulated in IPv6 are not supported. The only layer 3 GRE modes supported are IPv4 encapsulated in IPv4 and IPv6 encapsulated in IPv6.

Configuring a Layer 3 GRE Tunnel

To configure a layer 3 GRE tunnel for a source Branch Gateway and destination Branch Gateway, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway for which you want to configure a layer 3 GRE tunnel, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.

     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.

     c. Click **Config**.

        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the List view.

     c. Click a gateway under **Device Name**.

        The dashboard context for the gateway is displayed.

d. Under **Manage**, click **Device**.

The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. In the **Interface** tab, click **+** from the **GRE Tunnel** table to add a GRE tunnel. The **Add GRE Tunnel** section is displayed.
4. Select the **IP version** as **IPv4**.
5. Specify a tunnel ID in the **Tunnel ID** field.
6. Select the **Mode** as **L3**.
7. Select the **IPv4 address type** as one of the following options based on your requirements:
   - **Dynamic**—Select this option if you are configuring the tunnel ID for a device group. Then, select the required tunnel pool from the **Dynamic IP address pool** drop-down list. For more information on creating a tunnel pool, see Configuring Tunnel Pools for Aruba Gateways.
   - **Static**—Select this option if you are configuring the tunnel ID for a specific Branch Gateway. Then, enter the tunnel IP and the IP mask in the **IP address** and **IP mask** fields, respectively.
8. To enable OpenFlow on the tunnel, select the **Enable** check box.
9. To make the tunnel interface as trusted, select the **Trusted** check box.
10. Specify the MTU size for the tunnel interface in the **MTU** field.
11. Select one of the following options as the local end point of the tunnel from the **Tunnel Source** drop-down list based on your requirements:
    - **loopback**—Select this option to set the loopback IP as your tunnel source.
    - **ipaddr**—Select this option if you have a specific IP address as the tunnel source and specify the IP address in the **IP address** field.
    - **system-ip**—Select this option if your tunnel source is the IP address of the SD-WAN Gateway being configured.
    - **vlan**—Select this option if your tunnel source is a specific VLAN interface and specify the VLAN ID in the **VLAN** field.
12. Specify the destination IP address of the tunnel in the **Tunnel destination** field.
13. Select a route ACL name from the **Route ACL name** drop-down list to attach a route ACL to the inbound traffic on the L3 GRE tunnel interface.
14. To enable tunnel keepalives, select **Enable keepalive** and configure the following Keepalive options:
    - (Optional)To interoperate with Cisco network devices, select the **Cisco compatible** check box.
    - Specify a value for **Heartbeat interval (secs)**.

      The default value is 10 seconds.
    - Specify a value for **Heartbeat retries**.

      The default value is 3 retries.

    For more information on tunnel keepalive feature, see Configuring Tunnel Keepalives
15. To enable OSPF on the tunnel, select **Enable OSPF** and configure the following options:
    - **Area network (eg. 0.0.0.0)**—Enter the IP address of the OSPF area.
    - **Authentication**—If you want to authenticate OSPF neighbors for secure exchange of routing information, turn on the **Authentication** toggle switch. By default, the MD5 authentication method is used. Enter the **Message Digest key** and password.
    - **Cost**—Enter a value for cost. By default, the cost value is set to 1.
    - **Dead Interval**—Enter a dead time interval to enable devices to determine if a participating router is dead. If the hello packets are not received by a neighboring router for a given duration, the

router is declared as dead after the dead time interval is elapsed. The default dead time interval is 40 seconds.

- **Hello Interval**—Specify the interval for exchanging hello packets with the neighboring devices. The default value is 10 seconds.
- **Priority**—Specify a number to indicate a priority level for the routes transmitted from the tunnel interface. The default value is 1.
- **Retransmit Interval**—Specify a time interval for retransmitting LSAs. The default value is 5 seconds.
- **Transmit Delay**—Specify a delay interval for retransmitting LSAs. The default value is 1.

16. Click **Save Settings**.

If a VLAN interface has IPv6 addresses configured, one of them is used as the tunnel source IPv6 address. If the selected IPv6 address is deleted from the VLAN interface, then the tunnel source IP address is reconfigured with the next available IPv6 address.

Configuring Layer 2 GRE Tunnels

The headend gateway supports GRE tunnels between Branch Gateways and other network devices that support GRE tunnels.

Layer 2 GRE Tunnels

Layer 2 GRE tunnels allow you to have the same VLAN in multiple locations (separated by a layer 3 network) and be connected. The forwarding method for a layer 2 GRE tunnel is bridging.

However, the drawback of using layer 2 GRE tunnels is that all broadcasts are flooded through the tunnel, adding traffic load to the network and the Branch Gateway.

Configuring a Layer 2 GRE Tunnel

To configure a layer 2 GRE tunnel for a source Branch Gateway and destination Branch Gateway, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway for which you want to configure a layer 2 GRE tunnel, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.

d. Under **Manage**, click **Device**.

The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. In the **Interface** tab, click **+** from the **GRE Tunnel** table to add a GRE tunnel. The **Add GRE Tunnel** section is displayed.
4. Select the **IP version** as **IPv4**.
5. Specify a tunnel ID in the **Tunnel ID** field.
6. Select the **Mode** as **L2**.
7. Specify the layer 2 protocol to be used on the tunnel in the **Protocol** field.
8. In the **Vlans** field, specify the VLAN IDs of all the interfaces from which the traffic to be encapsulated originate.
9. To enable OpenFlow on the tunnel, select the **Enable** check box.
10. To make the tunnel interface as trusted, select the **Trusted** check box.
11. Specify the MTU size for the tunnel interface in the **MTU** field.
12. Select one of the following options as the local endpoint of the tunnel from the **Tunnel Source** drop-down list based on your requirements:
    - **loopback**—Select this option to set the loopback IP as your tunnel source.
    - **ipaddr**—Select this option if you have a specific IP address as the tunnel source and specify the IP address in the **IP address** field.
    - **system-ip**—Select this option if your tunnel source is the IP address of the SD-WAN Gateway being configured.
    - **vlan**—Select this option if your tunnel source is a specific VLAN interface and specify the VLAN ID in the **VLAN** field.
13. Specify the destination IP address of the tunnel in the **Tunnel destination** field.
14. To enable tunnel keepalives, select **Enable keepalive** and configure the following Keepalive options:
    - Specify a value for **Heartbeat interval (secs)**.

      The default value is 10 seconds.
    - Specify a value for **Heartbeat retries**.

      The default value is 3 retries.

    For more information on tunnel keepalive feature, see Configuring Tunnel Keepalives.
15. Save the changes.

Configuring IKE Policies

Branch Gateways support both IKEv1 and IKEv2 protocols to establish IPsec tunnels. Though both IKEv1 and IKEv2 support the same suite-B cryptographic algorithms, IKEv2 is a simpler, faster, and more reliable protocol than IKEv1.

This section covers the following topics:

- Configuring IKEv1 Policies and Dynamic Maps
- Configuring IKEv2 Policies and Dynamic Maps

Configuring IKEv1 Policies and Dynamic Maps

SD-WAN allows you to add or edit an existing IKEv1 policy or an IKEv1 dynamic map that can be used for an IPsec connection. Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. You can also define the authentication method and server addresses on the Branch Gateway.

The IKE policy selections, along with any preshared key, must be reflected in the VPN client configuration. When using a third-party VPN client, set the VPN configuration on clients to match the choices made above.

Use the following procedure to configure the authentication method, IKEv1 policies and dynamic IPsec maps on the Branch Gateway:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **VPN >IKEv1**.
6. To configure the authentication method, enable the required option:
   - To enable L2TP, select **L2TP**.
   - To enable XAuth, select **XAuth**.
7. Select an authentication method for IKEv1 clients. Currently, supported methods include:
   - **PAP**
   - **EAP**
   - **CHAP**
   - **MSCHAP**
   - **MSCHAPv2**
8. In the **IKEv1 Policies** table, click an existing policy to edit it, or click **+** to open the **Add IKEv1 Policy** section. Configure the required parameters as described in Table 259.

Table 259: *IKEv1 Policy Parameters*

Parameter	Description
Priority	Specify the priority number for this policy. Set the value to 1 for the configuration to take priority over the default setting.
Enable policy	Select the check box to enable the IKEv1 policy when it is saved.
Encryption	select one of the following encryption types: - DES - 3DES - AES128 - AES192 - AES256

Table 259: *IKEv1 Policy Parameters*

Parameter	Description
Hash algorithm	select one of the following hash types: ■ MD5 ■ SHA ■ SHA1-96 ■ SHA2-256-128 ■ SHA2-384-192
Authentication	Select one of the following authentication types for the IKE rule: ■ Pre-Share ■ RSA (for clients using certificates) ■ ECDSA-256 (for clients using certificates) ■ ECDSA-384 (for clients using certificates)
Diffie-Hellman group	Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie–Hellman Group for the ISAKMP policy, select one of the following options: ■ Group 1: 768-bit Diffie–Hellman prime modulus group ■ Group 2: 1024-bit Diffie–Hellman prime modulus group ■ Group 14: 2048-bit Diffie–Hellman prime modulus group ■ Group 19: 256-bit random Diffie–Hellman ECP modulus group ■ Group 20: 384-bit random Diffie–Hellman ECP modulus group
Lifetime	Set the lifetime of the IKE security association in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds.

9. In **IKEv1 IPSec Dynamic Maps**, click an existing dynamic map to edit it or click **+** to open the **Add IKEv1 Dynamic Map** section. Configure the required parameters as described in Table 260.

Table 260: *IKEv1 Dynamic IPsec Map Parameters*

Parameter	Description
Priority	Set the priority level for the IPsec map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next highest-priority map until a match is found.
Name	Enter a name for the dynamic map.
Dynamic map	Select the check box to enable the dynamic map. This is enabled by default.
PFS group	(Optional) Configure PFS settings for the dynamic peer by assigning a Diffie-Hellman prime modulus group. PFS group provides an additional level of security by ensuring that the IPsec SA key was not derived from any other key, and therefore, cannot be compromised if another key is broken. Select one of the following groups: ■ Group 1: 768-bit Diffie–Hellman prime modulus group

Table 260: *IKEv1 Dynamic IPsec Map Parameters*

Parameter	Description
	■ Group 2: 1024-bit Diffie–Hellman prime modulus group ■ Group 14: 2048-bit Diffie–Hellman prime modulus group ■ Group 19: 256-bit random Diffie–Hellman ECP modulus group ■ Group 20: 384-bit random Diffie–Hellman ECP modulus group
Transforms	Click **+** to open the **New Transform** section. The procedure to add an existing transform is as follows: 1. To add an existing transform, select **Add existing transform** 2. Select a transform from the list. 3. Click **Save Settings**. 4. To add a new transform, select **Add new transform**. 5. From the **Encryption** drop-down list, select one of the following encryption types: ■ DES ■ 3DES ■ AES128 ■ AES192 ■ AES256 6. From the **Hash** algorithm drop-down list, select one of the following hash types: ■ MD5 ■ SHA ■ SHA1-96 ■ SHA2-256-128 ■ SHA2-384-192 7. Click **Save Settings**.
Lifetime(seconds)	Set the lifetime of the security association for the dynamic peer in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds.
Lifetime(kilobytes)	Set the lifetime of the security association for the dynamic peer in kilobytes.

10. Save the changes.

Configuring IKEv2 Policies and Dynamic Maps

To configure the EAP passthrough, IKEv2 policies, and dynamic IPsec maps on the Branch Gateway, complete the following steps:

1. To configure a Branch Gateway group:
   - In the **Network Operations** app, use the filter to select **Groups**.
   - Under **Manage**, click **Devices** > **Gateways**, click the settings 

icon. The gateway configuration page is displayed.
2. Click **VPN >IKEv2**.

3. In **EAP passthrough**, select the EAP passthrough for IKEv2 clients. The currently supported methods include:
   - EAP-TLS
   - EAP-PEAP
   - EAP-MSCHAPv2
4. In the **IKEv2 Policies** table, click an existing policy to edit it, or click **+** to open the **Add IKEv2 Policy** section. Configure the required parameters as described in Table 261.

Table 261: *IKEv2 Policy Parameters*

Parameter	Description
Priority	Specify the priority number for this policy. Set the value to 1 for the configuration to take priority over the default setting.
Enable policy	Select the check box to enable the IKEv1 policy when it is saved.
Encryption	Select one of the following encryption types: ■ DES ■ 3DES ■ AES128 ■ AES192 ■ AES256
Hash algorithm	Select one of the following hash types: ■ MD5 ■ SHA ■ SHA1-96 ■ SHA2-256-128 ■ SHA2-384-192
Authentication	Select one of the following authentication types for the IKE rule: ■ Pre-Share (for IKEv1 clients using pre-shared keys) ■ RSA (for clients using certificates) ■ ECDSA-256 (for clients using certificates) ■ ECDSA-384 (for clients using certificates)
Diffie-Hellman group	Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie–Hellman Group for the ISAKMP policy, select one of the following options: ■ Group 1: 768-bit Diffie–Hellman prime modulus group ■ Group 2: 1024-bit Diffie–Hellman prime modulus group ■ Group 14: 2048-bit Diffie–Hellman prime modulus group ■ Group 19: 256-bit random Diffie–Hellman ECP modulus group ■ Group 20: 384-bit random Diffie–Hellman ECP modulus group
PRF	This algorithm is an HMAC function used to hash certain values during the key exchange. Set this to one of the following values based on the value selected for Hash algorithm: ■ PRF-HMAC-MD5 ■ PRF-HMAC-SHA1

Table 261: *IKEv2 Policy Parameters*

Parameter	Description
	■ PRF-HMAC-SHA256 ■ PRF-HMAC-SHA384
Lifetime	Set the lifetime of the IKE security association in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds.

5. In **IKEv2 IPSec Dynamic Maps**, click an existing dynamic map to edit it or click **+** to open the **Add IKEv2 Dynamic Map** section. Configure the required parameters as described in Table 262.

Table 262: *IKEv2 Dynamic IPsec Map Parameters*

Parameter	Description
Priority	Set the priority level for the IPsec map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next highest-priority map until a match is found.
Name	Enter a name for the dynamic map.
Dynamic map	Select the check box to enable the dynamic map. This is enabled by default.
PFS group	(Optional) Configure PFS settings for the dynamic peer by assigning a Diffie-Hellman prime modulus group. PFS group provides an additional level of security by ensuring that the IPsec SA key was not derived from any other key, and therefore, cannot be compromised if another key is broken. Select one of the following groups: ■ Group 1: 768-bit Diffie–Hellman prime modulus group ■ Group 2: 1024-bit Diffie–Hellman prime modulus group ■ Group 14: 2048-bit Diffie–Hellman prime modulus group ■ Group 19: 256-bit random Diffie–Hellman ECP modulus group ■ Group 20: 384-bit random Diffie–Hellman ECP modulus group
Transforms	Click **+** to open the **New Transform** section. 1. To add an existing transform, select **Add existing transform** 2. Select a transform from the list and save the changes. 3. To add a new transform, select **Add new transform**. 4. From the **Encryption** drop-down list, select one of the following encryption types: ■ DES ■ 3DES ■ AES128 ■ AES192 ■ AES256 5. From the **Hash** algorithm drop-down list, select one of the following hash types: ■ MD5

Table 262: *IKEv2 Dynamic IPsec Map Parameters*

Parameter	Description
	■ SHA ■ SHA1-96 ■ SHA2-256-128 ■ SHA2-384-192 6. Click **Save Settings**.
Lifetime(seconds)	Set the lifetime of the security association for the dynamic peer in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds.
Lifetime(kilobytes)	Set the lifetime of the security association for the dynamic peer in kilobytes.

6. Save the changes.

Routing

Aruba's SD-Branch solution leverages WAN services that interconnect hub and spoke sites to establish VPN tunnels, which encapsulate and forward corporate traffic. Each WAN service is referred to as the underlay network, while the VPN tunnels form the overlay network.

The Branch Gateway and VPNC in an SD-Branch network must have IPv4 routes to determine how each device must reach Aruba Central and its VPN peers over any intermediate public or private IPv4 networks (underlay routes). Routes are also required to determine which internal networks must be reached by the Aruba Gateways through the overlay VPN tunnels (overlay routes).

Dynamic Routing

To enable interoperability with other systems in the network and provide flexible routing options, the Aruba SD-Branch solution supports the following dynamic routing protocols:

- BGP—The BGP routing protocol allows exchanging routing information between the peers within or between autonomous systems to determine the optimal paths for traffic flows. Network administrators can configure Aruba Gateways to advertise routes to an upstream router in the MPLS provider network. For more information, see Advertising Routes Using BGP.
- OSPF—OSPF is a link state routing protocol that routes traffic information by sending Link-State Advertisements (LSAs) to all other routers within a specific area. Depending on the deployment architecture, network administrators can either implement static routes or leverage dynamic routing through OSPF. Small deployments with single VPNC hub site can implement static routes, while larger deployments with multiple VPNC hub sites can be configured to use OSPF. For more information, see Routes Advertisement Using OSPF.

Underlay Routing

For establishing VPN tunnels, the VLAN interfaces on the Branch Gateways and VPNCs must be reachable over each WAN service. To provide IP reachability through each WAN service, a combination of default gateways and static routes are required.

Based on the type of WAN service, you can configure different types of routes:

- Internet WAN Services—Requires default gateways to be defined on both Branch Gateways and VPNCs. The default routes are manually configured on VPNCs and dynamically learned by Branch Gateways from the ISP through DHCP or PPPoE.
- MPLS/Private WAN Services—Requires static default routes on Branch Gateways and static routes on VPNCs. These routes must be manually configured Branch Gateways and VPNCs. A default gateway is required on each Branch Gateway for MPLS networks. The default gateway must be defined with a cost of 15 or higher.

For deployments with multiple Internet WAN services, Branch Gateways load-balance or steer sessions out of the respective Internet WAN uplinks based on the configured DPS and PBR policies. VPNCs typically implement a single default route and leverage the stateful packet inspection firewall to tag each VPN tunnel to the correct VLAN interface.

Overlay Routing

To simplify overlay routing and provide scalability, the Aruba Gateways support a combination of dynamic and static route configuration:

- Branch Gateways can be configured with static routes to determine that the destination networks are reachable through the VPN tunnels. One static route is defined per VPNC peer for each WAN uplink.
- Branch Gateways can be configured to advertise internal LAN networks to each L2 active VPNC peer using Aruba IKEv2 extensions. Each advertised LAN is installed as an IKEv2 route on each L2 active VPNC (one route per active WAN uplink).
- The VPNCs participate in OSPF and BGP, and learn corporate routes from neighboring routers and redistribute IKEv2 overlay routes to the neighboring OSPF or BGP peers.

After the overlay routing has been configured between Branch Gateways and VPNCs, firewalls in the data center and corporate network will need to know how to reach branch networks that are behind VPNCs.

Routes Configuration on Aruba Gateways

See the following topics for information on how to configure routes:

- Configuring Static IP Routes
- Configuring Static Default Gateways
- Configuring Default Gateways for Dynamic Routing
- Routes Advertisement Using OSPF
- Advertising Routes Using BGP
- Routes Advertisement Using RIPv2
- Advertising Overlay Routes

Configuring Static IP Routes

For overlay routing using static IP routes, ensure that you define static routes for each branch network and data center as follows:

- Define static routes for each branch network on the router in the data center.
- Define static routes for each branch network on the VPNC for each remote network, peer, and link.
- Define static routes for each data center or a hub site for each Branch Gateway.

NOTE

Static routing is not recommended for multiple VPNC hub deployments as additional mechanisms such as IP SLA need to be implemented on routers to provide dynamic failover between primary and secondary hub sites.

Creating a Static IP Route

To configure a static IP route, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **Routing** > **IP Routes**.
7. Under **IP Routes**, click **+** to add a static route to a destination network or host.
8. Enter the IP address and netmask for the **Destination IP address** and **Destination network mask**, respectively.
9. Configure a forwarding setting:
   - **Using Forwarding Router Address**—Enter the next hop IP address in dotted decimal format (A.B.C.D). You can also enter the distance metric (cost) for this route. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.
   - **Using IPsec Tunnel to VPNC**—Select the VPNC and the uplink to use. Select this option for a Hub and Spoke VPN. For more information, see Configuring the SD-Branch Overlay Network.
   - **Using Site-to-Site IPsec**—Enter the IPsec map name to use in a static IPsec route map. Select this option for a site-to-site VPN. For more information, see Configuring Site-to-Site VPN.
   - **Using Null Interface**—Select this option to designate a null interface.
10. Specify a value for the **Cost**.
11. Enter a value for **Distance**. The **Distance** parameter is used for prioritizing routes distributed by various routing protocols. By default, the administrative distance for static routes is set to 1; that is, static routes are prioritized over the routes distributed by dynamic routing protocols such as OSPF or BGP. If a static route has the same administrative distance as a dynamic route, the static routes take precedence. The allowed range of values is 1–255.
12. Click **Save Settings.**

Configuring Static Default Gateways

Static default gateways are required for all deployments implementing Internet based WAN services. The default gateway is statically defined on VPNCs and dynamically derived on the Branch Gateways from the Internet Service Provider (ISP) through DHCP or PPPoE. A static default gateway is also required on Branch Gateways connecting to an MPLS WAN or private WAN services.

Aruba recommends that you configure static default gateways at the device level, because default gateways are typically unique to each Branch Gateway. However, if the devices in a deployment share a common gateway, you can configure default gateways at the group level.

To configure default gateways for routing, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains the VPNC.
2. The dashboard context for a group is displayed.
3. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
4. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.
5. Under **Manage**, Click **Device**.

   The gateway configuration page is displayed.
6. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
7. Click **Routing** > **IP Routes**.
8. Under **Static Default Gateway**, click **+** to add a new default gateway.
9. Select **Ipv4** from the **IP version** drop-down list.
10. To use a default gateway IP, select the **Default Gateway IP** option and enter the default gateway IP address.
11. To use an IPsec map, select the **IPsec Map** option and select the IPsec map.
12. In the **Uplink** field, click the edit icon to open the **Available/Selected Uplinks** window to add or remove available uplinks.
13. Enter a value for **Cost**.
14. Click **Save Settings**.

Configuring Default Gateways for Dynamic Routing

The default gateway is statically defined on VPNCs and dynamically derived on the Branch Gateways from the ISP through DHCP or PPPoE.

The default gateways that are dynamically derived through DHCP, Cellular link, or PPPoE are installed in the route table with a default cost of 10. If a deployment includes Branch Gateways with multiple internet based WAN services that implement both dynamic and static addressing, Aruba recommends that you define static default gateways at a cost equal to the dynamically learned default gateways, so that both default gateways can be installed in the routing table on Branch Gateways.

To configure dynamic default gateways on Branch Gateways:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.

   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **Routing** > **IP Routes**.
7. Expand **Dynamic Default Gateway**.

8. To configure the server type from which Branch Gateways can learn the default gateways, select **DHCP**, **PPPoE**, or **Cellular**.
9. Specify the cost for each server type you selected. The Branch Gateway first tries to obtain a gateway IP address using the option with the least cost. If the Branch Gateway is unable to obtain a gateway IP address, it tries to obtain a gateway IP address using the option with the next lowest path cost.
10. Click **Save Settings**.

Routes Advertisement Using OSPF

Open Shortest Path First (OSPF) is a routing protocol used for distributing routing information to the neighboring layer-3 devices. The OSPF configuration allows advertising branch networks into an OSPF area and also enables VPNCs to learn corporate routes. OSPF simplifies routing, allows dynamic exchange of branch and corporate routes between VPNCs, and also provides the ability to support failover to an available VPN hub site. Therefore, Aruba recommends that you use OSPF for routing in large SD-Branch deployments with multiple VPN hub sites.

OSPF Areas

OSPF operates within a single Autonomous System. An autonomous system consists of a network, or a group of networks with a common administrative entity and routing policies. In OSPF deployments, a single Autonomous System can be divided into smaller groups called areas. An OSPF area typically includes a set of networks and hosts grouped together under a common subnet. Distributing routes using OSPF areas reduces the number of link-state advertisements (LSA) and the size of the link state database that each router must maintain.

Aruba Gateways support advertising routes in the following OSPF areas:

- Normal Area—Allows advertising all routes to all the routers within the area.
- Stub Area—Allows routers to advertise only the default route.
- Not-So-Stubby Area (NSSA)—Allows external routes from the routing devices that belong to more than one OSPF area; for example, Area Border Router (ABR).

Most deployments connect VPNCs to normal OSPF areas either behind routers or firewalls in the data center.

Best Practices for OSPF Configuration

Consider the following recommendations before configuring and enabling OSPF on VPNCs:

- You can use the loopback interface, any VLAN interface, or the Gateway Pool address as the system IP address of the VPNC, and also use it as the OSPF router ID. For more information on configuring system IP address and loopback address, see Configuring System IP Address.
- Ensure that the VPNC is not elected as a designated router in an OSPF area.
- If using IKEv2 overlay routes for redistribution, configure VPNC to redistribute IKEv2 overlay routes at a specific cost. Ensure that the VPNCs at the primary hub site are configured to redistribute IKEv2 overlay routes at a lower cost than the VPNCs at the secondary hub site.

Workflow for Configuring OSPF Routing

You can configure OSPF on Branch Gateway device, Branch Gateway group, VPNC device and VPNC group.

Complete the following steps to configure OSPF:

- Enabling OSPF
- Configuring Route Maps
- Configuring Prefix List
- Configuring Route Redistribution Criteria
- Enabling OSPF on VLAN Interfaces
- Enabling OSPF on Layer-3 GRE Tunnel Interface
- Configuring Administrative Distance

To view, monitor, and troubleshoot OSPF routing configurations, see the following pages:

- Viewing Configuration Status
- Monitoring Routes
- Troubleshooting

Enabling OSPF

You can enable OSPF in the group or device dashboards for the Branch Gateway and VPNC.

To enable OSPF configuration, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **OSPF**.The **OSPF** page opens.
4. Under **General**, turn on the **Enable OSPF** toggle switch.
5. To enable distribution of default information, select the **Default Information** check box.
6. For Area ID, enter the configured router ID. Ensure that the router ID is the same as the IPv4 address assigned to the loopback interface on the VPNC.
7. Under **Area**, click **+** to add an OSPF area.
8. Select any of following area types:

- **Normal**—To enable advertising of routes to all the routers in a backbone or regular area within an Autonomous System.
- **Stub**—To advertise only the default routes. Stub areas do not propagate external routes and replace external routes with the default routes. For Stub area, you can configure the default cost and also disable or enable the link state advertisement.
- **NSSA**—To allow external routes from the routing devices that belong to more than one OSPF area; for example, ABRs. For NSSA area, you can configure the default cost and enable distribution of the default information. If required, you can also disable redistribution and link state summarization.

9. Click **Save Settings**.

Configuring a Prefix List

You can configure the **Prefix List** in the group and device dashboards for the Branch Gateway and VPNC.

A prefix list allows routing systems to determine which routes must be accepted when they peer with other networks. A prefix list includes IP prefixes with a match criteria that allows or denies route redistribution. Prefix lists contain one or more ordered entries which are processed sequentially.

Prefix lists can be used as a match criteria for applying route map rules on network subnets. For example, if you want to prevent a route for 10.0.0.0/24 from being redistributed, you can define a rule to match the prefix and add it a as match criterion in the OSPF redistribution route map. For more information, see Configuring Route Maps.

To create a prefix list, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **OSPF**.
4. Click the **+** icon in the **Prefix Rules** table.
5. Enter a name for the prefix rule.

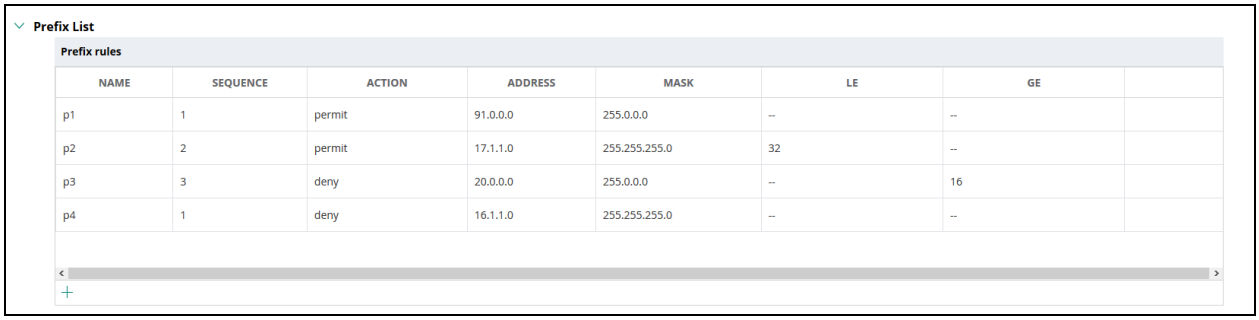
6. Enter a sequence number.
7. Define the action to perform when the traffic matches the condition defined in the prefix rule.
8. Enter a network address to which you want to apply the prefix rule.
9. Enter the subnet mask of the network.
10. If you want to define a prefix length parameter and use it as a match criteria for applying rules, enter an appropriate value for the optional **LE** and **GE** operators. The allowed range of values is 1–32.

    If the **LE** parameter is configured, the prefix rules are applied only if the subnets are equal to or smaller than the value specified for LE. Similarly, if the **GE** parameter is configured, the prefix rules are applied only if the subnets are equal to or greater than the value specified for GE. If either **LE** or **GE** parameter is not configured, the prefix rule is applied only to those subnets that match the exact address or subnet mask configured in the rule.
11. Click **Save Settings**.

Example of a Prefix List

The following figure shows the prefix list configured for a VPNC in Aruba Central:

Figure 222 *OSPF Prefix List*



In the above example, the following prefix entries are processed sequentially based on the sequence number configured for each entry.

- The **p1** prefix list entry permits advertising the exact prefix 91.0.0.0/8 by allowing 91.0.0.0 with the subnet mask of 255.0.0.0.
- The **p4** prefix list entry prevents the exact prefix 16.1.1.0/24 from being advertised by denying 16.1.1.0 with the subnet mask of 255.255.255.0.
- The **p2** prefix list entry permits advertising the exact prefix 17.1.1.0/24 and all other prefixes within the length of 32 bits. The LE parameter in the prefix list defines maximum prefix length for rule application.
- The **p3** prefix list prevents all prefixes within 20.1.0.0/8 that are at least 16 bits in length from being advertised. The GE parameter in the prefix list defines the minimum prefix length for rule application.

Configuring OSPF Route Maps

You can configure the **OSPF Route Maps** in the group and device dashboards for the Branch Gateway and VPNC.

Route maps allow you to configure a filtering criteria by defining a set of rules or match statements with a permit or deny condition. A route map includes a series of match statements to determine if a route matches the criteria defined in the statement and then applies the permit or deny rule accordingly. You can also configure an additional set of parameters to adjust the attributes and metrics for routes that match the criteria defined in the match statement.

The following list includes some of the important points to consider when configuring a route map:

- A route map includes name, sequence number, permit or deny rule, the match and set statements. The match statements determine the route or the traffic to which the rule must be applied, whereas the set statements allow you configure attributes or adjust metrics for the route that matches the criteria defined in the match statement.
- The route map rules are applied sequentially; that is, based on the sequence number defined for each entry.
- The route map can use a prefix list in the match statement to apply the allow or deny rule. For more information on prefix lists, see Configuring a Prefix List.

Creating a Routing Map

To create a routing map, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **OSPF.**
4. To add a route map, click the **+** icon in the **Route Maps** table. The **Create New Route Map** panel is displayed.
5. Configure the following parameters as per your network requirements:

Table 263: *Route Map Configuration Parameters*

Parameter	Description
Name	Enter a name for the route map.
Sequence Number	Enter a sequence number for the route map. Sequence numbers allow route maps to be processed in an order. If you are configuring multiple match clauses or statements, ensure that you define a sequence number to uniquely identify each match statement.

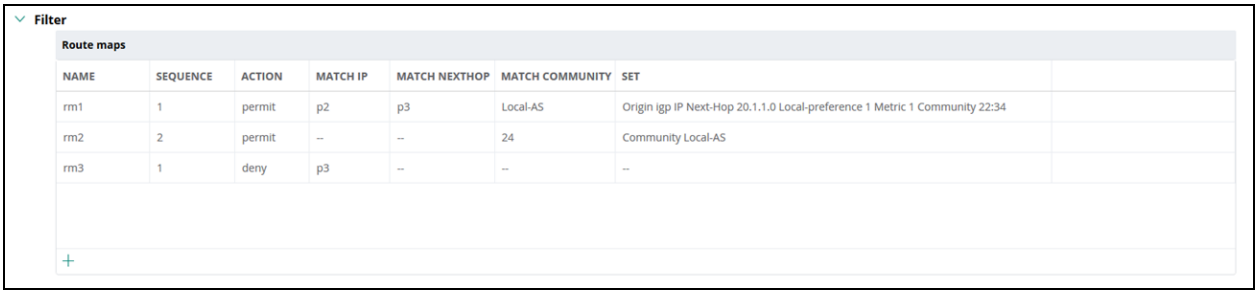
Parameter	Description
Action	Configure an allow or deny rule for the match condition.
Match	Configure the match condition for the routes that have a destination network. The match statements define a set of conditions for determining if the route redistribution must be allowed or denied. To add a match statement, click the **+** icon in the **Match** table. You can set match type to any of the options listes here: ■ **IP address**—If you have selected the **IP address** for match type, you can assign a prefix list to a match statement. The match condition determines if the route advertisements from the OSPF neighbor with the prefixes must be allowed or denied. ■ **Next-hop IP address**—If you have selected the **Next-hop IP** address for match type, you can assign a prefix list to a match statement. The match condition determines if the route advertisements from the OSPF neighbor with the prefixes must be allowed or denied. ■ **Community**—**Community** is applicable only for BGP routes. ■ **Interface VLAN**—If you have selected **Interface VLAN** for match type, enter the interface VLANS separated by comma. You can enter up to 10 Interface VLANs. The value you enter must be between 1 to 4095. To know how to configure VLANs, see Configuring VLANs on Aruba Gateways. ■ **OSPF route tag**—If you have selected **OSPF route tag** for match type, a match tag condition is added. You need to enter the tag names separated by comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.
Set	Configure a set of rules or attributes to apply to the OSPF traffic that matches the conditions defined in a match statement. To add a set attribute, click the **+** icon in the **Set** table and configure the following attributes as per your requirement: ■ **as-path-prepend**—Prepends AS numbers through which the packets have traversed. You can apply the AS path prepending criteria to determine the best path. ◦ **AS number**— Enter any valid Autonomous System (AS) number between 1 to 65535. ■ **last-as**—Prepends the last AS number to the AS path. The valid range of values is 1–10. ■ **Community** is applicable only for BGP routes. ■ **ip next-hop**—Sets a next-hop IPv4 address as an attribute in the routes. ■ **local-preference**—Sets a preference value to the routes for determining the best AS path. When the neighboring device receives multiple routes to the same destination network, the route with the highest local preference value takes precedence. The valid range of values for local preference is 0–4294967295. ■ **metric**—Sets a metric value for determining the preferred path into an Autonomous System. You can define a metric value between 0—4294967295. When a metric value in a route matches this value, the route is advertised. ■ **origin**—Sets the origin of the route. The following options are available: ◦ **incomplete**(EGP)—To specify that the route is originated from exterior routing protocol. ◦ **igp**—To specify that the route is originated from interior routing protocol. ■ **OSPF route tag**—Sets the tag attribute of the route. ■ **OSPF route-type**—Sets the external metric (E1 or E2) attribute of the route.

6. Click **Save Settings**.

Example of an OSPF Route Map

The following figure shows the route maps configured for OSPF routes in Aruba Central:

Figure 223 *OSPF Route Maps*



Configuring OSPF Route Redistribution

You can configure the **OSPF Route Redistribution** in the group and device dashboards for the Branch Gateway and VPNC in **Advanced Mode**.

Redistribution rules allow you to enable advertising of routing information from the connected, static, OSPF, and BGP interfaces into overlay routing. Routing information from other sources is not automatically redistributed into overlay routing, but need to be configured for each source protocol locally on each Gateway.

Redistribution criteria can be configured in the following modes:

Configuring Route Redistribution Criteria in Advanced Mode

To configure rules for redistributing routes to OSPF areas, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **OSPF**.
4. Click **Redistribution**.
5. To add a redistribution rule, click **+** under the **Redistribution Rules** table and configure the following parameters:
   a. From the **Source Protocol** drop-down, select a source type:
      - **Static**—To redistribute IP static routes.
      - **IKE Overlay**—To redistribute branch routes advertised by the Branch Gateways after establishing an IPsec tunnel with the VPNC at the hub site. By default, the VPNCs redistribute the IKEv2 overlay routes learnt from Branch Gateways irrespective of the route summarization status. Optionally, you can enable route summarization for IKE overlay routes on the VPNCs to avoid LSA flooding within an OSPF area.
      - **IAP-VPN Overlay**—To redistribute routes that were received from deployments with Instant APs.
      - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site.
      - **SD-WAN Overlay**—To redistribute routes learnt from the SD-WAN overlay network through the Overlay Agent Protocol.
   b. From the **Route Type** drop-down, select an OSPF route type. Aruba Gateways support propagating OSPF routes as External Type 1 (E1) and External Type 2 (E2) routes.
      - **E1**—The External Type 1 applies both external cost to the destination and the cost to reach the boundary router in an Autonomous System.
      - **E2**—The External Type 2 type applies only the external cost to the destination.
   c. Enter an appropriate value for **Cost**.
   d. Optionally, you can select a **Route Map** to associate to the routes.
   e. Click **Save Settings**.
6. To summarize overlay routes before advertising, click the **+** icon in **Overlay route summary table** and configure the following information:
   a. **Source Protocol**—Select the source protocol of the overlay routes that you want to summarize.
   b. **Network**—Enter the network IP address. For IKE overlay routes, ensure that the configured IP address range includes all networks assigned to LAN VLAN interfaces of Branch Gateways.
   c. **Netmask** —Enter the subnet mask.
   d. **Cost**—Specify the cost.
   e. Click **Save Settings**.
7. To exclude a subnet:
   a. Click the **+** icon in the **Excluded Subnet** table.
   b. Add the subnet and netmask.
   c. Click **Save Settings**.

Enabling OSPF Configuration on VLAN Interfaces

You can enable the **OSPF configuration on VLAN Interfaces** in the group or device dashboards for a Branch Gatewayand VPNC.

To enable OSPF configuration for a VLAN interface, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **OSPF**. Then, click **Interface Settings**.
4. Click the **+** icon in the VLAN table.
5. Select the **VLAN ID**.
6. Enter the IP address of the OSPF area.
7. If you want to authenticate OSPF neighbors for secure exchange of routing information, turn on the **Authentication** toggle switch. By default, MD5 authentication method is used.
8. Enter the **Message Digest key**.
9. Enter the password and retype to confirm.
10. Configure the following parameters as per your deployment requirements:
    - **Cost**—Cost for the OSPF routes. By default, the cost value is set to 1.
    - **Dead Interval**—Dead time interval to enable devices to determine if a participating router is dead. If the hello packets are not received by a neighboring router for a given duration, the router is declared as dead after the dead time interval is elapsed. The default dead time interval is 40 seconds.
    - **Hello Interval**—Timer for exchanging hello packets on the VLAN interface. The default value is 10 seconds.
    - **Priority**—Number indicating a priority level for routes transmitted from the interface. The default value is 1.
    - **Retransmit Interval**—Timer for retransmitting LSAs. The default value is 5 seconds.
    - **Transmit Delay**—Delay interval for retransmission of LSAs. The default value is 1.
11. Click **Save Settings**.

Enabling OSPF on Layer-3 GRE Tunnel Interface

Aruba SD-Branch supports site-to-site VPN tunnel configuration for interoperability with third-party VPNCs at the data center. For site-to-site tunnel configuration, you can enable OSPF on the Layer-3 GRE tunnel interface, so that the OSPF packets exchanged between the branch devices and the VPNC are encapsulated using GRE before entering the IPsec tunnels.

To enable OSPF on the Layer-3 GRE tunnel interface, complete the following steps:

1. To configure a layer 3 GRE tunnel on a Branch Gateway group or a Branch Gateway, complete either one of these steps:
2. Go to **Interface** > **GRE Tunnel**. Select a GRE tunnel. If there are no GRE tunnels configured, add a new GRE tunnel.
3. Click **+** from the **GRE Tunnel** table to add a GRE tunnel. The **Add GRE Tunnel** section is displayed.
4. Ensure that the tunnel mode is set to **L3**.
5. Turn on the **Enable OSPF** toggle switch and configure the following parameters:
   - **Area network (eg. 0.0.0.0)**—Enter the IP address of the OSPF area.
   - **Authentication**—If you want to authenticate OSPF neighbors for secure exchange of routing information, turn on the **Authentication** toggle switch. By default, the MD5 authentication method is used. Enter the **Message Digest key** and password.
   - **Cost**—Enter a value for cost. By default, the cost value is set to 1.
   - **Dead Interval**—Enter a dead time interval to enable devices to determine if a participating router is dead. If the hello packets are not received by a neighboring router for a given duration, the router is declared as dead after the dead time interval is elapsed. The default dead time interval is 40 seconds.
   - **Hello Interval**—Specify the interval for exchanging hello packets with the neighboring devices. The default value is 10 seconds.
   - **Priority**—Specify a number to indicate a priority level for the routes transmitted from the tunnel interface. The default value is 1.
   - **Retransmit Interval**—Specify a time interval for retransmitting LSAs. The default value is 5 seconds.
   - **Transmit Delay**—Specify a delay interval for retransmitting LSAs. The default value is 1.
6. Click **Save Settings**.

Configuring OSPF Administrative Distance

You can configure the **OSPF Administrative Distance** in the group or device dashboards for the Branch Gateway and VPNC.

Administrative distance is one of the main criterion to determine a preferred route when there are multiple paths to the same destination. The route with the a lower administrative distance takes precedence for route redistribution.

To configure administrative distance for OSPF routes, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.

        The dashboard context for the group is displayed.

b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To select a VPNC or a Branch Gateway device in the filter:
  a. Set the filter to **Global**.
  b. Under **Manage**, click **Devices**, and then click **Gateways**.
     A list of gateways is displayed in the **List** view.
  c. Click a gateway listed under **Device Name**.
     The dashboard context for the device is displayed.
  d. Under **Manage**, Click **Device**.
     The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Under **Manage**, click **Device** > **Routing** > **OSPF**.
4. Click **Advanced**.
5. Enter a value for distance within a range of 1–255. By default, the distance is set to 130.
6. Click **Save Settings**.

Viewing OSPF Configuration Status

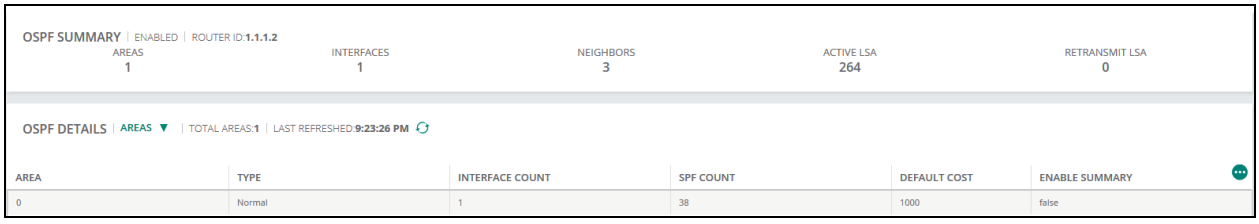
To verify the OSPF configuration and route details, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Overview**. The **Gateway Details** page is displayed.
5. Click **Routing** > **OSPF**. The **OSPF Summary** page is displayed. The OSPF summary page displays the total number of OSPF areas configured on the device,
6. VLAN interfaces on which OSPF is enabled, OSPF neighbors, and active and retransmitted LSAs.

OSPF Areas

To view details of the OSPF areas, select **Areas** in the **OSPF Details** panel.

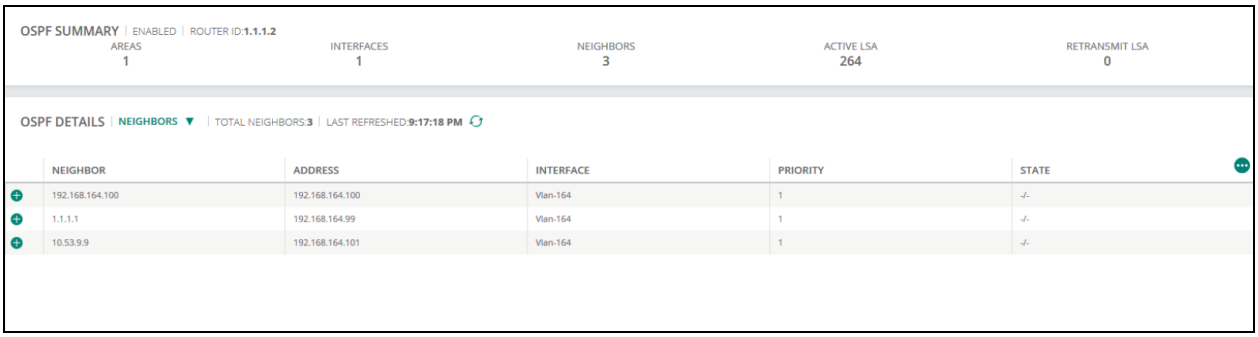
Figure 224 *OSPF Areas view*



OSPF Neighbors

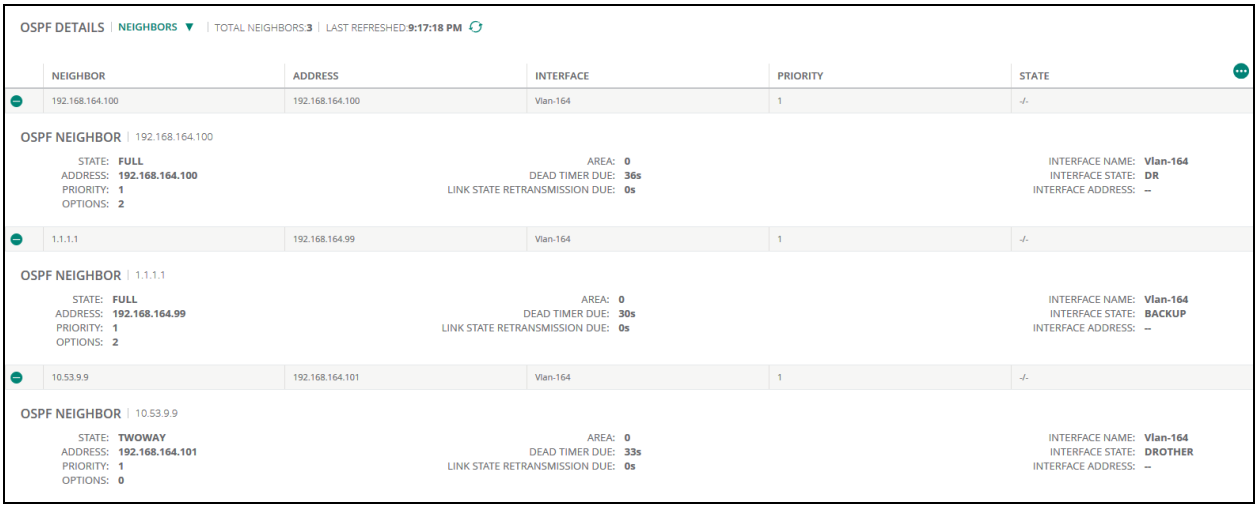
To view a list of OSPF neighbors, click **Neighbors** in the **OSPF Details** panel.

Figure 225 *OSPF Details view*



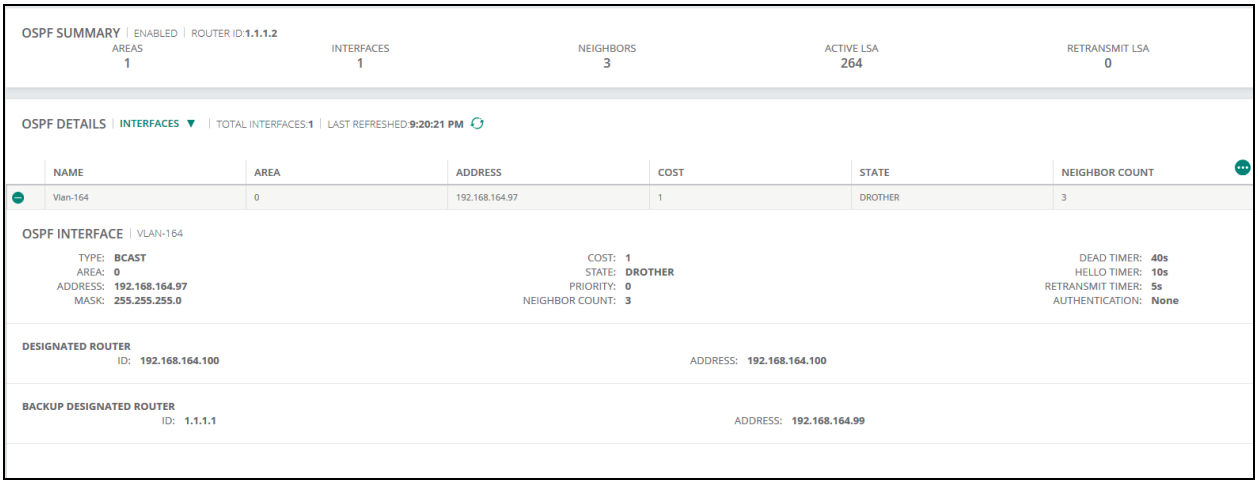
To view more information about the OSPF neighbor, click the neighbor entry in the table.

Figure 226 *OSPF neighbor details view*



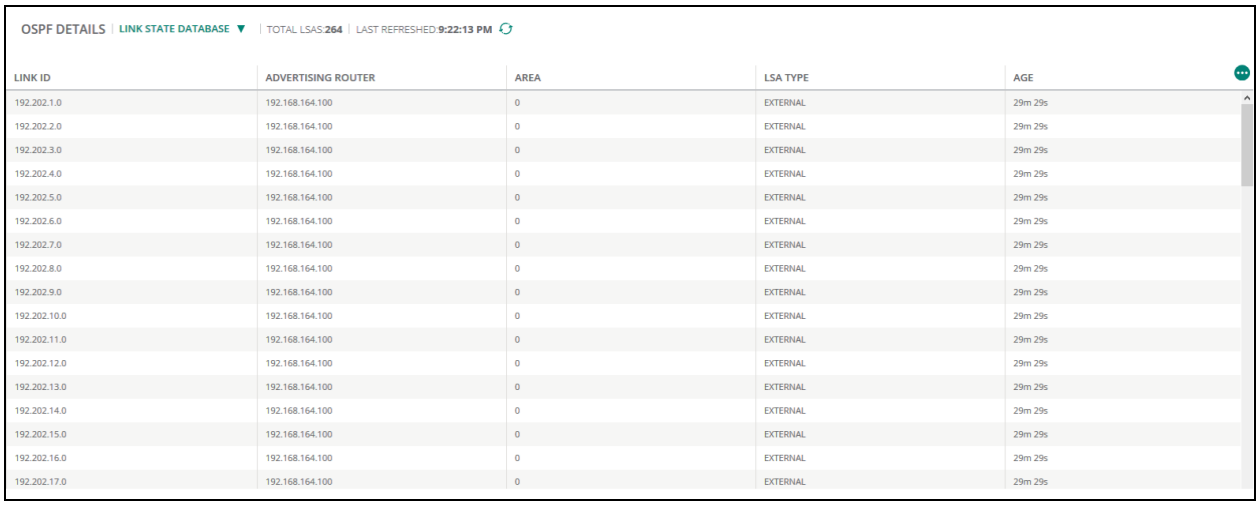
OSPF Interfaces

To view the list of VLAN interfaces on which the OSPF configuration is enabled, click **Interfaces** in the **OSPF Details** panel.



OSPF Link State Database

To view the Link State Database with LSAs transmitted by the Gateway, click **Link State Database** in the **OSPF Details** panel.



Monitoring OSPF Routes

To view the route table, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway that is configured as a VPNC.

   The dashboard context for a group is displayed.

2. Under **Manage**, click **Devices** > **Gateways**.

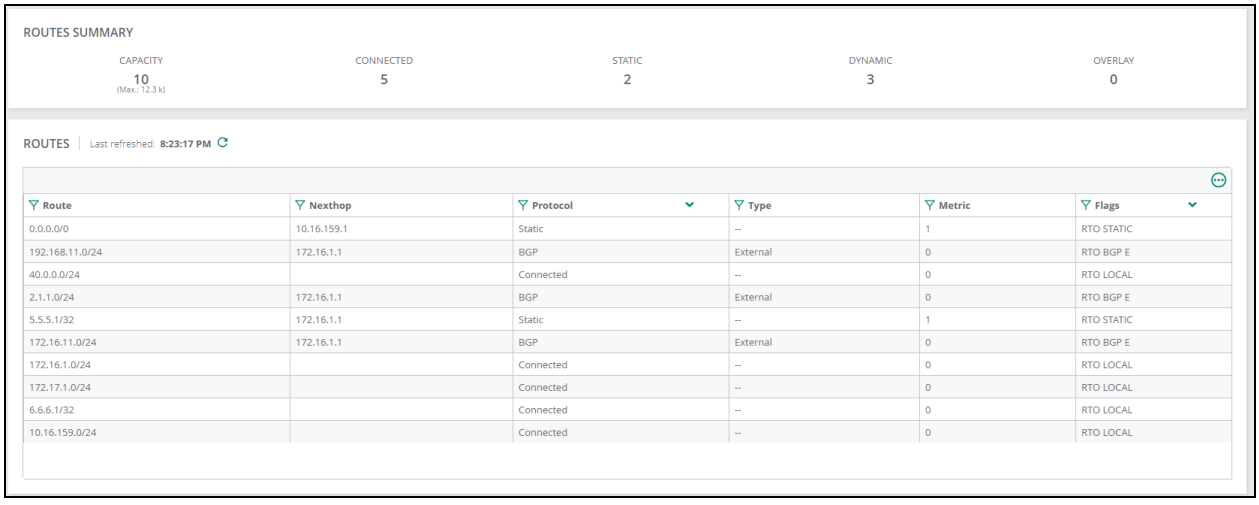
   A list of gateways is displayed in the **List** view.

3. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.

4. Under **Manage**, click **Overview**. The **Gateway Details** page is displayed.
5. In the Gateway monitoring dashboard, click **Routing** > **Route Table**. A list of routes advertised by the Gateway is displayed.
6. Sort the route table by the OSPF protocol to view the OSPF routes.

Figure 227 *Routes Summary*



Troubleshooting OSPF Configuration Issues

To troubleshoot OSPF configuration issues, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.
4. Under **Analyze**, click **Tools**. The **Tools** page for troubleshooting devices is displayed.
5. Click **Commands**.
6. From **Category**, select **Networking**.
7. From the command list, select the OSPF commands that you want to use. For example, **show ip ospf neighbor** and **show ip ospf database**.
8. Click **Run**.
9. Verify the command output and resolve configuration errors if any.
10. Go to the **Gateway Details** page. Verify the configuration status and monitor OSPF routes. If the issue persists, contact Aruba Technical Support.

Advertising Routes Using BGP

To support interoperability with an existing network infrastructure, Aruba SD-Branch solution supports the BGP dynamic routing protocol to enable VPNCs to redistribute overlay routes learned from Branch Gateways into BGP and advertise those routes in the data center network.

BGP is a dynamic routing protocol used for exchanging routing information within and between Autonomous Systems (AS). In a typical deployment, routers are configured to function as BGP peers or neighbors, and exchange routing information after establishing a TCP connection. If BGP is used for routing between two different ASs, it is referred to as eBGP. Similarly, when BGP is used within an AS, it is referred to as iBGP.

When BGP support is enabled, Aruba Gateways function as BGP peers and advertise routes to their iBGP and eBGP neighbors.

The Multipath feature allows you to load balance the traffic across multiple available links. BGP paths with same BGP path selection attributes (weight, local preference, AS Path, Origin code, MED, IGP metric) qualify for multipath next-hops. AS Path could be different, but length should be same.

The SD-WAN Orchestrator carries BGP attributes such as the Origin, AS-Path, Community, Extended Community, and Large Community. Route Maps can be used to set filters and attributes for Overlay BGP Redistributed routes.

The following are the guidelines for configuring BGP for Gateways:

- If BGP routing is required between two different AS, ensure that you configure the neighboring router in the MPLS network and the router at the data center as eBGP peers of Aruba Gateways.
- The loopback interface can be used as the system IP of the VPNC and also as the BGP router ID. Ensure that you configure loopback interface on each VPNC. For more information, see Configuring System Information on Aruba Gateways.

- The minimum software version required for BGP configuration on Aruba Gateways is ArubaOS 8.4.0.0-1.0.5.0.
- There are various parameters to set a route preference. The following list provides a few of the preference criteria for choosing the optimal route:
- Route with the lowest administrative distance (routes with the lowest external distance and internal distance to the boundary router)
- Route with the highest value defined for the local preference attribute
- Route with the lowest metric value (BGP Multiple Exit Discriminator (MED))
- Routes received from eBGP neighbors

Complete the following steps to configure BGP routing on the Gateway devices:

- Enabling BGP
- Configuring a Prefix List
- Configuring an IP Community List
- Configuring Route Maps
- Adding BGP Neighbors
- Advertising Networks to BGP
- Configuring Redistribution Rules for BGP Routes
- Configuring BGP Timers
- Configuring Multipath Selection
- Configuring Graceful Restart
- Configuring Administrative Distance
- Configuring BGP over an IPsec Tunnel

To view, verify, and troubleshoot BGP routing configurations, see the following pages:

- Verifying the BGP Configuration
- Troubleshooting BGP Configuration Issues

Enabling BGP

To enable BGP support on a Branch Gateway or a Branch Gateway group, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.

        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click **Config**.

        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:

a. Set the filter to **Global**.
b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
d. Under **Manage**, Click **Device**.
   The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**.
4. If you want to enable BGP support on all devices provisioned in Aruba Central, click **Enable BGP.**
5. To enable distribution of default information, select the **Default Information** check box. This allows the local BGP peer to advertise the default route 0.0.0.0 to all of its BGP neighbors (both iBGP and eBGP neighbors) for use as a default route.
6. Select the **Route map** that permits advertising the default route to the BGP neighbors from the drop-down list. See Configuring Route Maps.
7. Enter the **Autonomous System** number.
8. Enter the **Router ID**. The router ID is the IPv4 address of Gateway used for identifying it as the router in an AS.
9. Click **Save Settings**.

Configuring a Prefix List

A prefix list allows routing systems to determine which routes must be accepted when they peer with other networks. It includes IP prefixes with a match criteria that allows or denies route redistribution. It contains one or more ordered entries which are processed sequentially.

Prefix lists can be used as a match criteria for applying route map rules on network subnets. For example, if you want to prevent a route for 10.0.0.0/24 from being redistributed, you can define a rule to match the prefix and add it a as match criterion in the BGP redistribution route map. For more information, see Configuring Route Maps.

To create a prefix list:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:

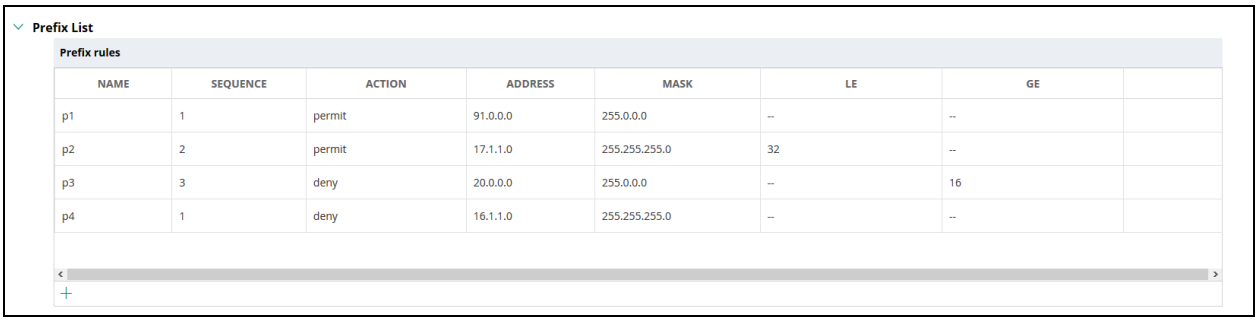
a. Set the filter to **Global**.
b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
d. Under **Manage**, Click **Device**.
   The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**.
4. Click the **+** icon in the **Prefix Rules** table.
5. Enter a name for the prefix rule.
6. Enter a sequence number.
7. Define the action to perform when the traffic matches the condition defined in the prefix rule.
8. Enter a network address to which you want to apply the prefix rule.
9. Enter the subnet mask of the network.
10. If you want to define a prefix length parameter and use it as a match criteria for applying rules, enter an appropriate value for the optional **LE** and **GE** operators. The allowed range of values is 1–32.
    If the **LE** parameter is configured, the prefix rules are applied only if the subnets are equal to or smaller than the value specified for LE. Similarly, if the **GE** parameter is configured, the prefix rules are applied only if the subnets are equal to or greater than the value specified for GE. If either the **LE** or **GE** parameter is not configured, the prefix rule is applied only to those subnets that match the exact address or subnet mask configured in the rule.
11. Click **Save Settings**.

Example of a BGP Prefix List

The following figure shows the prefix list configured for a VPNC in Aruba Central:

Figure 228 *BGP Prefix List*



In the above example, the following prefix entries are processed sequentially based on the sequence number configured for each entry.

- The **p1** prefix list entry permits advertising the exact prefix 91.0.0.0/8 by allowing 91.0.0.0 with the subnet mask of 255.0.0.0.
- The **p4** prefix list entry prevents the exact prefix 16.1.1.0/24 from being advertised by denying 16.1.1.0 with the subnet mask of 255.255.255.0.

- The **p2** prefix list entry permits advertising the exact prefix 17.1.1.0/24 and all other prefixes within the length of 32 bits. The LE parameter in the prefix list defines maximum prefix length for rule application.
- The **p3** prefix list prevents all prefixes within 20.1.0.0/8 that are at least 16 bits in length from being advertised. The GE parameter in the prefix list defines the minimum prefix length for rule application.

Configuring an IP Community List

The IP community list feature allows administrators to configure a set of community attributes to apply on the BGP routes exchanged between Aruba Gateways and their BGP peers. The community attribute allows grouping routes with similar properties and is generally used for tagging routes and modifying BGP routing policies. The IP community list allows you to configure a community or an extended community, or groups of both used for filtering or modifying community values. You can attach a community to a route map, which can in turn be associated to a BGP neighbor profile.

To create a community list:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**.
4. Click **+** in the **Community-list rules** table.
5. Enter a name for the community list.
6. Set a permit or allow rule as per your requirement.
7. If required, select a community value. The following attributes are available:
   - **Internet**—Advertises the prefix to all BGP neighbors.
   - **No-Export**—Does not advertise the prefix to any eBGP neighbor. It advertises the prefix only to iBGP neighbors.
   - **No-Advertise**—Does not advertise the prefix to any peer, iBGP or eBGP neighbor.

- **Local-AS**— Does not advertise the prefix outside of the local AS.

  You can also enter a value for the following types of community strings and click **+** to add.

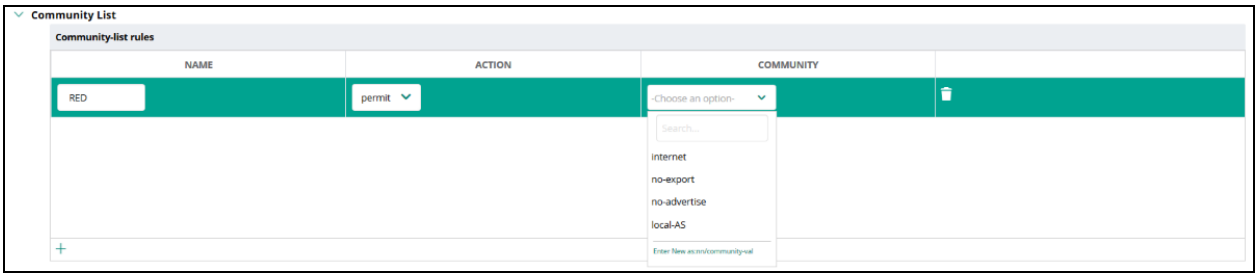
- **as:nn**—The BGP community string in the AS:NN format, where AS refers to the Autonomous System number and NN refers to the network number. The valid range of values is 0-65535.
- **community-val**—The BGP community value string. The valid range of values is 1–4294967295.

  You can specify one or more community values. If the community list has more than one value, the route map matches only those routes that have all the values defined in the list.

8. Click **Save Settings**.

The following figure shows the community list configuration options available on Aruba Gateways:

Figure 229 *BGP Community List*



After you create the community list, associate it to a route map. For more information, see Configuring Route Maps.

Configuring Route Maps

Route maps allow you to configure a filtering criteria by defining a set of rules or match statements with a permit or deny condition. It includes a series of match statements to determine if a route matches the criteria defined in the statement and then apply the permit or deny rule accordingly. You can also configure an additional set of parameters to adjust the attributes and metrics for routes that match the criteria defined in the match statement.

The following list includes some of the important points to consider when configuring a route map:

- A route map includes name, sequence number, permit or deny rule, the match and set statements. The match statements determine the route or the traffic to which the rule must be applied, whereas the set statements allow you configure attributes or adjust metrics for the route that matches the criteria defined in the match statement.
- The route map rules are applied sequentially; that is, based on the sequence number defined for each entry.
- The route map can use a prefix list in the match statement to apply the allow or deny rule. For more information on prefix lists, see Configuring a Prefix List.
- Route maps can be attached to the BGP neighbor profiles for the inbound and outbound routes. You can associate route maps for the inbound and outbound traffic when configuring a BGP neighbor profile. When the route map policy is applied to the inbound or outbound BGP route, and if the traffic matches the specified criteria, the attribute set for the match condition is applied. If you do not have a route map attached to an iBGP neighbor profile, the iBGP neighbor can access all inbound and outbound routes. For more information on BGP neighbor profiles. see Adding BGP Neighbors.

Creating a Route Map

To create a routing map:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**.
4. To add a route map, click the **+** icon in the **Route Maps** table. The **Create New Route Map** panel opens.
5. Configure the following parameters as per your network requirements:

Table 264: *Route Map Configuration Parameters*

Parameter	Description
Name	Enter a name for the route map.
Sequence Number	Enter a sequence number for the route map. Sequence numbers allow route maps to be executed in an order. If you are configuring multiple match clauses or statements, ensure that you define a sequence number to uniquely identify each match statement.
Action	Configure an allow or deny rule for the match condition.
Match	Configure the match conditions for the routes that have a destination network. The match statements define a set of conditions for determining if the route redistribution must be allowed or denied. To add a match statement, click the **+** icon in the **Match** table. You can set match type to one of the following: ■ **IP address** ■ **Next-hop IP** ■ **Interface VLAN—**If you have selected Interface VLAN for match type, enter the interface VLANS separated by comma. You can enter up to 10 Interface VLANs. The value you enter must be between 1 to 4095. To know how to configure VLANs, see Configuring VLANs on Aruba Gateways.

Parameter	Description
	■ **OSPF route tag**—If you have selected OSPF route tag for match type, a match tag condition is added. You need to enter the tag names separated by comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295. ■ **Network segment** ■ **Community** If you have selected the **IP address** or **Next-hop IP** address for match type, you can assign a prefix list to a match statement. The match condition determines if the route advertisements from the BGP neighbor with the prefixes must be allowed or denied. If you have selected **Community** for match type, use one of the following options to define the community string. ■ **as:nn**—The BGP community string in the AS:NN format. The valid range of values is 0-65535. ■ **community-val**—The BGP community Value string. The valid range of values is 1–4294967295. Allows you to specify a community value. ■ **well-known community**—A well-known BGP community. Allows you to configure one of the following options: ◦ **Internet**—Advertises subnets to all BGP neighbors. ◦ **No-Export**—Does not advertise prefix to any eBGP neighbor. ◦ **No-Advertise**—Does not advertise subnets to BGP neighbors. ◦ **Local-AS**—Prevents sending packets outside the local AS. ■ **Community list**—Allows you to select a community list configured on the Gateway. Select **Append** or **Delete**. ◦ **Append**—Appends the selected community list to the existing community attribute of routes matching the route map. ◦ **Delete** —Removes the selected community list from the community attribute of routes matching the route map.
Set	Configure a set of rules or attributes to apply to the BGP traffic that matches the conditions defined in a match statement. To add a set attribute, click the **+** icon in the **Set** table and configure the following attributes as per your requirement: ■ **as-path-prepend**—Prepends AS numbers through which the packets have traversed. You can apply the AS path prepending criteria to the BGP traffic to determine the best path. ◦ **AS number**— Enter any valid AS number between 1 to 65535. ■ **last-as**—Prepends the last AS number to the AS path. The valid range of values is 1–10. ■ **community**—Sets a BGP community string as an attribute in the routes. BGP community strings add additional information to the prefixes advertised to BGP neighbors. You can set one of the following types of community string: ◦ **as:nn**—The BGP community string in the AS:NN format. The valid range of values is 0-65535. ◦ **community-val**—The BGP community Value string. The valid range of values is 1–4294967295. ◦ **well-known community**—A well-known BGP community. You can configure one of the following options: • **Internet**—Advertises subnets to all BGP neighbors.

Parameter	Description
	• **No-Export**—Does not advertise prefix to any eBGP neighbor. • **No-Advertise**—Does not advertise subnets to BGP neighbors. • **Local-AS**—Prevents sending packets outside the local AS. ◦ **Community list**—Allows you to select a community list configured on the Gateway. ■ **ip next-hop**—Sets a next-hop IPv4 address as an attribute in the routes. ■ **local-preference**—Sets a preference value to the routes for determining the best AS path. When the iBGP neighbor receives multiple routes to the same destination network, the route with the highest local preference value takes precedence. The valid range of values for local preference is 0–4294967295. Local preference configuration is recommended only for iBGP neighbors. ■ **metric**—Sets a metric value for determining the preferred path into an AS. You can define a metric value between 0—4294967295. When a metric value in a route matches this value, the route is advertised. Metric configuration is recommended only for eBGP peers. ■ **origin**—Sets the origin of the route. The following options are available: ◦ **Incomplete**(EGP)—To specify that the route is originated from exterior routing protocol. ◦ **IGP**—To specify that the route is originated from interior routing protocol. ■ **OSPF route tag**—Sets the tag attribute of the route. ■ **OSPF route-type**—Sets the external metric (E1 or E2) attribute of the route.

6. Click **Save Settings**.

Configuration Example

The following figure shows the route maps configured for BGP routes in Aruba Central:

Figure 230 *BGP Route Maps*

Adding BGP Neighbors

To add a BGP neighbor profile for the Branch Gateway or a Group, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.

        The dashboard context for the group is displayed.

b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To select a VPNC or a Branch Gateway device in the filter:
  a. Set the filter to **Global**.
  b. Under **Manage**, click **Devices**, and then click **Gateways**.
     A list of gateways is displayed in the **List** view.
  c. Click a gateway listed under **Device Name**.
     The dashboard context for the device is displayed.
  d. Under **Manage**, Click **Device**.
     The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**.
4. Click the **+** icon in the **Neighbors** table.
5. In the **Create New Neighbor panel**, configure the following parameters:
   - **Neighbor IP Address**—Enter the IPv4 address of the peer router.
   - **Local Address**—Select a VLAN. Ensure that the selected VLAN has a valid IP address assigned.
   - **Remote-AS**—Enter the number of the AS to which the peer router belongs.
   - **Multi-hop**—Select this check box if you want the gateway to route packets to its remote BGP peer that is more than one hop away.
   - **Route Map In** and **Route Map Out**—If you have created route maps for filtering inbound and outbound BGP routes, select a route map. Ensure that the same route maps are not used for inbound and outbound BGP routes.
   - **Allow AS in**—If you are configuring an eBGP peer, select this check box to allow seamless exchange of routing information between two branches that have the same AS number.

     For example, in some deployments, two branch routers at different locations that are configured as eBGP peers may share the same AS number. When the branch routes are exchanged between these routers, the packets may get dropped by default, as they share the sameAS number. When the allow AS in option is enabled, eBGP peers can exchange the routing information.
   - **Next hop self**—Select this check box to enable an iBGP peer to use an external eBGP peer as the next hop when routing packets to an external source. The BGP route messages include the next-hop information so that a router can forward packets to a particular destination. The **next hop self** configuration is required when an iBGP peer of a router has an eBGP peer.

     For example, Router1 is an iBGP peer for Router2, which in turn is an eBGP peer for another router (Router3) in a remote AS. When the Router2 advertises a route learned from Router3 to Router1 through iBGP, it will use the original next hop address. As Router1 is an iBGP peer, it will not have the route for the next hop. When the **next hop self** feature is enabled on Router2, it will set next hop address to the one (usually, the loopback address of the Router3) that the Router1 (iBGP peer) can reach.
   - **Passphrase** and **Retype Passphrase**—If you want to enable MD5 authentication in BGP neighbor profiles, assign a passphrase. Ensure that the passphrase length is within the 1–16 range. When BGP MD5 authentication is enabled, any TCP segment belonging to BGP that is

exchanged between the peers is verified and accepted only if the authentication is successful. For authentication to be successful, peer devices must have the same password in their respective BGP profiles. If authentication fails, the BGP peers cannot exchange or advertise routes to each other.

- **Max-prefix limit**—You can configure a prefix limit to take action on the BGP prefixes when the number of prefixes exceeds the configured value. The default value is zero. When the number of prefixes exceeds the limit, you can configure the action to be taken as **Drop** or **Warning**. The default action is **None**. If you select **Drop**, the BGP prefixes from the neighbor are dropped; if you select **Warning**, a warning message is displayed in the monitoring dashboard while the gateway continues to receive prefixes. When the number of prefixes exceeds the route limit, an alert is generated and displayed in the gateway monitoring dashboard irrespective of the action configured. The alert is cleared when the number of prefixes falls below the configured limit.
- Click **Save Settings**.

Advertising Networks to BGP

To advertise a network to BGP, you must configure a network statement with the network address and subnet mask details. To configure a network statement:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**.
4. To add a network, click **+** in the **Advertise Network** table.
5. Enter the network IP address and subnet mask.
6. Click **Save Settings**.

Aggregating Routes

For dynamic route summarization and faster calculation of best routing paths, you can configure a route aggregation criteria. The route aggregation feature summarizes multiple routes into a single route

advertisement, and thus helps in reducing the number of routing tables exchanged between BGP peers.

From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch gateways advertise an aggregate route only when there are any summarized routes in the BGP routing table.

To configure a route aggregation criteria on the Branch Gateway or a Group, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**.
4. Then, click **Advertise Networks**.
5. Under **Aggregate Routes**, configure the following parameters:
   - **Address**—Enter a network IP address.
   - **Mask**—Enter the subnet mask.
   - **Route Map**—Select a route map. This route map can be used only to set attributes of the aggregate route. For more information on route maps, see Configuring Route Maps.
6. Click **Save Settings**.

Configuring Redistribution Rules for BGP Routes

To configure redistribution rules for the Branch Gateway or a Group, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.

b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To select a VPNC or a Branch Gateway device in the filter:
  a. Set the filter to **Global**.
  b. Under **Manage**, click **Devices**, and then click **Gateways**.
     A list of gateways is displayed in the **List** view.
  c. Click a gateway listed under **Device Name**.
     The dashboard context for the device is displayed.
  d. Under **Manage**, Click **Device**.
     The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**. Then, click **Redistribute**.
4. To add a network, click the **+** icon in the **Redistribution Rules** table.
5. From the **Source Protocol** drop-down, select the type of routes to redistribute:
   - **Static**—To redistribute the static routes manually configured on Branch Gateways.
   - **OSPF**—To redistribute the routes learnt from an OSPF neighbor.
   - **IKE Overlay**—To redistribute branch routes advertised by Branch Gateways after establishing an IPsec tunnel with the VPNC at the site. By default, the VPNCs redistribute the IKEv2 overlay routes learnt from Branch Gateways irrespective of the route summarization status.
   - **IAP-VPN**—To redistribute routes that were received from micro-branch deployments with Instant AP
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site.s.
   - **SD-WAN Overlay**—To redistribute routes learnt from the SD-WAN overlay network through the Overlay Agent Protocol.

From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch gateways are capable of redistributing a route to null into BGP.

6. Optionally, you can select a route map to associate to the routes.
7. Click **Save Settings**.

Configuring BGP Timers

To configure BGP timers on Gateways, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.

b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To select a VPNC or a Branch Gateway device in the filter:
  a. Set the filter to **Global**.
  b. Under **Manage**, click **Devices**, and then click **Gateways**.
     A list of gateways is displayed in the **List** view.
  c. Click a gateway listed under **Device Name**.
     The dashboard context for the device is displayed.
  d. Under **Manage**, Click **Device**.
     The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**. Then, click **Advanced**.
4. Define the time interval in seconds for the following BGP timers:
   - **Keepalive Timer**—Allows you to set an interval for keeping a BGP session functional. The keepalive timer enables BGP peers to exchange keepalive messages at the specified interval in order to determine if a link is available. The allowed range of values is between 0 to 65535. By default, the keepalive interval is set to 30 seconds.
   - **Hold Timer**—Allows you to configure a duration for which Gateways can wait for a keepalive message from its BGP peers. When Gateways do not receive a keepalive message within the specified hold time, they stop advertising routes to the peer device and reset the routing session. The allowed range of values is between 0 to 65535. By default, the hold time is set to 90 seconds.

Configuring Multipath Selection

Enabling multipath allows you to load balance the traffic across multiple available links. When there are multiple paths with the same BGP path-selection attributes such as the origin code, MED, IGP metric, AS path and so on, they are considered for mutipath nexthops.

To configure Multipath Selection on Gateways, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:

a. Set the filter to **Global**.
b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
d. Under **Manage**, Click **Device**.
   The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**> **Advanced**.
4. Select **Enable multipath**. Multipath is disabled by default.

This feature is currently available only for links within the same AS, that is between iBGP peers.

Configuring Graceful Restart

Graceful restart allows a device with a pending restart to inform the neighbors of the restart condition. While undergoing a graceful restart, the device neighbors continue to forward packets without disrupting network performance.

To configure Graceful Restart on Gateways, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**. Then, click **Advanced**.
4. Select **Enable graceful restart**. Enabling graceful restart on the gateway device allows it to communicate the status to its neighboring devices . Graceful restart is disabled by default.

5. Set the **Graceful restart timer**. You can set the timer between 1 and 4095 seconds. By default, it is set to 120 seconds. The BGP routes are active during the graceful restart period.

Configuring Administrative Distance

Administrative distance is one of the main criteria to determine a preferred route when there are multiple paths to the same destination. The route with the lower administrative distance takes precedence for route redistribution.

To configure administrative distance, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **BGP**. Then, click **Advanced**.
4. Define a route preference value for **External distance** (eBGP) and **Internal distance** (iBGP) routing within a range of 1–255.
   By default, the external distance is set to 110 and internal distance is set to 160 on Aruba Gateways.
5. Click **Save Settings**.

Configuring BGP over an IPsec Tunnel

To enable BGP routing over an IPsec tunnel:

1. Configure a site-to-site tunnel between the devices that you want to configure as BGP peers.
2. Ensure that an IPsec tunnel is established between the devices.
3. Configure a BGP neighbor profile for eBGP peer on both devices and ensure that the **Multihop** option is enabled in the BGP neighbor profile.
4. Configure a static IP route on Gateway to allow it to reach the neighbor device with next-hop using the IPSec map.

5. Ensure that similar steps are configured on both eBGP peers.
6. Verify that the BGP peers are exchanging routes over the tunnel interface.

Verifying the BGP Configuration

To verify the BGP configuration and monitor BGP routes:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one Branch Gateway.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the List view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **BGP**.

   The BGP monitoring dashboard is displayed.

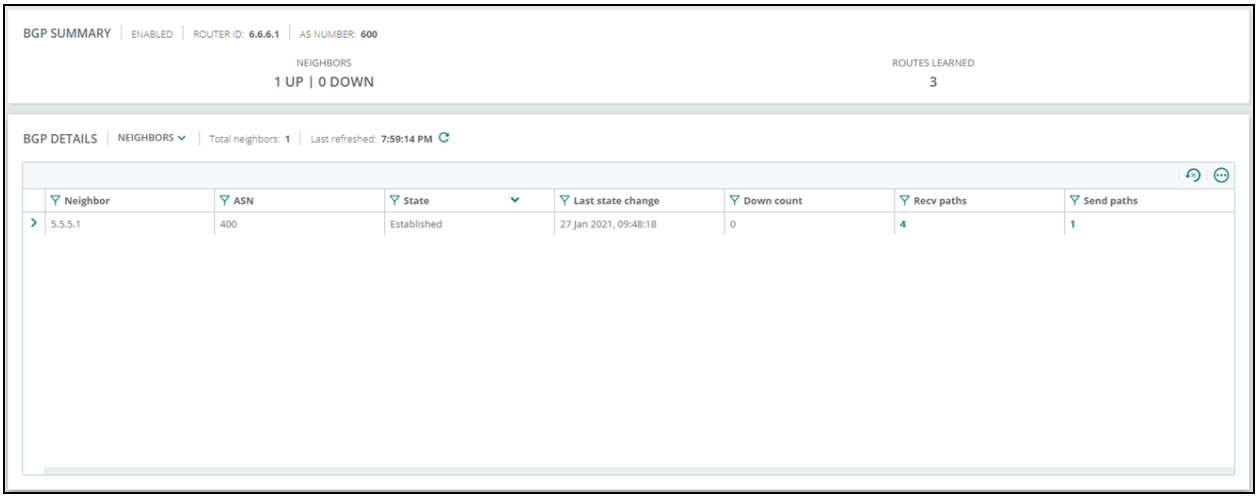
BGP Summary

The **BGPsummary** section displays the total number of neighbors, routes that were learned, router ID, and AS number details.

BGP Neighbors

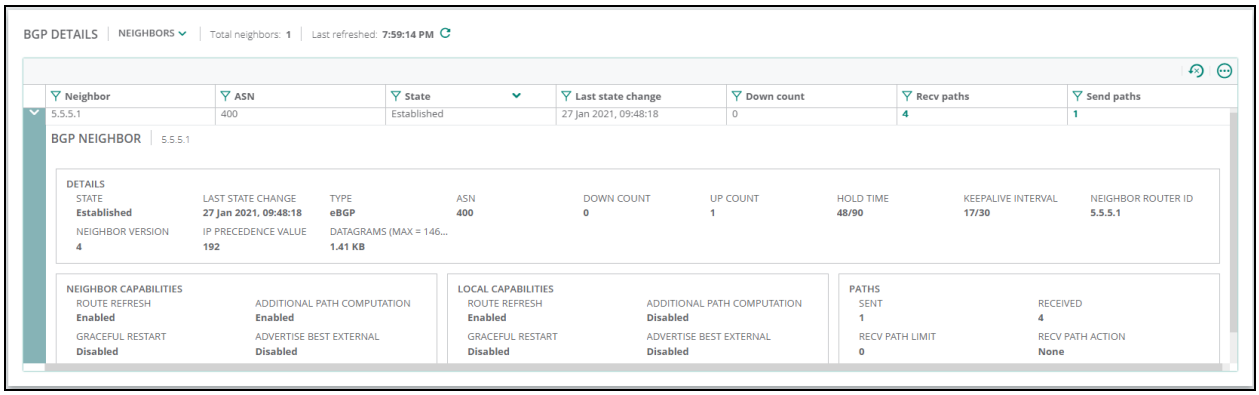
To view a list of BGP neighbors, click **Neighbors** in the **BGP Details** panel.

Figure 231 *BGP Summary*



To view more information about the BGP neighbor, click the neighbor entry in the table.

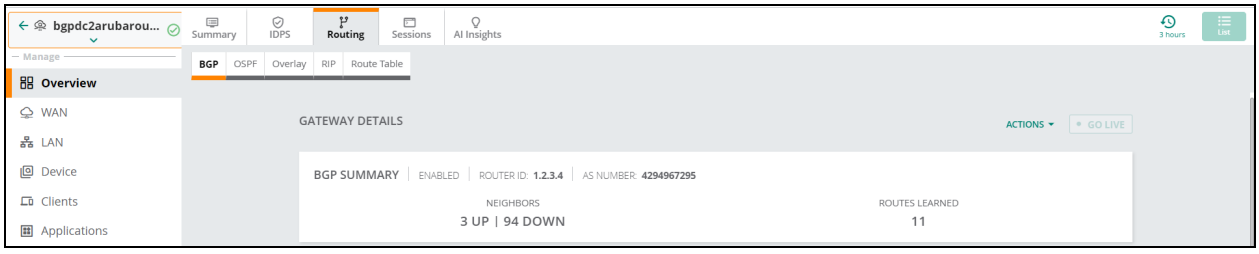
Figure 232 *BGP neighbor information*



BGP Routes

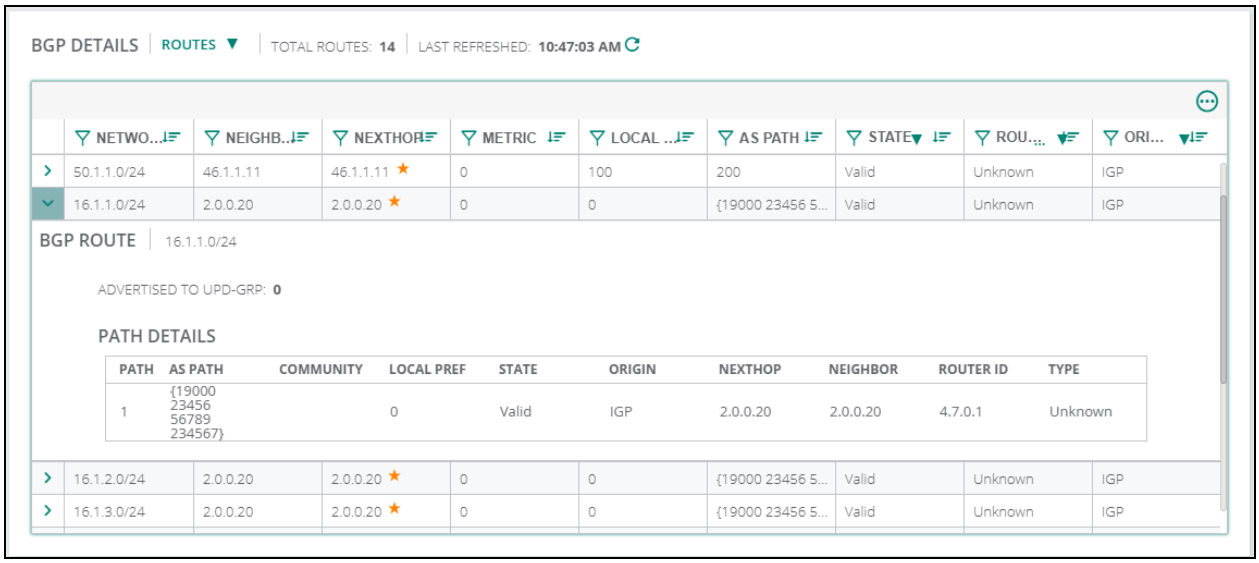
To view a list of routes advertised through BGP, click **Routes** in the **BGP Details** panel.

Figure 233 *List of routes advertised*



To view the details of a route, click the route entry in the table.

Figure 234 *Route details*



Viewing Route Table with BGP Routes

To view the route table:

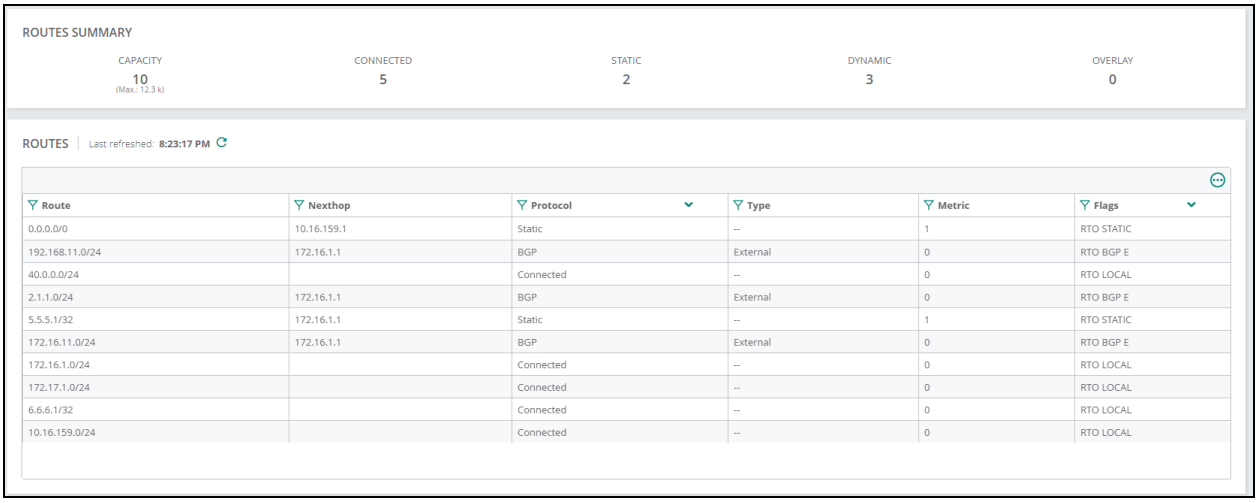
1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one Branch Gateway.

2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the List view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **Route Table**. A complete list of routes advertised by the Gateway is displayed.
5. Sort route the table by the BGP protocol to view the BGP routes.

Figure 235 *BGP routes*



For more information on the monitoring section, see Gateway > Overview > Routing.

Troubleshooting BGP Configuration Issues

To troubleshoot BGP configuration issues:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one Branch Gateway.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the List view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Analyze**, click **Tools**.
5. Click **Commands.**
6. From **Category**, select **Network**.
7. From the command list, select the BGP commands that you want to use. For example, **show ip bgp** or **show ip bgp neighbors**.
8. Click **Run**.
9. Verify the command output and resolve configuration errors if any.
10. Go to Gateway Details page, verify the configuration status, and monitor BGP routes. If the issue persists, contact Aruba Technical Support.

Routes Advertisement Using RIPv2

Routing Information Protocol (RIPv2) is a distance vector Interior Gateway Protocol (IGP) that uses the hop count metric for advertising subnets to the network. To support interoperability with an existing network infrastructure, Aruba Gateways support advertising routes learned from the SD-WAN overlay network into the data center network.

When RIPv2 support is enabled, Aruba Gateways function as peer devices and advertise routes to their RIP neighbors.

The following is a list of best practices for configuring RIPv2 on Aruba Gateways:

- The loopback interface can be used as the system IP of the Gateway and also as the RIP router ID. Ensure that you configure loopback interface on each Gateway. For more information, see Configuring System IP Address.
- The minimum software version required for RIP configuration on Aruba Gateways is ArubaOS 8.5.0.0-2.0.0.0.
- There are various parameters to set a route preference.

Workflow for Configuring RIPv2 Routing on Gateways

The **RIPv2** tab in the Gateway routing configuration page allows you to enable RIPv2 support on Gateways. The following steps are required on the Gateway devices for RIPv2 routing:

- Enabling RIPv2
- Configuring RIPv2 on a VLAN Interface
- Configuring RIP Timers for All VLAN Interfaces on Gateways
- Configuring Administrative Distance
- Configuring Infinity Value for RIP Routing

To verify, monitor, and troubleshoot RIPv2 routing configurations, see the following pages:

- Verifying RIP Configuration and Monitoring Routes
- Troubleshooting RIP Configuration Issues

Enabling RIPv2

By default, RIP is disabled on Gateways. You must enable RIPv2 on the gateway for sending RIP information.

To enable RIPv2 support on Gateways, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices**, and then click **Gateways**.

        A list of gateways is displayed in the **List** view.

     c. Click **Config**.

        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:

a. Set the filter to **Global**.
b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
d. Under **Manage**, Click **Device**.
   The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **RIP**.
4. To enable RIPv2, click **General** and turn on the **Enable RIPv2** toggle switch.
5. Click **Save Settings**.

Configuring RIPv2 on a VLAN Interface

You can configure RIPv2 on a VLAN interface in the Network Operations app by either selecting an individual Gateway or a group containing at least one Gateway.

To configure RIPv2 on a VLAN interface, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **RIP**.
4. Expand **Interface Settings**. The **Create New Interface** page is displayed.
5. Click **+** in the VLAN table.
6. Select the **Vlan ID**

7. Enter a value for **Metric**. You can define a metric value within the range of 1–255.

   RIP uses hop count as metric. The hop count refers to the number of routers that a packet can traverse before reaching its destination. For example, if you set the metric value to 2, two hop counts are used as metric for distributing RIP routes from the VLAN interface.

   A directly connected network has a metric of 1. By default, the metric value for RIP-enabled VLAN interfaces is set to 1.

8. Select **Passive** to enable passive mode and to prevent the VLAN interface from transmitting packets.

   When passive mode is enabled, the IP address of the VLAN interface is not advertised as an external route. By default, passive mode is disabled.

9. Select **Split-horizon** to prevent the interface from advertising routes learned from the same interface. When **Split-horizon** is enabled on a VLAN interface, the Gateway does not send the RIP routes that were learned from the same interface and thus avoids routing loops.
10. Select **Poison-reverse** to instruct the VLAN interface to advertise learned routes on the same interface. When **Poison-reverse** is enabled, a metric value of 16 is used for RIP routes.
11. Select one of the following options for **Authentication** if you want to authenticate RIP neighbors for secure exchange of routes, .
    - **Message-Digest**—Configures message digest key as a passphrase for authentication.
    - **Plain-Text**—Configures a plain-text password for authentication.
12. Configure timers for routing RIP updates on the VLAN interface:
    - **Update timer**—Determines how often RIP updates are sent over the VLAN interface. By default, the update timer is set to 30 seconds. The accepted range of values is 1–31536000.
    - **Flush timer**—Determines how long a route is maintained in the RIP database after it is declared invalid. Once the flush timer expires, the route is removed from the RIP database. By default, the flush timer is set to 120 seconds. The accepted range of values is 1–31536000.
    - **Invalid timer**—Determines the duration for declaring a RIP update as invalid. If a valid route update is not received for a route for the specified duration, the route is declared invalid but is maintained in the RIP database. By default, the invalid timer is set to 180 seconds. The accepted range of values is 1–31536000.
13. Click **Save Settings**.

Configuring RIP Timers for All VLAN Interfaces on Gateways

To configure RIP timers on all VLAN interfaces on Gateways, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.

        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices**, and then click **Gateways**.

        A list of gateways is displayed in the **List** view.

     c. Click **Config**.

        The configuration page is displayed for the selected group.

   - To select a VPNC or a Branch Gateway device in the filter:

a. Set the filter to **Global**.
b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
d. Under **Manage**, Click **Device**.
   The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** >**RIP**, and then click **Advanced**.
4. Define the time interval in seconds for the following RIP timers:
   - **Update timer**—Determines how often RIP updates are sent over the VLAN interfaces configured on Gateways. By default, the update timer is set to 30 seconds. The accepted range of values is 1–31536000.
   - **Flush timer**—Determines how long a route is maintained in the RIP database after it has been declared invalid. Once the flush timer expires, the route is removed from the RIP database. By default, the flush timer is set to 120 seconds. The accepted range of values is 1–31536000.
   - **Invalid timer**—Determines the duration for declaring a RIP update as invalid. If the route is not for the specified duration, the route is declared invalid but is maintained in the RIP database. By default, the invalid timer is set to 180 seconds. The accepted range of values is 1–31536000.

Configuring Administrative Distance

Administrative distance is one of the main criteria to determine a preferred route when there are multiple paths to the same destination learned from different routing protocols. The route with the lower administrative distance takes precedence for route redistribution.

To configure administrative distance, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.

d. Under **Manage**, Click **Device**.
   The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **RIP**, and then click **Advanced**.
4. Define a value for **Distance**. By default, the administrative distance value is set to 150.
5. Click **Save Settings**.

Configuring Infinity Value for RIP Routing

The infinity parameter defines the maximum number of next hops allowed for the RIP network. A RIP network is usually no wider than 15 hops, and therefore, the infinity value is set to 16 by default.

To change the infinity value, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To select a VPNC or a Branch Gateway device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name**.
        The dashboard context for the device is displayed.
     d. Under **Manage**, Click **Device**.
        The device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **RIP**, and then click **Advanced**.
4. Select a value for **Infinity**.
5. Click **Save Settings**.

Verifying RIP Configuration and Monitoring Routes

To verify RIP configuration and monitor RIP routes, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a VPNC group or a Branch Gateway group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the group contains at least one VPNC or a Branch Gateway.

The dashboard context for the group is displayed.

b. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To select a VPNC or a Branch Gateway device in the filter:
  a. Set the filter to **Global**.
  b. Under **Manage**, click **Devices**, and then click **Gateways**.
     A list of gateways is displayed in the **List** view.
  c. Click a gateway listed under **Device Name**.
     The dashboard context for the device is displayed.
  d. Under **Manage**, Click **Device**.
     The device configuration page is displayed.

2. Under **Manage**, click **Overview** > **Routing** > **RIP**.
   The **RIP Summary** page is displayed.
   The **RIPsummary** page displays the RIP version, interfaces on which RIP routing is enabled, the total number of neighbors, routes, and infinity value.
   The **RIP Details** panel displays detailed information for RIP interfaces, neighbors, and routes.

For more information, see Gateway > Overview > Routing.

Troubleshooting RIP Configuration Issues

To troubleshoot RIP configuration issues, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** to view the dashboard for all devices.
2. Under **Analyze**, click **Tools**.
   The **Tools** page for troubleshooting devices is displayed.
3. Click **Commands**.
4. Set the device type to **Gateway** and select the gateway device you want to troubleshoot.
5. From the **Categories** drop-down list, select **Network**.
6. From the command list, select the RIP commands that you want to use. For example, **Show IP RIP**, **Show IP RIP Interfaces** or **Show IP RIP neighbors**.
7. Click **Run**.
8. Verify the command output and resolve configuration errors if any.
9. Go to the Gateway monitoring dashboard, verify the configuration status, and monitor RIP routes. If the issue persists, contact Aruba Technical Support.

Configuring Policies for PBR

For most SD-WAN deployments, Branch Gateways forward traffic through the overlay network or to the Internet using destination-based routing. Each Branch Gateway includes static routes for the corporate subnets that point to their respective VPN overlay tunnels as well as default gateways for each WAN uplink.

However, for some deployments, you may need to forward traffic from a subset of devices through a specific VPN overlay tunnel or to a specific Internet WAN uplink. Alternatively, you may require all traffic (corporate and Internet) to be forwarded through the overlay VPN tunnels or force all traffic to be forwarded locally using Policy Based Routing (PBR). A typical use case for PBR would be to force all traffic to a specific VPNC or a tunnel endpoint.

PBR allows your network administrators to create policies for making routing decisions. You can create a PBR rule that can forward traffic as normal, or route traffic over a VPN tunnel specified by an IPsec map. The PBR rules can also route traffic to a next hop router on a next hop list, or redirect it over an L3 GRE tunnel or tunnel group. PBR rules allow administrators to make use of all available uplinks.

PBR Policies for WAN Networks

In the SD Branch solution, the administrators can create PBR policies to configure preferred VPN traffic routing paths for different types of traffic based on their source and destination IPs and ports.

To use PBR policies or rules on WAN networks, you must configure the following features and parameters on Aruba Gateways:

- **PBR next hop**—The PBR next hop can be physical links such as the Ethernet or 3G/4G uplinks. The administrators can also use logical links like site-to-site VPN tunnel.
- **Route ACL**—The administrators can define traffic match conditions and the next hop for the traffic in the ACL.
- **Attach Points**—To apply the PBR rules, the administrators associate the ACL rules to a user role or VLAN.

  After the next hop list is configured and attached to route ACL, the active IP address for the next hop is selected based on the reachability and priority.

  When the user traffic hits the route ACL, the following actions are applied:
- If PBR is disabled on the user-role or VLAN, traffic is directly sent to the routing block where the regular routing takes place.
- If the PBR is enabled, the traffic is evaluated against the route ACL and the appropriate PBR next hop is selected for routing.
- If traffic does not match any rule in route ACL, it is passed to the routing module for regular forwarding.

If Dynamic Path Steering selects an uplink that is not provided by PBR, the PBR forwarding path takes precedence.

Configuring Policies for PBR

To configure a policy for PBR on Branch Gateways, complete the following steps:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.

     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.

     c. Click **Config**.

        The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
    a. Set the filter to **Global** or a group containing at least one Branch Gateway.
    b. Under **Manage**, click **Devices** > **Gateways**.
    A list of gateways is displayed in the List view.
    c. Click a gateway under **Device Name**.
    The dashboard context for the gateway is displayed.
    d. Under **Manage**, click **Device**.
    The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **Policy-Based Routing**.
4. Click **+** below the **Policies** table to create a new routing policy.
5. Enter name for the policy and save the changes.
6. Select the policy from the **Policies** table.
7. Click **+** to add ACL rules. For more information on ACL rule configuration, see Configuring Access Rules.
8. Save the changes.
9. Assign the policy to a user role or VLAN. For more information, see Assigning PBR Policies to User Role or VLAN.

Assigning PBR Policies to User Role or VLAN

To assign a PBR policy to a user role or a VLAN, complete the following steps:

1. To assign a policy to a user role, see Configuring User Roles for Clients.
2. To assign a policy to a VLAN, complete the following steps:
    a. To configure a gateway group or a gateway device, complete either one of these steps:
        - To configure a Branch Gateway group or VPNC group, complete the following steps:
            a. Set the filter to a group containing at least one Branch Gateway.
            The dashboard context for a group is displayed.
            b. Under **Manage**, click **Devices** > **Gateways**.
            A list of gateways is displayed in the **List** view.
            c. Click **Config**.
            The configuration page is displayed for the selected group.
        - To configure a Branch Gateway or VPNC, complete the following steps:
            a. Set the filter to **Global** or a group containing at least one Branch Gateway.
            b. Under **Manage**, click **Devices** > **Gateways**.
            A list of gateways is displayed in the List view.
            c. Click a gateway under **Device Name**.
            The dashboard context for the gateway is displayed.
            d. Under **Manage**, click **Device**.
            The gateway device configuration page is displayed.
3. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
4. Click **Interfaces** > **VLANs** tab.

5. Select a VLAN from the **VLANs** table.
6. Select the VLAN ID to which you want to assign a routing policy from the **VLAN IDs** table.
7. Under the **IPv4** tab, expand **Other option**.
8. Select a routing policy from the **ACL** drop-down list.
9. Save the changes.

Configuring Next Hop Lists for PBR

You can configure SD-WAN Gateway to use policy-based routing and forward packets to a next hop device. With the next hop list, the administrators can ensure that when the next hop device becomes unreachable, the packets matching the policy can still reach their destination.

From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, when using IP Next-Hop lists, Aruba SD-Branch gateways allow configuring two options for tracking. When configured to use an IP address or a DHCP default-gateway, gateways can either track the immediate next-hop or the IP/FQDN of the remote host defined as WAN Health Check.

To define a next hop list, complete the following steps:

1. To configure a gateway group or a gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Routing** > **NextHop Configuration**.
4. Click **+** to add a new next hop list and configure the following parameters:

Figure 236 *Next Hop Settings*

Parameter	Description
NextHop-list name	Name of the new next hop list.

Parameter	Description
NextHop IP/DHCP	IP address of the next hop device or the VLAN ID of the VLAN used by the next hop device. If the VLAN gets an IP address using DHCP and the default gateway is determined by the VLAN interface, the gateway IP is used as the next hop IP address. When you click **+** to define a next hop IP or DHCP value, a pop-up list with a field that requires you to select either the **IP** or **DHCP** option is displayed. ■ If you selected **IP**, enter the IP address and priority of the next hop device in the **IP** and **Priority** fields, respectively. ■ If you selected **DHCP**, enter the VLAN ID and priority of the next hop device in the **VLAN ID** and **Priority** fields, respectively. Priorities of next hops define which next hop should get a higher priority to carry the session traffic. A higher number indicates a higher priority (1 – 255). If two next hops have the same priority, they will be load-balanced.
IPsec name map	A next hop list may require policy-based redirection of traffic to different VPN tunnels. To add an IPsec name map, complete the following steps: 1. Click **+** from the **IPsec name map** table. The **Add New IPsec Map** pop-up is displayed. 2. Select one of the following options from the **Forward settings** drop-down list based on your requirement: ■ **Using Site-to-Site IPSec**—Select this option for a site-to-site VPN or Zscaler tunnel and select the required IPsec map from the **Using site-to-site IPSec** drop-down list. If uplink VLAN is configured for the selected IPsec map, then you can select the required uplink from the **Uplink** field. **NOTE:** The **Uplink** field does not appear for IPsec maps that are not configured with uplink VLAN. ■ **Using IPsec Tunnel to VPNC**—Select this option for a Hub and Spoke VPN and select the required MAC address and the uplink of the VPNC from the **Using IPSec tunnel to VPNC** and **Uplink** options lists respectively. You can also select **None** if you want to use Auto-VPN. For more information, see Configuring the SD-Branch Overlay Network. 3. Enter the priority value for the forward setting in the **Priority** field. **NOTE:** Use the same priority for different paths from the same SD-WAN Gateway but different priorities for different Zscaler data centers. 4. Click **OK**.
Preemptive-failover	If **Preemptive-failover** is disabled and the highest-priority device on the next hop list is disabled, the new primary next hop device functions as the primary device even when the original device comes back online. **NOTE:** Ensure that **Preemptive failover** is enabled for Zscaler tunnels.

5. Click **Save Settings**.

Configuring Policies for Dynamic Path Steering

For a transport-independent SD-WAN fabric, the SD Branch devices form IPsec tunnels over all WAN circuits. For your branch setup to work across asymmetric links, a path selection criteria is required to enable Branch Gateways to dynamically choose an upstream path in real-time. To enable Branch Gateways to dynamically

steer traffic to an upstream path, you can create WAN policies with specific performance criteria for different types of traffic, so that the best local uplink or optimal path (MPLS or the internet) is used for a given traffic flow.

The dynamic path selection feature allows you to steer and route traffic in real-time and load-balance traffic across available uplinks. For example, you can create policies that would route the most critical traffic, such as voice traffic, through the MPLS network, while the rest of the traffic is load-balanced. You could also set policies to route the voice traffic over uplinks with the least amount of packet loss, while the other types of traffic can be routed to uplinks with the lowest latency.

The Aruba SD Branch solution also supports Forward Error Correction (FEC), the ability to compensate any packet loss during traffic flow. This is achieved by inserting intermittent error recovery or redundant packets in the traffic flow. These redundant packets make up for the lost packets when the link loss quality goes below the configured SLA limit. The uplink works until the packet loss reaches the FEC threshold beyond which it becomes non-compliant. This feature improves applications' performance across the WAN and proves very useful for business-critical applications.

For optimal use of uplink resources, you can configure path steering policies with specific match criteria to choose an uplink. The uplink choice is driven by the parameters in the threshold profile, which include latency, jitter, packet loss, and bandwidth utilization metrics.

How Dynamic Path Selection Works

A dynamic path steering policy serves as a global policy that determines paths for the outgoing corporate and Internet traffic. The policy consists of the following configurable components:

- **Rules**—The policy includes a sequential list of rules for traffic steering.
- **Service Level Agreements (SLAs) and Threshold Settings**—Each of these rules can be configured with specific threshold settings that are based on SLAs.
- **WAN path preferences**—The policy also allows you to set a path preference and enable load balancing of sessions among multiple paths.

The status bar remains gray color when there is no data to display.

Example

The following example illustrates the path selection workflow:

1. A client device tries to connect to the network.
2. The authentication server authenticates the client, assigns the employee role, and then directs the client to the SD-WAN Gateway.
3. The firewall classifies the session as Skype.
4. The routing for an employee using Skype states that the next-hop is a VPNC and that the paths available are MPLS, INET1, and LTE.
5. As Skype is classified as **UCC**, the policy categorizes it as **voice** traffic. The policy is configured to use MPLS as the preferred path with an SLA criterion.
6. If the threshold metrics for MPLS meet the SLA for the voice policy, the session goes through the tunnel that is established using the MPLS uplink.
7. If at any point in time the measured SLA for MPLS drops, the SD-WAN Gateway steers traffic to another active tunnel.

NOTE

If none of the uplink group members are compliant with the policies configured, the SD-WAN Gateway chooses the best among the available uplinks.

Configuring a Dynamic Path Steering Policy

The Dynamic Path Steering policy configuration procedure includes the following tasks

NOTE

Ensure that you configure health check probe destinations and uplinks before configuring the dynamic path steering policies.

1. Creating a Dynamic Path Steering Policy
2. Configuring Traffic Specification Rules
3. Configuring SLA Parameters
4. Configuring WAN Path

Creating a Dynamic Path Steering Policy

To create a dynamic path steering policy, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway for which you want to create a dynamic path steering policy, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **WAN** > **Dynamic Path Steering**
4. To create a new policy, click **+**.
5. Enter the name of the policy.
6. Configure Traffic Specification Rules.
7. Click **Save Settings**.
8. Click **Next**.
9. Select SLA for the new policy. You can select an existing SLA or create a new one.

10. Select the WAN path for the new policy.
11. Click **Finish**.

Configuring Traffic Specification Rules

To add traffic specification rules, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Go to **WAN** > **Dynamic Path Steering**.
7. From the list of policies, select the policy to edit.
8. Click the edit icon in **Traffic Specification Rules**.
9. To add a new rule, click **+**, and then configure the following parameters:
   - **Source**—You can set the source to any of the following options:
     - **Any**—For the traffic coming from any of the source.
     - **User**—For the traffic originating from a specific user.
     - **Host**—For the traffic that has a specific host. If you select this option, you have to provide the IP address of the Host.
     - **Network**—For the traffic that has a specific source IP from a subnet of IP addresses. If you select this option, you have to enter the IP address and the subnet mask of the source network.
     - **Alias**—For the traffic originating from an alias of a host or network. If you select this option, you have to select the **Source alias** from the drop-down list.
     - **User Role**—For the traffic originating from a specific user role. If you select this option, you have to select an existing user role from the list or create a new role to steer traffic only from users with that role.
   - **Destination**—You can set the destination to any of the following options:
     - **Any**—For the traffic coming from any of the source.
     - **Host**—For the traffic that has a specific host. If you select this option, you have to provide the IP address of the Host.
     - **Network**—For the traffic that has a specific source IP from a subnet of IP addresses. If you select this option, you have to enter the IP address and the subnet mask of the destination network.
     - **Alias**—For the traffic originating from an alias of a host or network. If you select this option, you have to select the **Destination alias** from the drop-down list.

- **Application/Port**—You can select any of the following options:
  - **Application**—To set rules for a specific application, for example, Facebook.
  - **Application Category**—To set traffic rules for application category, for example, social networking.
  - **Web Categories/Reputations**—To set rules for web categories, for example, travel.
  - **UDP**—To set rules for the traffic passing through the UDP ports.
  - **TCP**—To set rules for the traffic passing through the TCP ports.
  - **Service**—To set rules for any specific network service.

10. Click **Save Settings**.
11. Click **Next** to configure SLA parameters.

For example, if you set the source as **User Role** such as *employee*, and the destination is restricted to a specified network, based on other configurations such as preferred uplinks and SLAs set, the Dynamic Path Steering feature steers traffic dynamically through the most viable path.

Configuring SLA Parameters

To set SLA parameters for the traffic type configured for the policy, complete the following steps:

1. In the policy definition, configure the following SLA categories and parameters:
   - **Name**—Name of the service. The default services are **BestForInternet**, **BestForVoice**, and **HighlyAvailable**. Click **Create new SLA** to add a new service.
   - **Latency**—To measure the round-trip ping time. You can set a threshold value in milliseconds.
   - **Jitter**—To measure if the packets are delivered in a proper order. You can set a threshold value in milliseconds to observe jitters in packet transmission.
   - **Loss**—To measure packet loss. You can set a specific percentage of packet loss allowed for the traffic type.
   - **Utilization**—To measure the percentage of bandwidth utilization. You can set a specific percentage of bandwidth utilization as a metric to prioritize and load-balance the traffic.
   - **Loss correction (FEC)**—Select this check box if you want to enable Forward Error Correction and improve link and application performance.
   - **Loss percentage with FEC**—Enter the FEC threshold in percentage beyond which the link becomes unstable due to packet loss.
   - **FEC ratio**—Define the loss-recovery packets to data packets ratio to compensate for the lost packets . You can choose the FEC ratio based on the link quality. If you anticipate or experience more packet loss, you could select 1: 2 which is a more aggressive FEC ratio to preserve bandwidth. The following are the available FEC ratios to choose from:
     - 1:2 - For every 2 packets that match the DPS policy, one extra packet is sent. This increases the bandwidth usage by 50%.
     - 1:4 - For every 4 packets that match the DPS policy, one extra packet is sent. This increases the bandwidth usage by 25%.
     - 1:8 - For every 8 packets that match the DPS policy, one extra packet is sent. This increases the bandwidth usage by 12.5%.

- For all the 72XX platforms, FEC is supported for 512 K sessions; for all other platforms, FEC is supported for 128 K sessions.
- FEC must not be enabled on the Branch Gateway when the VPNC is running SDWAN 2.1 or earlier version.

2. Click **Next** to configure WAN path.
3. Set probe options for SLAs if required. To set the probe options select an SLA and click **Show Probe Options**:
   a. Set the probe interval in seconds. During this interval, a number of probes are sent to determine the SLA thresholds.
   b. For **Bursts per Probe**, specify the number of probes to be sent during the probe interval.

Configuring WAN Path

To configure a WAN path for traffic types defined in the policy, complete the following steps:

1. Click the edit icon in **WAN Path Selection**.
2. In the policy definition, set the following parameters for WAN path selection:
3. Click **Finish**.

Routing Traffic After Path Selection

After path selection, the next hop is determined by the IP forwarding table. When a path is selected, the IP forwarding table determines the next hop. Based on the routes configured on the Branch Gateway, the next hop can be an IPsec map or the router IP address.

- If the next hop is an IPsec map, the session is forwarded to the IPsec map that is configured in the forwarding table associated with the selected path.
- If the next hop is a router IP address, the session is forwarded to the default gateway that is associated with the selected path.

SaaS Application Traffic Management with SaaS Express

The Software as a Service (SaaS) Express feature is an Aruba SD-Branch solution for the traffic management of SaaS applications. SaaS Express provides the best user experience when connecting the users from a branch site to SaaS applications. The methods and techniques used by SaaS Express to achieve its purpose are explained in detail in this guide.

Why Aruba SaaS Express?

It is a key challenge for network administrators to cope with the rapid adoption of SaaS applications, such as Microsoft 365 (formerly Office 365), Dropbox, Salesforce, and many others. The SaaS providers recommend enterprises to use split tunnel to send SaaS traffic directly over the internet from each branch location for accessing SaaS applications. This approach raises a concern for the enterprises wherein, this could result in loss of visibility into SaaS usage and performance. Also, the policy controls implemented to optimize the SaaS experience may affect the clients at those branch locations.

Following are the important factors to consider when optimizing the SaaS traffic:

- SaaS applications are hosted all over the world and the closest entry point to the SaaS service could be different from the one that is chosen by default for a location. Thus, enterprises require a solution that

can direct SaaS traffic on the best available path from each branch location to improve the user experience.

- The ISP network used at a branch (to transport the SaaS traffic) is likely to have variable loss or latency that is difficult to track or predict.

Branch Gateways deployed at branch sites must have the ability to dynamically steer traffic to SaaS servers that provide the best performance by continuously monitoring the health of the servers and the WAN links.

Aruba SaaS Express connects users from a branch site to SaaS applications seamlessly and securely. It provides the following benefits:

- Network-wide visibility for all SaaS applications
- Improved performance for all SaaS applications
- Improved service reliability through dynamic steering of SaaS traffic
- Optimal user experience through best path connections to SaaS applications
- Optimized for Microsoft 365

See the following sections for information about deployment and criteria for optimal path selection:

- SaaS Express Fundamentals
- Design and Deployment
- Deployment Scenarios

SaaS Express Fundamentals

By using SaaS Express, the Branch Gateways dynamically identify the optimal path to reach high-priority SaaS applications. The following components are required to identify the optimal path:

- Branch Gateways must be capable of measuring the Quality of Experience (QoE) through all circuits with internet access. Branch Gateway will also be capable of monitoring the actual performance of the SaaS applications after a path is chosen and traffic is flowing through the gateway.
- Gateways must proxy DNS requests to those SaaS applications to ensure the closest SaaS nodes are resolved.
- Branch Gateways must forward SaaS traffic through the selected path (based on the measurements done by probing the SaaS front doors).

The following topics are discussed in this section:

Quality of Experience Measurement

Branch Gateways monitor the state of each WAN circuit by probing their default gateway and the tunnel destinations. It also probes a distributed responder service that is hosted on the Aruba Cloud (Aruba PQM Service) to assess the health and status of every uplink. The following components are required for assessing the health and status:

- A default gateway through every WAN interface to consider as the uplink.
- Gateways sending probes to all tunnel destinations (through all uplinks) to measure the health and state of the overlay.
- Gateways sending probes to a Health Check IP/FQDN (by default, Aruba PQM service) to measure health and state of the underlay.

These synthetic probes provide a good measure of how the overlay communications are working as well as the quality of the last mile for each WAN circuit. Based on the quality measured by the probes, Branch Gateways select the best WAN circuit as per the defined policies in the Dynamic Path Steering configuration. This happens regardless of whether the traffic is going over the SD-WAN overlay or directly out to the internet.

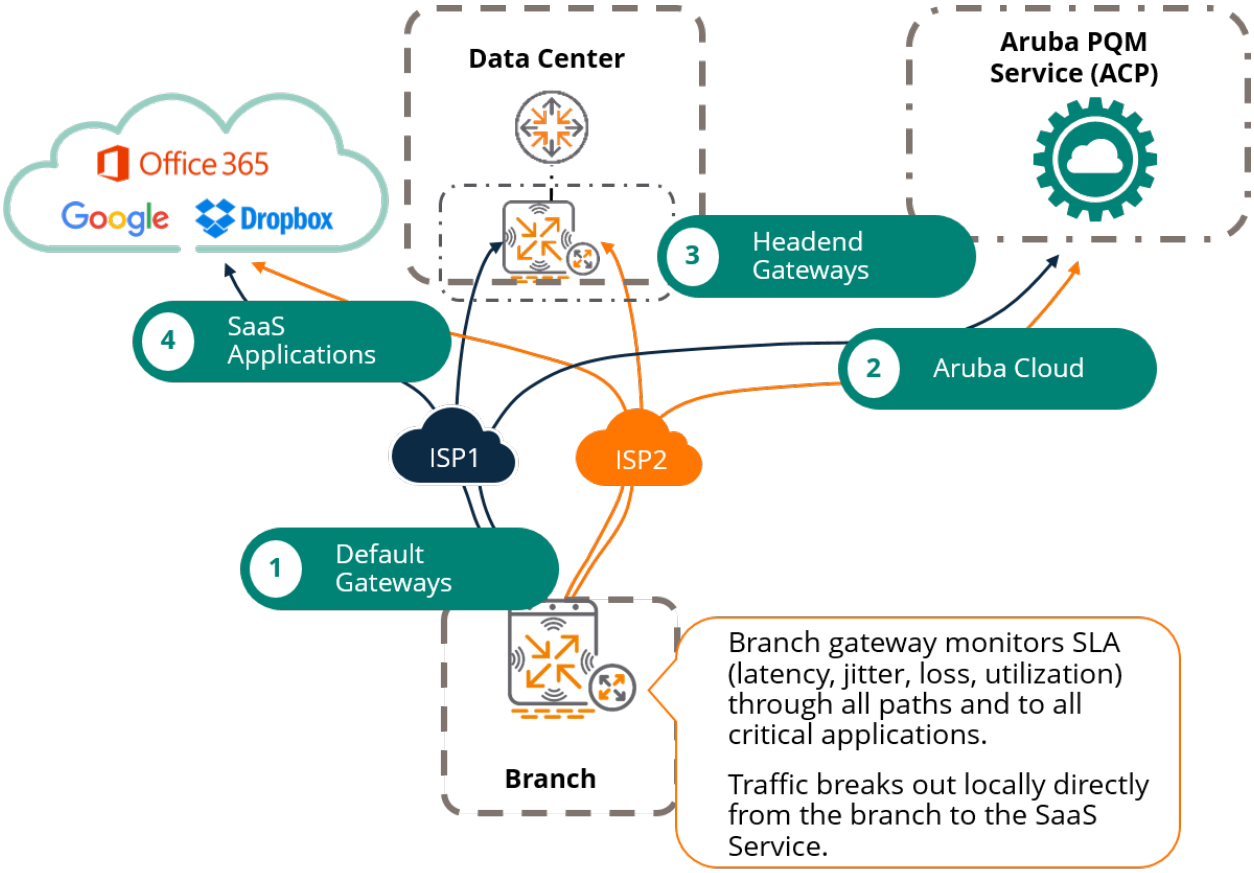
Active SaaS Monitoring

The active SaaS monitoring approach works well for internal networks as well as general internet traffic. However, business-critical SaaS applications (Microsoft 365, Google Workspace, Zoom, and so on) require a dedicated method to guarantee the best user experience. Problems outside the control of the enterprise network administrator, such as ISP-SaaS peering problems or DNS issues may impact a critical service for the business.

When SaaS Express is set to optimize an application, Branch Gateways resolve the front door URLs by querying the DNS servers configured (or learned through DHCP from the ISP) for SaaS applications every 15 minutes. This resolves the closest SaaS front doors and sends probes to SaaS front doors (every 10 seconds

when set to optimize or every 60 seconds in monitor-only mode). The statistics collected from these probes are used to enforce path steering policies on the SaaS traffic.

Figure 237 *Active SaaS Monitoring*

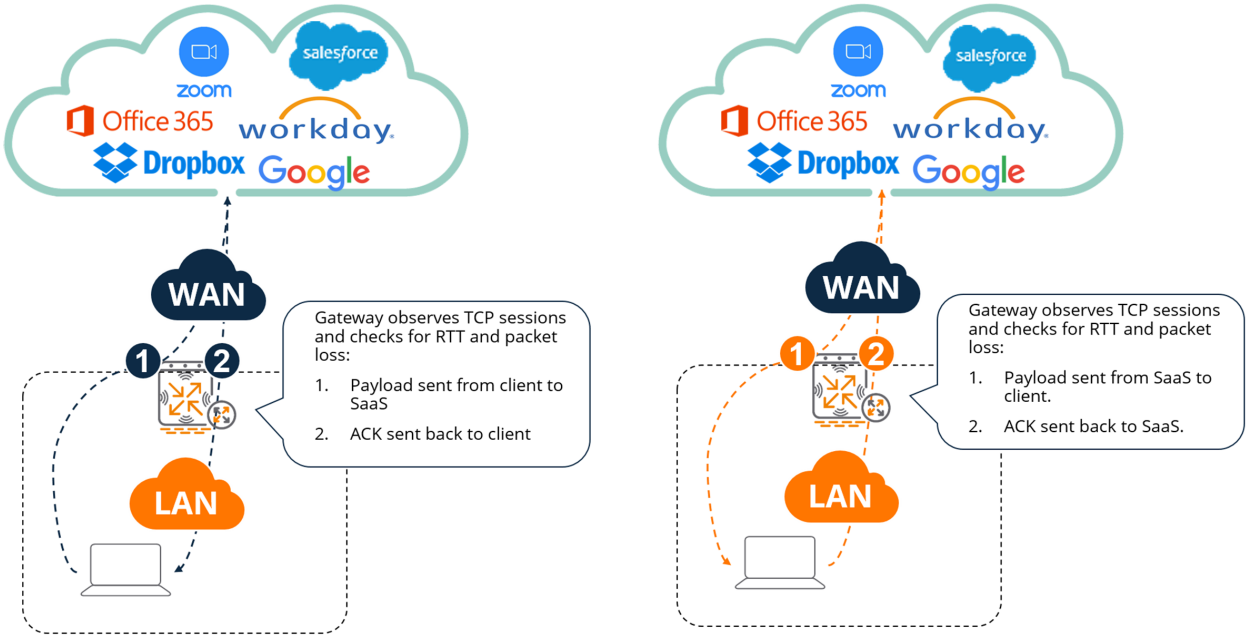


Passive SaaS Monitoring

The passive SaaS monitoring is used to restrict visibility. When the SaaS traffic starts going through the Branch Gateway, it measures the actual performance of the LAN and WAN segments by monitoring the TCP flows as they go through the gateway.

A better understanding of the SaaS applications' performance is achieved by having both active measurements (based on synthetic probes) as well as passive monitoring (based on observing TCP flows).

Figure 238 *Passive SaaS Monitoring*

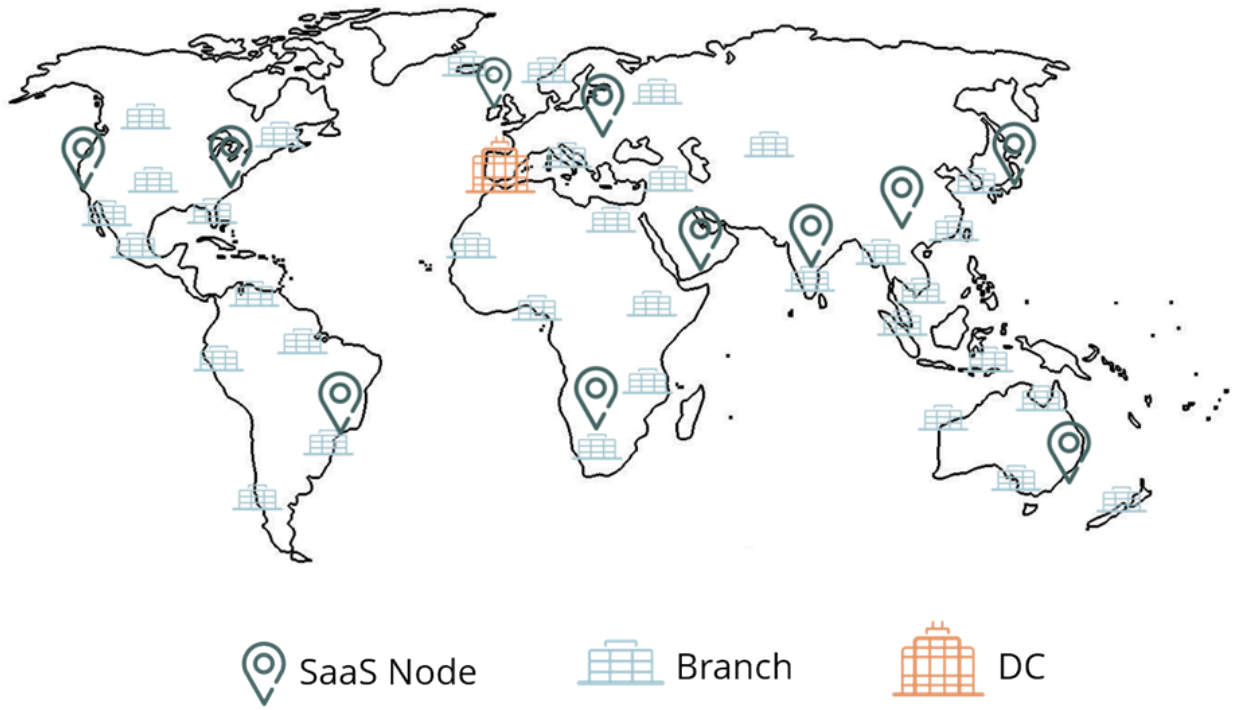


Ensure Routing to the Closest SaaS Node

It is common in enterprise networking for users to resolve addresses against the corporate DNS server that is either hosted in the datacenter or virtual private cloud. This provides additional control and security mechanisms for traffic that is going out to the internet along with allowing the resolution of internal IP addresses.

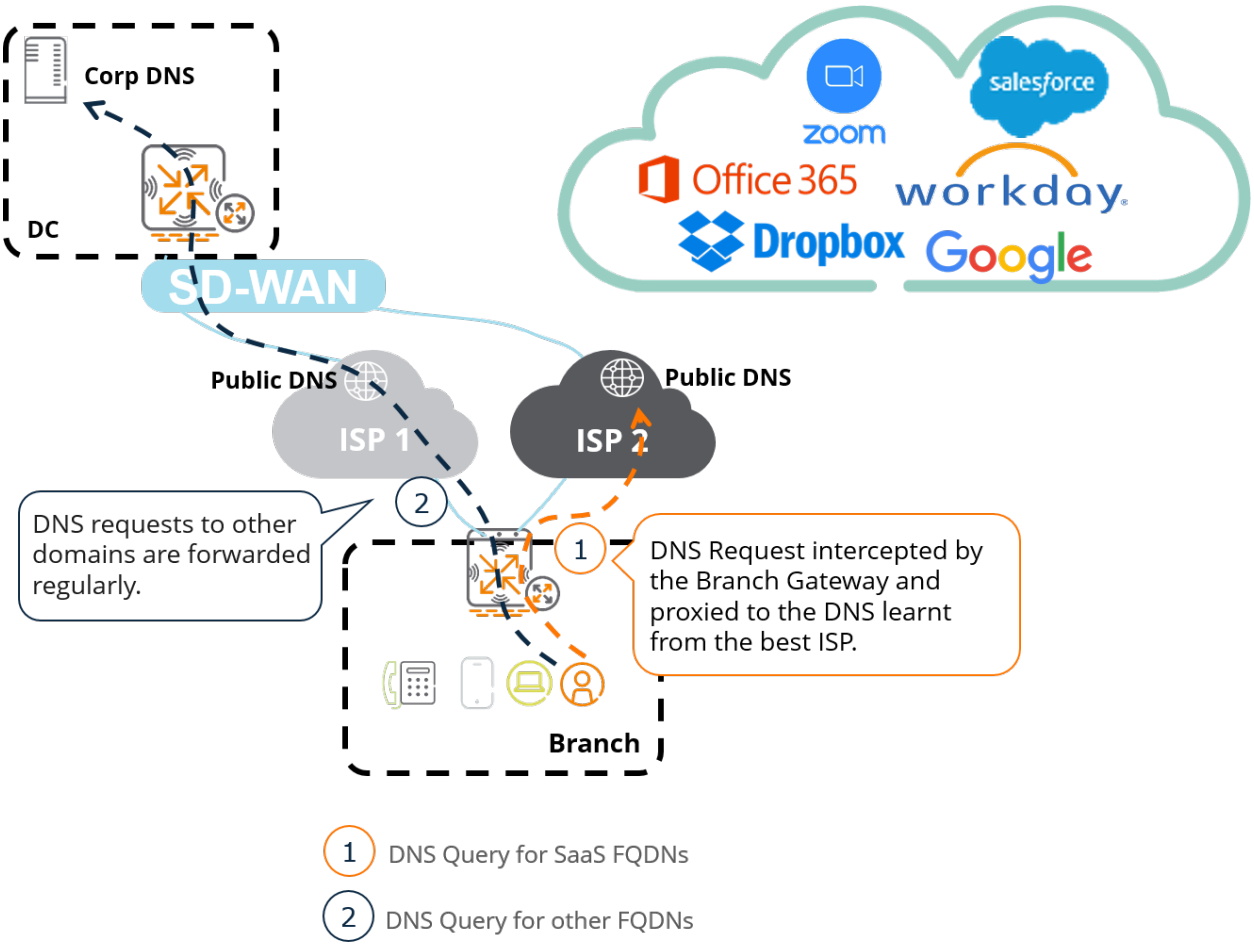
These reasons justify the use of corporate DNS servers that lead to suboptimal user experience as the IP addresses of the critical SaaS applications are resolved by a DNS server that can be in a different location. As an example, a user connecting from a branch in Australia could be resolving the IP address of portal.office.com against a DNS in Europe. This would result in this user connecting to the SaaS node closest to the DNS server (in Europe) instead of any other that may be closer (most SaaS applications have SaaS nodes all around the world).

Figure 239 *Closest SaaS Node*



When using SaaS Express, DNS requests going to the domains corresponding to the applications being optimized are captured by the Branch Gateway and proxied to the ISP. This mechanism works irrespective of the DNS server configured in the client devices.

Figure 240 *Sending DNS Requests*



Best Path for Routing the Traffic

SaaS Express is designed to optimize SaaS applications when the traffic exits through the local breakout. When using a split tunnel traffic pattern (where only the prefixes advertised by other gateways are routed through the overlay), SaaS chooses the local breakout. In full tunnel scenarios or in scenarios where the internet traffic is sent through a cloud security service, exceptions must be introduced in the routing policies to prevent sending SaaS traffic through the overlay.

Application Identification

Branch Gateways use different application identification mechanisms. The traffic must be properly classified to breakout locally, prioritize, and provide visibility on SaaS traffic.

DNS Snooping

When defining a SaaS application (or customizing the default ones), the FQDNs used by the application are defined as part of the SaaS Express configuration. When it is configured to optimize a particular application, the Branch Gateway DPI engine snoops the DNS requests to learn which IP addresses are being used by each application. This allows the application identification engine to form a cache of all the IPs or ports that are in use by that application.

For DNS snooping, DPI must be enabled on Branch Gateways.

Deep Packet Inspection

Branch Gateways performs Deep Packet Inspection for more than 3200 well-known applications. To make classification for SaaS applications more robust, pre-defined SaaS Express applications are associated with one or more of the applications classified by the DPI engine.

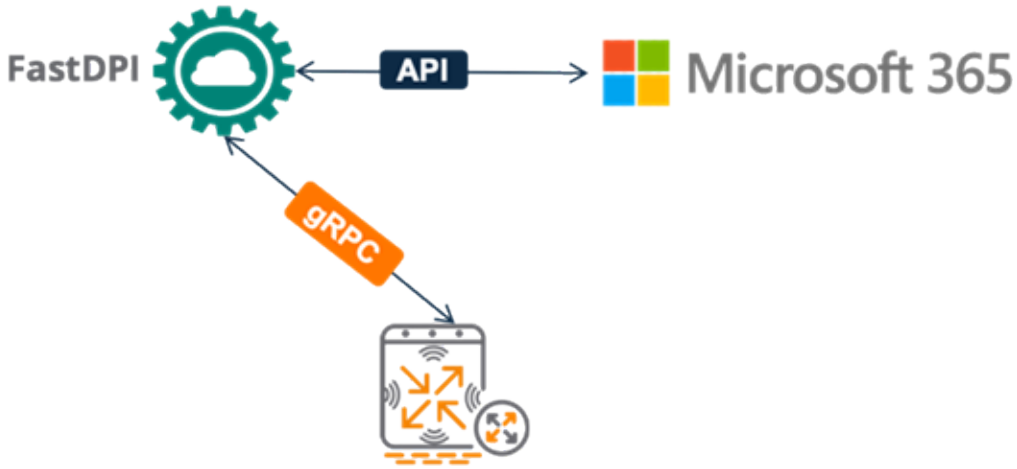
API to Classify Microsoft 365

Microsoft 365 provides an API to help SD-WAN vendors classify the IP addresses and FQDNs. By probing *aka.ms/IPURLWS*, the SD-WAN solution learns what IPs/FQDNs are being used by the different applications in Microsoft 365. These IPs/FQDNs are classified in the following categories:

- **Optimize**: Services hosted by Microsoft that involve real-time traffic, and therefore it must be optimized. As per the recommendation from Microsoft 365, these must be reached directly over the internet to minimize the distance. Microsoft guarantees the security of the resources.
- **Allow**: Services hosted by Microsoft that do not involve real-time traffic. Microsoft guarantees the security of the resources, so it is still recommended to reach these services directly over the internet.
- **Default**: Services that are required as part of the Microsoft 365 experience, but may or may not be hosted by Microsoft. Microsoft does not offer security guarantees, therefore recommends treating this as normal internet traffic.

SaaS Express uses *fastdpi*, a micro-service running on Aruba Central that polls Microsoft's API every 90 minutes to be up-to-date with any new IP/FQDN. Gateways configured to optimize Microsoft 365 applications query the *fastdpi* service through the dedicated control channel pre-established with Aruba Central (gRPC) to learn the list of IPs or domains used for every category. For SD-Branch versions 8.7.0.0-2.3.0.0 and higher, the SD-Branch automatically maps the prefixes in the **Optimize** and **Allow** categories to the corresponding *application_saas* aliases, and the FQDNs to the SaaS Express application definitions to facilitate according to Microsoft 365 best practices. The gateways act as DNS proxy for all FQDNs classified by Microsoft, and the *_saas* Microsoft application makes use of the IP addresses learned from the API for traffic classification (WAN or PBR policies).

Figure 241 *Classifying Microsoft 365*



Traffic Forwarding

When the SaaS application traffic is identified correctly, the SaaS Express option is effectively an extension of Dynamic Path Steering (DPS). The performance of a circuit is measured using synthetic probes and traffic is dynamically steered on available paths that comply with the Service Level Agreements (SLA). An additional nuance is the requirement to locally breakout SaaS application traffic, which results in adding exceptions to the Policy Based Routing (PBR) policies.

To facilitate this, when an application is defined in SaaS Express, a matching application group alias is created. This alias represents the IPs (in the case of Microsoft 365) or FQDNs used by the SaaS application. It allows the Branch Gateway to route all the traffic corresponding to each SaaS application through the defined path. These aliases are easily identified as the name is suffixed with *_saas*. For example, *dropbox_saas* or *exchange_saas*.

Design and Deployment

To design a network using SaaS Express, it is important to understand how SaaS Express interacts with other mechanisms as traffic traverses the Branch Gateway. Given the particular nature of SaaS Express, both control and data plane components must be considered.

Control-Plane Integration

The following elements are used in a control plane:

- Probes that are sent to the SaaS front doors to measure quality through every Internet Service Provider (ISP).
- DNS traffic is snooped to learn the destination IP addresses associated with each domain.
- DNS requests to SaaS domains are proxied to the servers learned from each ISP.

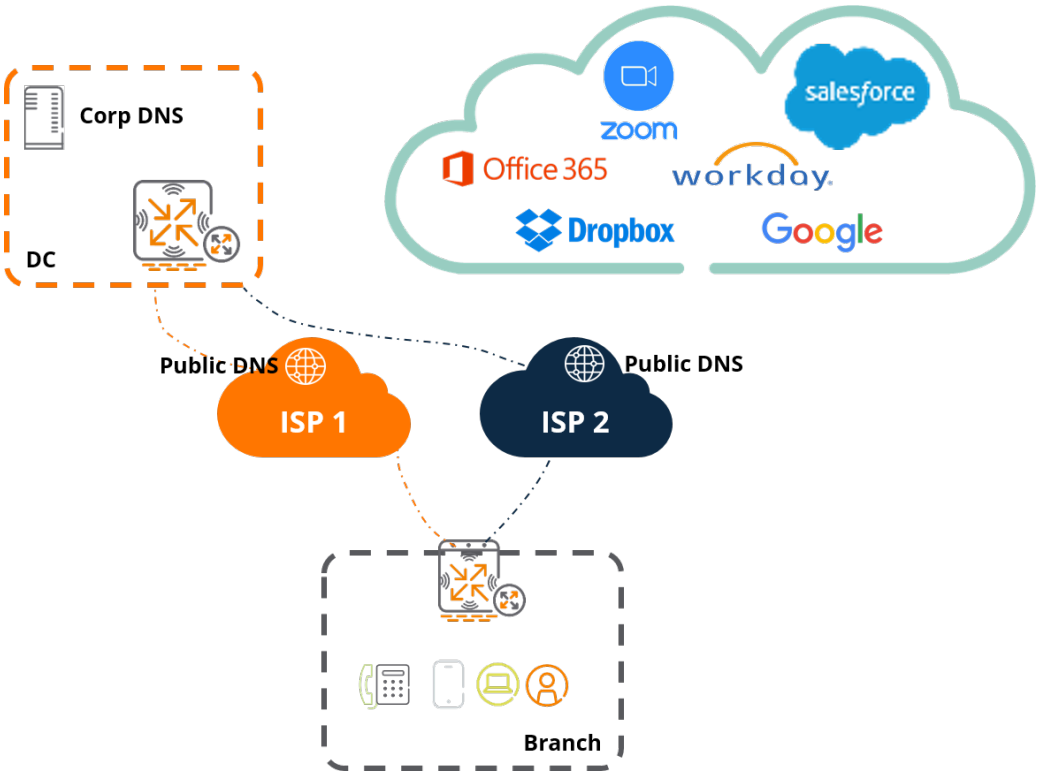
The synthetic probe works similarly like the underlay health checks. Probes are sent through every uplink interface configured in SaaS Express to all optimized (every 60 seconds) and monitored-only (every 10 seconds) applications. The SD-Branch versions 8.7.0.0-2.3.0.0 probes take the underlay path.

The DNS component is a little different as there are potential overlaps with other mechanisms. Firstly, Branch Gateways do not do DNS Snooping for only SaaS applications, this can be done for any type of session and has been enabling name-based firewall aliases in ArubaOS. When configuring PBR policies to locally breakout SaaS traffic, name-based aliases can also be used to locally breakout SaaS traffic. Although it is simpler to use the application group aliases created by SaaS Express, ensure that SaaS Express optimization must be enabled for the application for the *_saas* application group aliases to work.

Secondly, Branch Gateways can also serve as a DNS server for the branch (ArubaOS runs a small *dnsmasq* that can cache up to 150 entries). In such a case, Branch Gateways can selectively redirect DNS requests on a per-domain basis (up to 32 domains) using the Redirect DNS feature. It is configured in **System** > **General** > **DNS**. For more information, see Configuring Redirect DNS Servers.

When using SaaS Express, DNS requests going to the domains corresponding to the applications being optimized, are captured by the Branch Gateway's Data Plane. DNS requests are then proxied to the DNS server that is learned from a given ISP or configured in the SaaS Express Exit Profile. SaaS Express intercepts DNS requests in the Branch Gateway Data Plane and takes precedence over DNS redirect.

Figure 242 *Control plane—SaaS front door*



Data Plane Integration

In a data plane with data traversing the gateway, the following components are related to the SaaS traffic traversing the Branch Gateways:

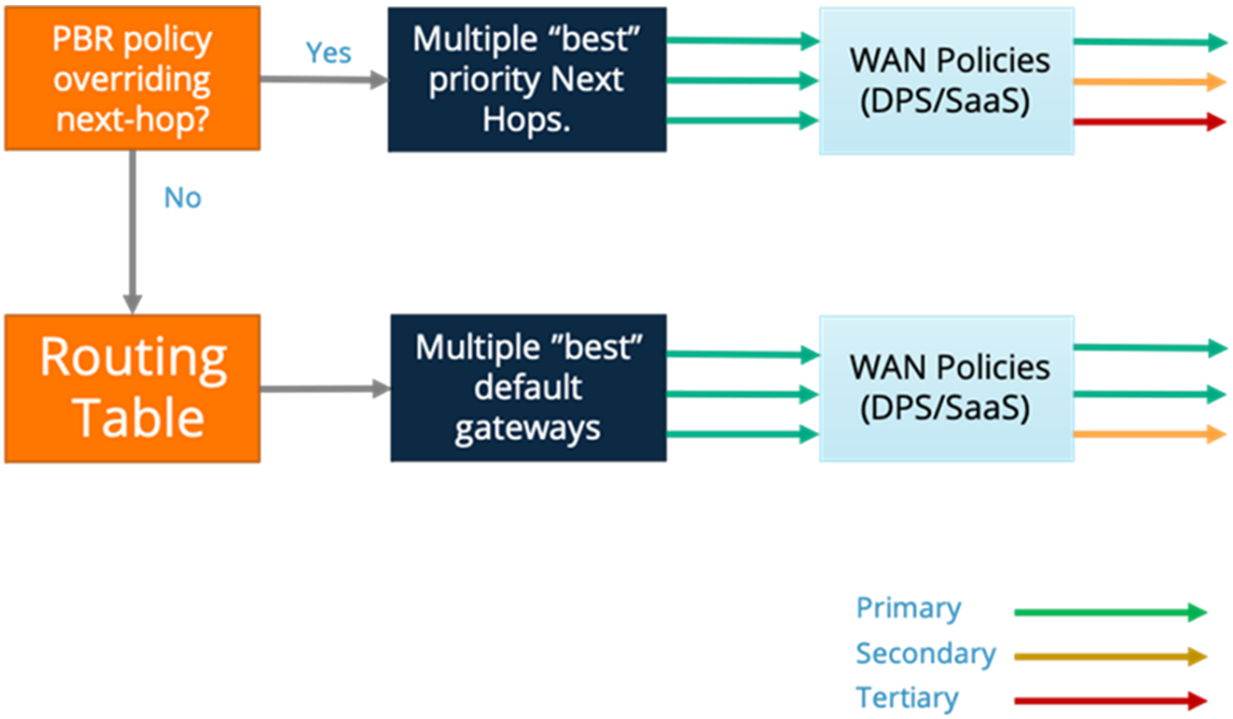
- Security: Firewall policies potentially leveraging applications defined by SaaS Express.
- Routing: PBR influences the paths or next-hops that are available for the application, while routing defines a set of best routes (or default gateways).
- WAN policies (which includes DPS and SaaS Express) choose between the best routes provided by PBR or rRouting.

For the security component, SaaS Express requires Advanced subscriptions, and the fact that these may not be present in all the members of a group (where security policies are defined), complicates the use of the _*saas* aliases. As a result, SaaS Express aliases are not available for use in session ACLs.

The global routing in combination with PBR determines the next hop(s). It provides up to four active (best cost/priority) paths to the WAN engine. WAN policies (SaaS/DPS) determines which path must be taken for each traffic flow. For SaaS Express to be effective, traffic for the optimized SaaS applications must locally breakout. Therefore, routing must determine the next hop and WAN must choose the path(s).

When SaaS and DPS policies coexist, SaaS policies always get index, 1-32, while DPS policies get index, 33-64. SaaS Express policies therefore always take precedence over DPS policies for any traffic going to the domains or IP addresses associated with the SaaS application being optimized.

Figure 243 *Data plane—Policy Based Routing*



Deployment Scenarios

The following are examples of SaaS Express deployment scenarios:

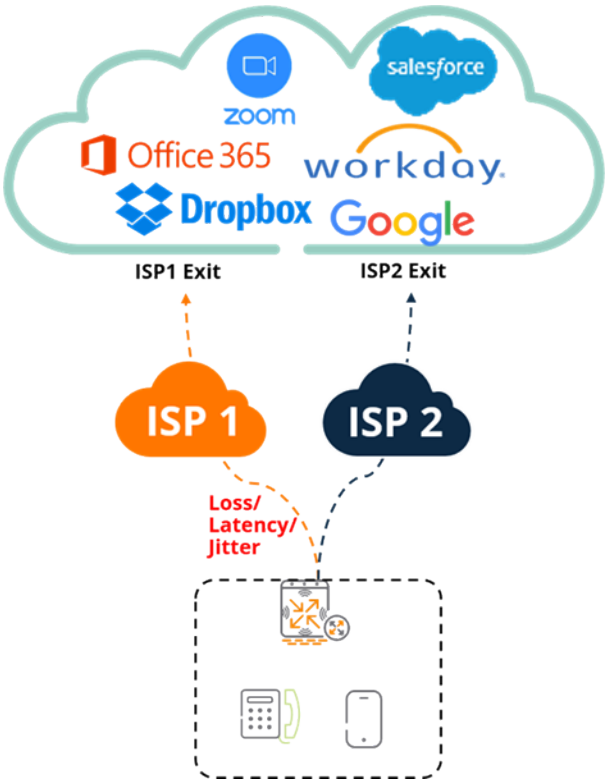
- Single Branch Gateway with multiple ISP Circuits
- Between Dual Branch Gateways with Branch HA (uplink sharing)
- Dual Branch Gateways Without Uplink Sharing

Single Branch Gateway with multiple ISP Circuits

The most straightforward scenario is that of a Branch Gateway with multiple ISP circuits. In this scenario, based on the measured performance and SLA threshold profile configured for the SaaS application, the Branch Gateways determine the optimal path and route for the designated SaaS application using the best available ISP circuit.

The following diagram illustrates SaaS traffic steering from a branch site with multiple ISP circuits.

Figure 244 *Branch Gateway with multiple ISP*

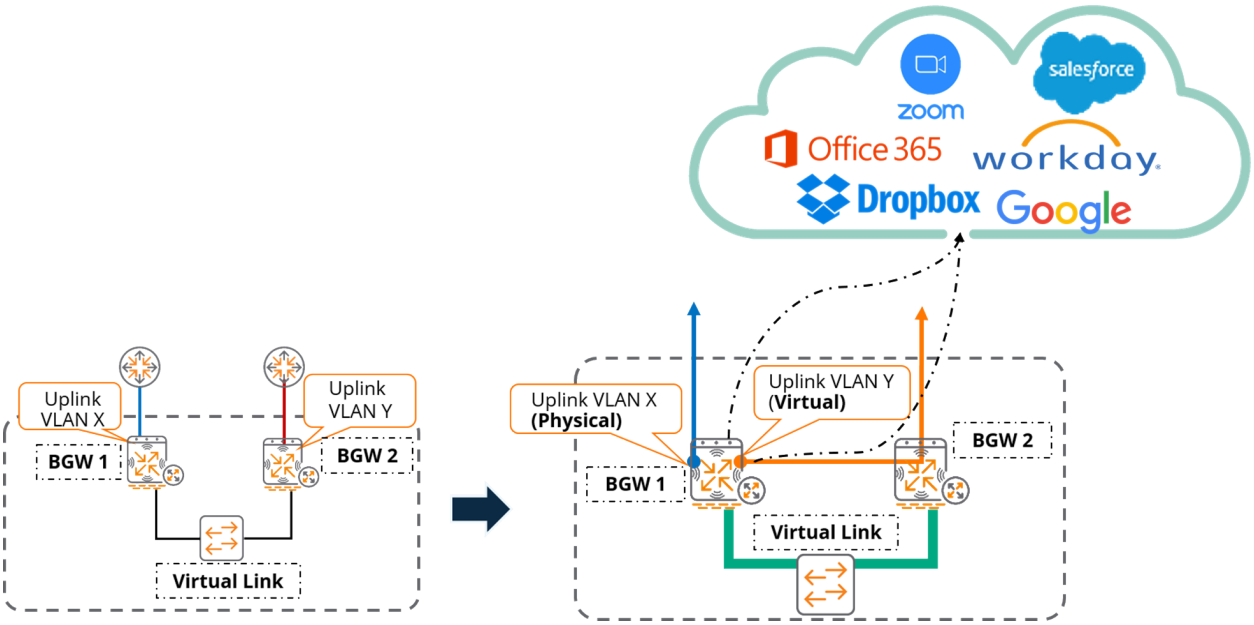


Between Dual Branch Gateways with Branch HA (uplink sharing)

The SaaS Express feature on Branch Gateway supports uplink sharing between Branch Gateways. To enable uplink sharing, Branch HA has to be enabled, and different WAN VLANs should be used to identify the uplinks. The result of that will be that Branch Gateways will build a virtual link between them to share any uplinks that are only physically present in one of the gateways.

The following diagrams illustrate how to set the WAN configuration as well as how the SaaS traffic would be routed in such a scenario.

Figure 245 *Branch Gateways With Uplink Sharing*

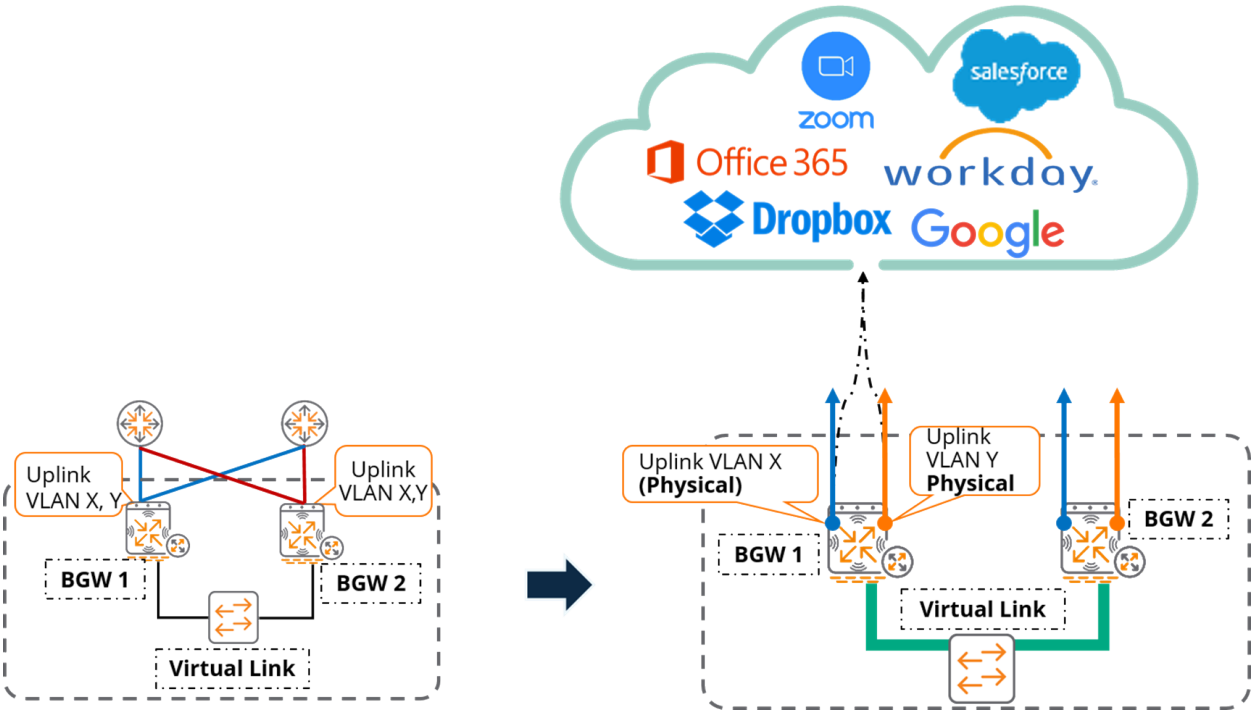


Dual Branch Gateways Without Uplink Sharing

There may be certain scenarios where one or all the uplinks are connected to both Branch Gateways. In those cases, enabling Branch HA would still make sense (for DHCP state sync or other purposes), but uplink sharing may not. To prevent gateways from sharing their uplink, set the same VLAN id on both gateways when connecting to a common uplink:

The following diagram illustrates how to set the WAN configuration as well as how the SaaS traffic is routed in such a scenario.

Figure 246 *Branch Gateways Without Uplink Sharing*



Configuring SaaS Express

The following topics are discussed in this section:

Prerequisites

- SaaS Express feature requires Advanced Gateway license. For more information, see Aruba Central License Feature Details.
- SaaS Express is only supported on the Branch Gateway. For more information, see Provisioning Aruba Gateways.
- The Branch Gateway must be running ArubaOS 8.4.0.0-1.0.6.0 or a later software version. However, the SaaS Express feature has been evolving over time and all the capabilities described in this guide may not be available on older versions. The content of this guide is based on running SaaS Express with ArubaOS 8.7.0.0-2.3.0.0. For more information on how to upgrade, see Updating Software Images on Aruba Gateways.

Best Practices

- Ensure that you assign a site to the gateway before enabling SaaS Express. If you assign the site after enabling SaaS Express, you can view the site in the monitoring dashboard only after two hours.
- Ensure the Deep Packet Inspection (DPI) is enabled on Branch Gateway groups. By default, the DPI is enabled on Branch Gateway groups. For more information, see Using Deep Packet Inspection.
- Ensure the uplink interfaces are configured and the wired uplink is functional. For more information, see Configuring Uplinks.
- Ensure the **App Performance Monitoring** and **DHCP Performance Monitoring** options are enabled on the Branch Gateways. For more information, see Configuring Global Firewall Parameters.

Configuring a Custom SaaS Application Profile

You can create a profile for a custom SaaS application as per your requirement even if it is not available in Aruba Central. You can create up to five custom applications.

To create a custom SaaS application profile, complete the following steps:

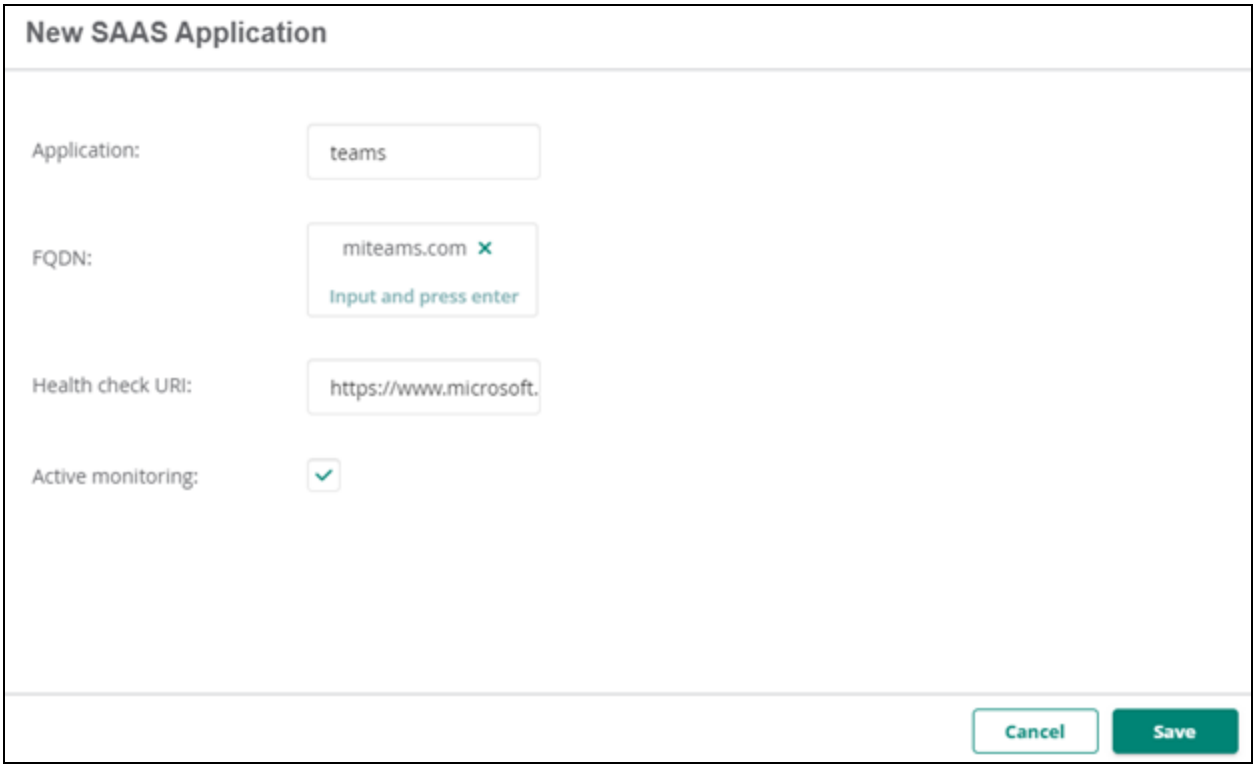
1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for all devices are displayed.
2. Under **Manage**, click **Applications** > **SaaS Express**.
   The map view of the SaaS Express dashboard is displayed.
3. Click the **Config** icon.
   The SaaS Express configuration page is displayed.
4. In the **SAAS applications** table, click **+** to add a new application profile.
5. In the **New SaaS Application** window, configure the following parameters:

- **Application**—Enter the name of the application that you want to configure.
- **FQDN**—Add the FQDN of the SaaS application site.
- **Health check URI**—Enter the health check probe URI. Branch Gateways use the health check probe URI to gather a set of servers for the SaaS application.
- **Active Monitoring**—Select this check box if you only want to monitor the performance of the SaaS application. You can view the performance scores in the monitoring dashboards. For monitoring the SaaS application performance, see Monitoring SaaS Express.

6. Click **Save**.

The following figure illustrates the custom SaaS application profile creation workflow:

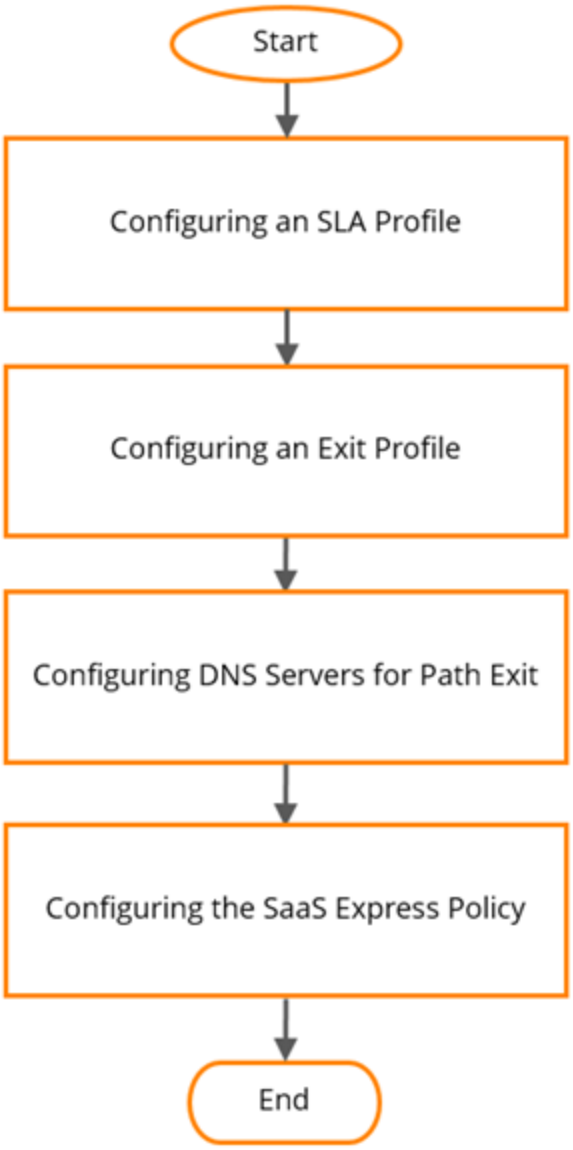
Figure 247 *Custom SaaS Application Creation Workflow*



SaaS Express Configuration Workflow

The following workflow explains the process to configure SaaS Express to route the SaaS application traffic to the best available path.

Figure 248 *Configuration Workflow for SaaS Express*



Workflow Steps

The following steps provide a brief description of the task purpose in each step:

1. Configure an SLA Profile—Set a threshold value for the latency, jitter, packet loss, and uplink utilization parameters.
2. Configure an Exit Profile—Define a primary link for all SaaS application traffic, and secondary and tertiary uplinks as fallback options, if the primary path does not meet the criteria for configured SLA of the SaaS application.
3. Configure the DNS Server for Path Exit—Specify the Branch Gateway as the DNS server for SaaS application FQDN resolution by defining the DNS server for that uplink.

4. Configure a SaaS Express Policy—Create a policy for a SaaS application that is present in Aruba Central using the parameters defined in the first three steps.

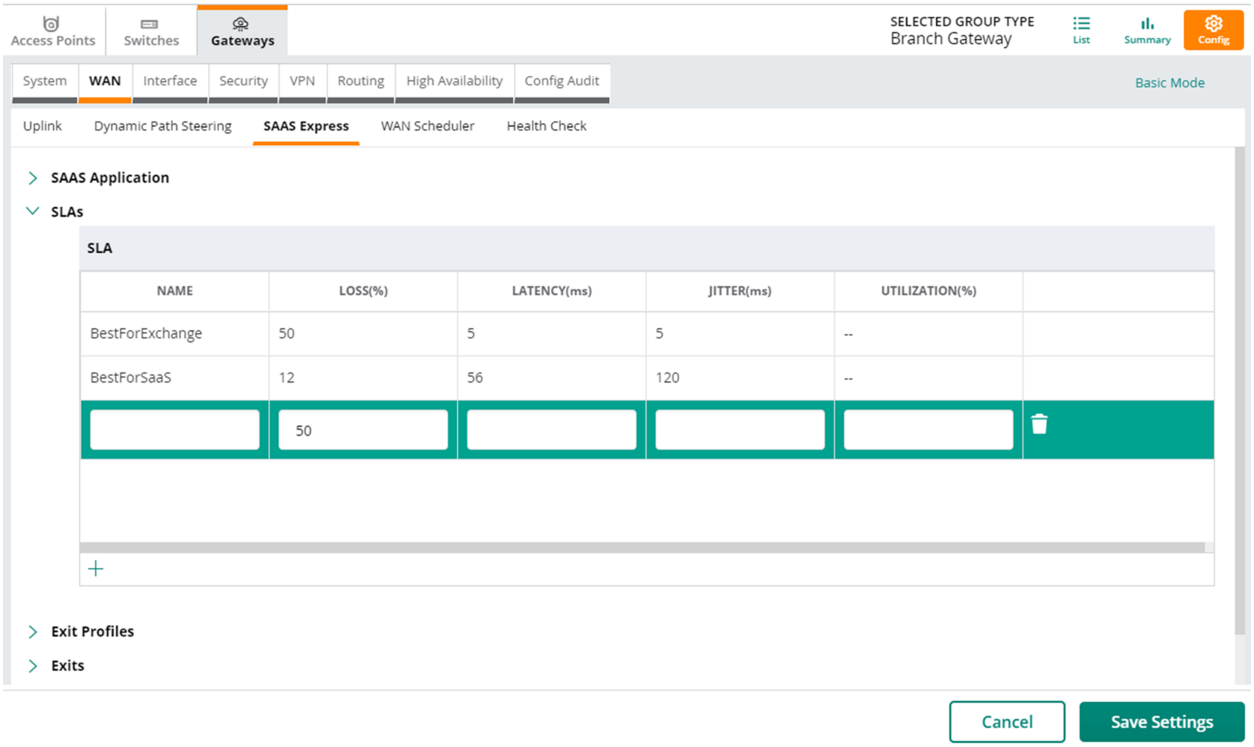
Step 1: Configuring an SLA Profile

An SLA profile defines a threshold value for path performance indicators such as latency, jitter, packet loss, and uplink utilization. To determine if the path meets the performance criteria, Branch Gateways use the loss, latency, and jitter information fetched from the HTTP probes. Branch Gateways determine the optimal path that meets the criteria defined in the SLA profile for the SaaS application.

To set SLA parameters for a SaaS application profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed. The SaaS SLA profile configuration is available in the **Advanced Mode**.
4. Click **WAN** > **SAAS Express**.
5. Click **SLAs**. By default, the Branch Gateway includes the **BestForSaas** exit profile.
6. To add a new SLA profile, click **+** in the **SLAs** table.
7. Configure the following performance indicators:
   - **Name**—Name of the service. By default, **BestForSaaS** is selected.
   - **Loss %**—To measure packet loss. You can set a specific percentage of packet loss allowed for the traffic type.
   - **Latency (ms)**—To measure the round-trip ping time. You can set a threshold value in milliseconds.
   - **Jitter (ms)**—To measure if the packets are delivered in an appropriate order. You can set a threshold value in milliseconds to observe jitters in packet transmission.
   - **Utilization%**—To measure the percentage of bandwidth utilization. You can set a specific percentage of bandwidth utilization as a metric to prioritize and load-balance the traffic.
8. Click **Save Settings**

Figure 249 *SLA Profile Creation*



Step 2: Configuring an Exit Profile

The exit profile defines a primary link (or a set of primary links) for the SaaS application traffic, as well as optional secondary and tertiary uplinks in case the primary uplink(s) do not meet the SLA configured for the SaaS application. By default, the **BestforSaaS** exit profile is available on the Branch Gateways.

To configure an exit profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.

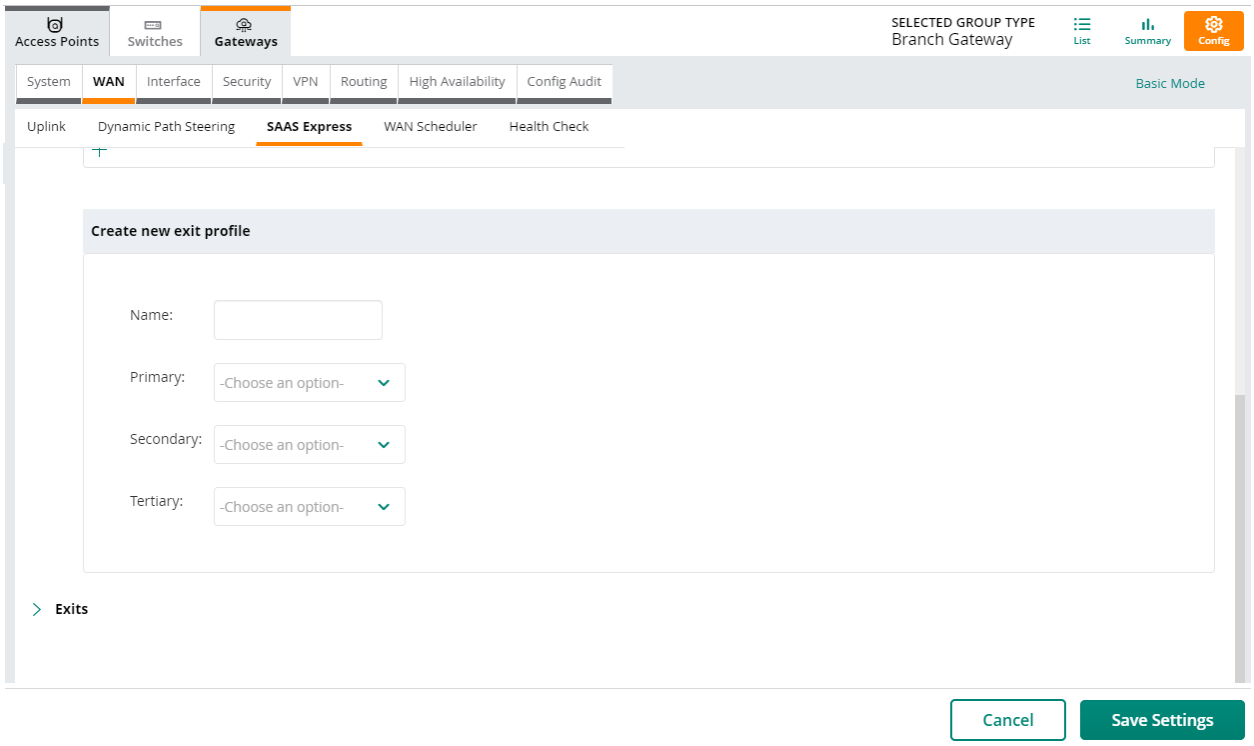
   The gateway group configuration page is displayed. The SaaS exit profile configuration is available in the **Advanced Mode**.
4. Click **WAN** > **SAAS Express**.
5. Click **Exit Profiles**. By default, Branch Gateways include the **BestForSaas** exit profile.
6. To add a new exit profile, click **+** in the **Exit Profile** table.

   The **Create New Exit Profile** section is displayed.
7. Select an uplink path from the available list of uplinks:
   - **Name**—Specify a name for the exit profile.
   - **Primary Path**—A primary uplink path for steering traffic. You can select multiple uplink IDs in a sequential order. When multiple primary paths are configured, the traffic is load-balanced across all primary paths that meet the configured SLA.

- **Secondary Path**—A secondary uplink path for steering traffic. To configure a secondary path, select the uplink type or ID. When a session is steered to a secondary path, it stays on the link until the end irrespective of the status of the primary path. When a primary path becomes active and meets the configured SLA, the new sessions are steered back to the primary path.
- **Tertiary Path**—The third uplink path is a last attempt to steer traffic (when both primary and secondary paths are down). When a session is steered to a tertiary path, it stays on the link until the end. When a primary path becomes active and meets the configured SLA, the new sessions are steered back to the primary path.

8. Click **Save Settings**.

Figure 250 *Exit Profile Creation*



Step 3: Configuring DNS Servers for Path Exit

When a client at a branch site initiates a DNS query to a SaaS application, the Branch Gateway intercepts the DNS query, acts as a proxy, and forwards the query to the DNS server. You can allow the gateway to use the DNS server(s) learned from the ISP through DHCP, or you can configure the DNS server for the SaaS application FQDNs by defining the DNS server for that uplink in the **Exits** table.

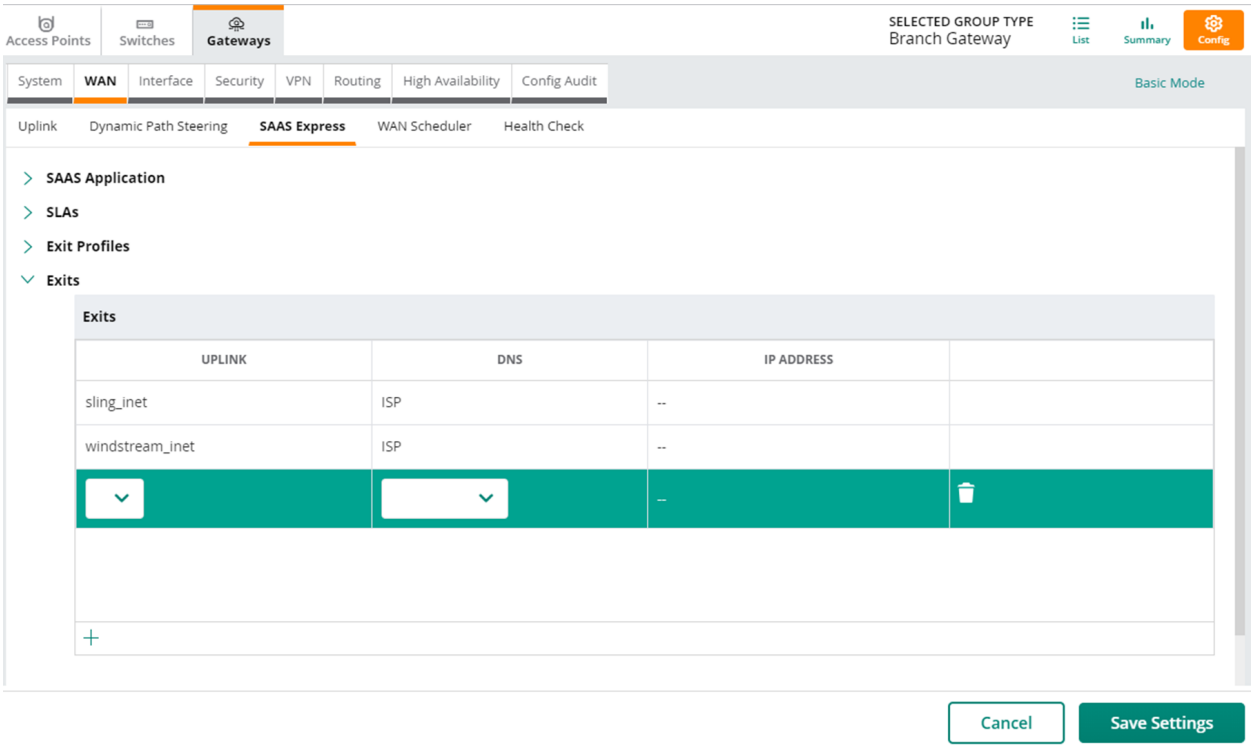
To configure the DNS server details:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed. The SaaS exit configuration is available in the **Advanced Mode**.
4. Click **WAN** > **SAAS Express** > **Exits**.

5. To add a new exit profile, click **+** in the **Exits** table.
6. In the **Uplink** column, select an uplink from the drop-down list.
7. In the **DNS** column, select one of the following options:
   - **IP address**

     If you select **IP address**, enter the DNS server IP address.
   - **ISP DNS**
8. Click **Save Settings**.

Figure 251 *Specifying DNS Server*



Step 4: Configuring the SaaS Express Policy

You can create a policy for a SaaS application that is present in Aruba Central. By default, Branch Gateways support a set of applications and application categories. The built-in application and application category lists include a set of SaaS applications; for example, Adobe, DropBox, Amazon, Google, Salesforce, Slack, Webex, and so on. A default application profile is configured for the SaaS applications that are already available on the Branch Gateways.

To create a SaaS Express policy, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.

   The gateway group configuration page is displayed. SaaS Express configuration is available in both the **Basic Mode** and **Advanced Mode**. The **Advanced Mode** is recommended as it provides all the options.

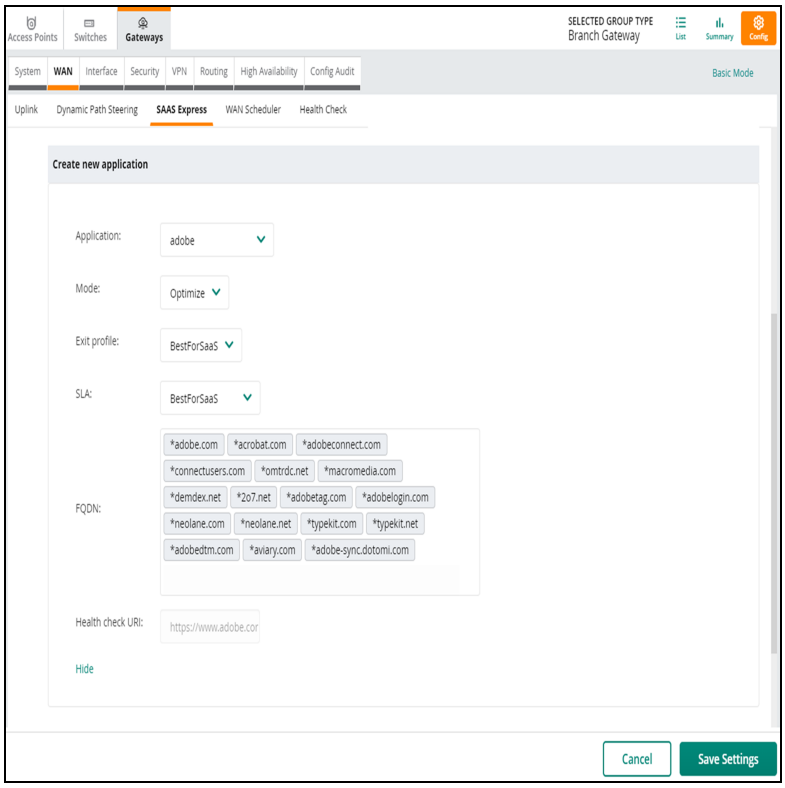
4. Click **WAN** > **SAAS Express**.
5. Click **SAAS Application**.
6. In the **SAAS application with optimized routing** table, click **+** to add a new application profile.

   The **Create New Application** section is displayed.
7. Configure the following parameters:
   - **Application**—Select the application from the drop-down list.
   - **Mode**—Select one of the following modes of deployment for the SaaS application:
     - **Optimize**—Optimizes the performance of the SaaS application by steering traffic and finding the best exit for the SaaS application (This option requires an Advanced Gateway license). The probing frequency used in this mode is two probes for every 10 seconds.
     - **Monitor**—Monitors the SaaS application performance by actively probing the application probe-URI to gather performance statistics on all the available uplinks. However, the performance of your SaaS applications is not optimized. The probing frequency used in this mode is two probes for every 60 seconds.
   - **Exit Profile**—Select an exit profile. The exit profile allows you to define an exit criterion for SaaS application traffic based on the best available path. The exit profile defines a primary link for all SaaS application traffic, and secondary and tertiary uplinks as fallback options if the primary path does not meet the SLA configured for the SaaS application. By default, the **BestforSaaS** exit profile is available on Branch Gateways. You can also configure a custom exit profile and associate it with the SaaS application profile.
   - **SLA**—Select an SLA profile.

     Click **show more** to display all the parameters.
   - **FQDN**—Add the FQDN of the SaaS application site.
   - **Health check URI**—Enter the health check probe URI. Branch Gateways use the health check probe URI to gather a set of servers for the SaaS application.
8. Click **Save Settings**.

The following figure illustrates the predefined SaaS application profile creation workflow:

Figure 252 *SaaS Express Policy Creation*



To know how to monitor your SaaS applications, see Monitoring SaaS Express .

Modifying the PBR Policy

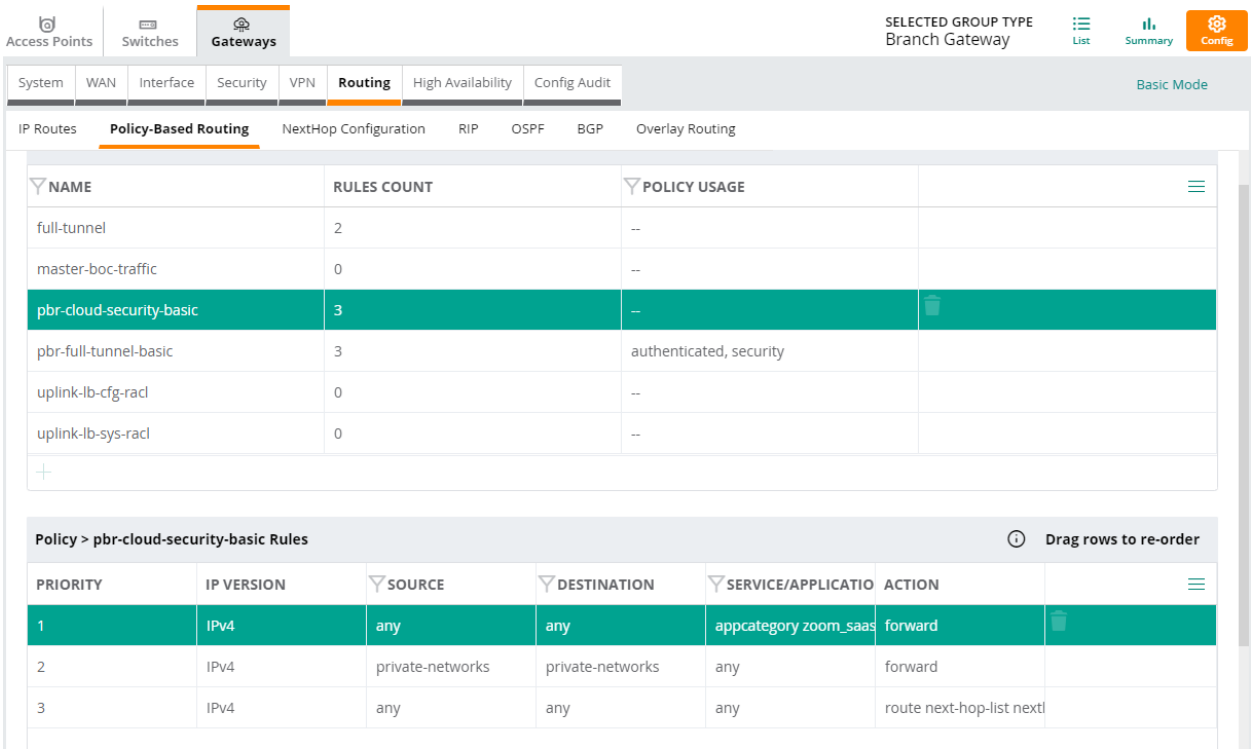
As described in the Design and Deployment section, though PBR is not strictly a part of the SaaS Express configuration, it is still inherently associated. For some roles or VLANs where the PBR policies are sending the traffic through a data center (full tunnel) or a cloud security partner, you must ensure that the SaaS applications are excluded from getting tunneled.

For more information about how to modify a PBR policy, see Configuring Policies for PBR.

To modify a PBR policy:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed. SaaS Express configuration is available in both the **Basic Mode** and **Advanced Mode**. The **Advanced Mode** is recommended as it provides all the options.
4. Click **Routing** > **Policy-Based Routing**.
5. Select the required PBR policy for the SaaS application that is configured for optimized routing.
6. Select the **Forward Regularly** option from the **Action** drop-down.

Figure 253 *Forward Regularly for PBR*



Troubleshooting Resources

The other resources for verifying the behavior of SaaS applications apart from the information provided by the monitoring dashboards are the data in the **Sessions** tab for the gateway and the troubleshooting commands in the **Tools** tab for more advanced issues.

The following topics are discussed in this section:

- Viewing Gateway Session Details
- Using Troubleshooting Commands

Viewing Gateway Session Details

The **Session Details** drop-down in the **Sessions** tab provides session-specific information for an application. For more information, see The Sessions Tab.

Navigating to the Sessions Tab

To navigate to the **Sessions** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

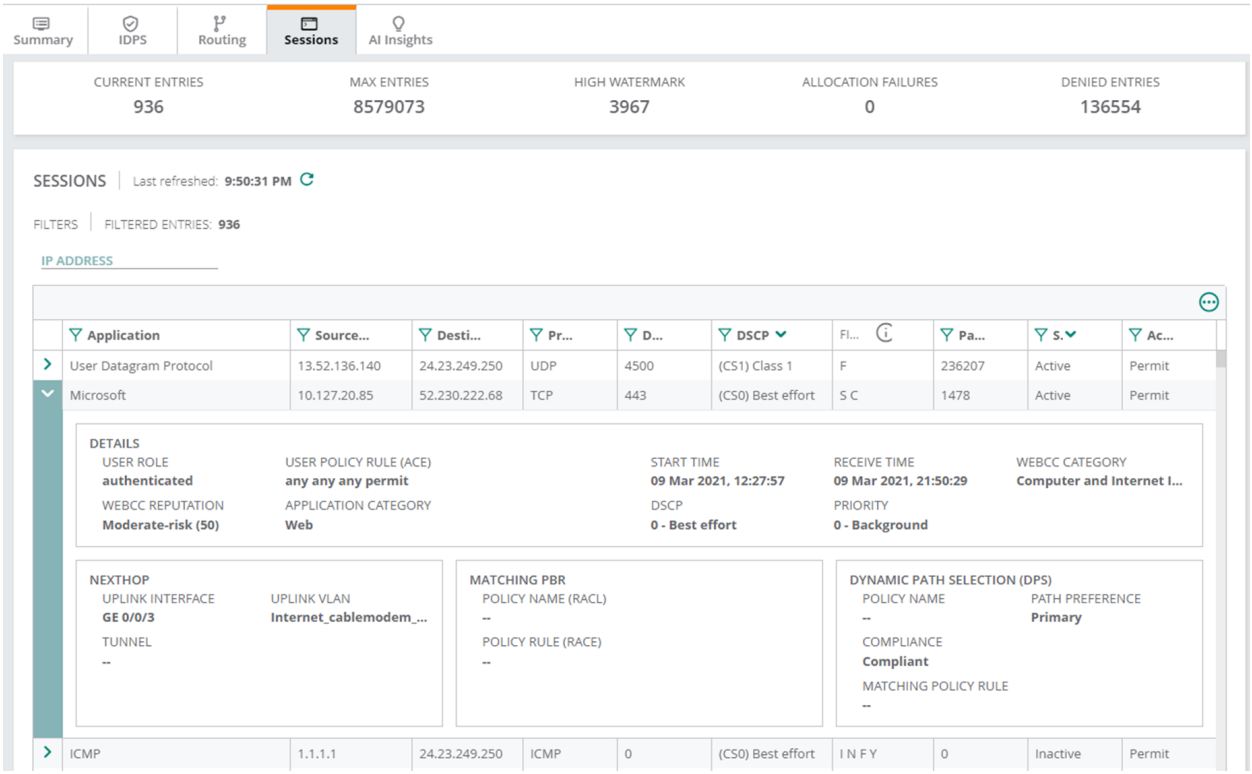
   The dashboard context for the specific gateway is displayed.

4. Under **Manage**, click **Overview** > **Sessions**.

   To exit the gateway dashboard, click the back arrow on the filter.

The following image illustrates the **Session Details** information.

Figure 254 *Gateway Session Details*



Using Troubleshooting Commands

The **Tools** menu in Aruba Central allows network administrators and users with troubleshooting permission to perform troubleshooting or run diagnostics tests on devices and networks managed by Aruba Central. For more information, see Using Troubleshooting Tools. The Commands tab allows you to perform a network health check on devices at an advanced level using command categories. Read-only users can also perform advance checks. For the list of all CLIs, output examples, and descriptions, see The CLI Bank.

Navigating to the Commands Tab

To navigate to the **Commands** tab:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.

c. Click a gateway listed under **Device Name** for which you want to perform a diagnostic test.

   The dashboard context for the gateway is displayed.

2. Under **Analyze** > **Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Gateway**.
4. From the **Available Devices** drop-down list, select the gateway. You can select multiple gateways.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. Click **Run**.

   The output is displayed in the **Device Output** section. For more information, see Troubleshooting Gateways.

CLIs for Verifying Configurations

For the users who want to investigate SaaS Express using the CLI for troubleshooting, the following commands, and their outputs are the key to verify configurations.

SaaS Application Configurations and Policies

It is best to start with reviewing the SaaS Express configured policies.

- `show saas app-list all`

  Use this command to view the SaaS applications that are enabled. A list of default SaaS applications defined in Aruba Central are listed and the **Enabled** column in the output indicates whether the application is disabled or enabled.

The following example displays the output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host)#show saas app-list all
SaaS Custom App Table
App Name  App ID  Mode      Probe Profile
intuit    12      DISABLED  saas_intuit_pp
oracle    14      DISABLED  saas_oracle_pp
zendesk   5       DISABLED  saas_zendesk_pp
zoom      18      MONITOR   saas_zoom_pp
google    2       MONITOR   saas_google_pp
box       7       DISABLED  saas_box_pp
slack     11      DISABLED  saas_slack_pp
amazon    6       DISABLED  saas_amazon_pp
adobe     10      MONITOR   saas_adobe_pp
netflix   28      DISABLED  saas_netflix_pp
webex     9       DISABLED  saas_webex_pp


Threshold Profile  Wan Policy      Pathsteer Profile
```

```
BestForSaaS        ---             BestForSaaS
BestForSaaS        ---             BestForSaaS
BestForSaaS        ---             BestForSaaS
SaaS-LTE           saas_zoom_wp    SaaS-LTE
BestForSaaS        saas_google_wp  BestForSaaS
BestForSaaS        ---             BestForSaaS
BestForSaaS        ---             BestForSaaS
BestForSaaS        ---             BestForSaaS
BestForSaaS        saas_adobe_wp   BestForSaaS
BestForSaaS        ---             BestForSaaS
BestForSaaS        ---             BestForSaaS
```

- `show saas app-list all <application name>`

  Use this command to view the ID for a specific application. The application ID displayed in the output is required for troubleshooting the application classification.

The following example displays the output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show saas app-list zoom
SaaS Custom App Table
App Name  App ID  Mode     Probe Profile  Threshold Profile
zoom      18      MONITOR  saas_zoom_pp   SaaS-LTE

Wan Policy    Pathsteer Profile
saas_zoom_wp  SaaS-LTE
```

- `show wan probe-profiles`

  Use this command to check the probe profile created for the configured SaaS application. The output displays the dynamically created probe profiles for the applications along with their respective health check URI.

The following example displays the output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show wan probe-profiles
Probe profiles
Name                        FQDN/IP                  Ref URI
saas_slack_pp               slack.com
HighlyAvailable             vpnc(Not resolved)
saas_zendesk_pp             www.zendesk.com          login/
saas_amazon_pp              www.amazon.com
```

```
saas_office365_pp            sdwan.measure.office.com  apc/trans.gif
saas_gotomeeting_pp          www.gotomeeting.com       meeting/join-meeting
saas_skype_teams_pp          sdwan.measure.office.com  apc/trans.gif
saas_concur_pp               www.concursolutions.com   nui/signin
saas_salesforce_pp           login.salesforce.com
saas_sharepoint_onedrive_pp  sdwan.measure.office.com  apc/trans.gif
saas_box_pp                  account.box.com           login
BestForVoice                 vpnc(Not resolved)
saas_dropbox_pp              www.dropbox.com           login
saas_intuit_pp               www.intuit.com            sign-in/
saas_exchange_pp             sdwan.measure.office.com  apc/trans.gif
saas_zoom_pp                 zoom.us
BestForInternet              0.0.0.0
saas_google_pp               www.google.com
saas_webex_pp                www.webex.com             manage/myaccount/index.html
saas_netflix_pp              fast.com
saas_oracle_pp               www.oracle.com            index.html

Mode  Frequency  Retries  Burst-Size  Jitter Enabled
http  10         3        2           TRUE
Ping  10         3        5           FALSE
http  10         3        2           TRUE
http  10         3        2           TRUE
http  10         3        2           TRUE
http  60         3        2           TRUE
http  10         3        2           TRUE
http  10         3        2           TRUE
http  10         3        2           TRUE
http  10         3        2           TRUE
http  10         3        2           TRUE
Ping  10         3        5           FALSE
http  60         3        2           TRUE
http  10         3        2           TRUE
http  60         3        2           TRUE
http  60         3        2           TRUE
Ping  10         3        5           FALSE
http  60         3        2           TRUE
http  10         3        2           TRUE
http  10         3        2           TRUE
http  10         3        2           TRUE
```

- `show wan policy-list`

  Use this command to check which WAN policy profile is created for the configured SaaS application. The user traffic is routed based on this profile. The WAN policy profile is dynamically created.

The following example displays the output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show wan policy-list
WAN Policy Table
Index  Policy Name  PrimaryGroup  BackupGroup1  BackupGroup2  BackupGroup3
1      default      all_inet      all_lte
1      any          any           any                         4

FallbackGroup  Threshold        Probe  Priority  Source  Destination  Service
               BestForInternet

Application  DSCP  IPv4/6
```

- `show saas threshold-profile`

  Use this command to view all the threshold profiles that are configured in Aruba Central for SaaS applications.

The following example displays the output of the command.

```
(host) #show saas threshold-profile
Name         ID  Latency  Jitter  Packet-Loss  BW-Utilization  mos
BestForSaaS  1   0        120     0            0               0
SaaS-LTE     2   200      50      20           0               0
```

- `show saas path-steer-profile`

  Use this command to verify the exit profiles of the SaaS applications.

The following example displays the output of the command.

```
(host) #show saas path-steer-profile
SaaS Pathsteer Profiles
Profile Name  prigrp_name      bkpgrp1_name  bkpgrp2_name  bkpgrp3_name  fbgrp_name
BestForSaaS   all_uplinks
concur        cablemodem_inet  cellular_lte
SaaS-LTE      all_inet         all_lte
```

SaaS DNS Configuration

DNS is an essential element of any SaaS communication, so proxy-DNS must also be given the same importance.

- `show saas dns-list`

  Use this command to verify that the DNS probes are set and see the server IPs discovered by the probes. The out displays all the DNS probes sent by the Branch Gateway and the client.

The following example displays the partial output of the command.

```
(host) #show saas dns-list
SaaS DNS Server Table
Index
1
75.75.75.75  cablemodem_inet  4086  DHCP
skype_teams (16)
https://sdwan.measure.office.com/apc/trans.gif (PRBE)  [2021-01-21 11:07:15]
13.107.128.7               [2021-01-21 11:07:15]
http://trouter2-azsc-uswc-2-a.trouter.teams.microsoft.com/ (CLNT)  [2021-01-21
10:55:54]
52.113.207.2               [2021-01-21 10:55:54]
http://us-prod.asyncgw.teams.microsoft.com/ (CLNT)  [2021-01-21 11:02:14]
52.114.159.187             [2021-01-21 11:02:14]
http://go.trouter.teams.microsoft.com/ (CLNT)  [2021-01-21 11:08:45]
52.114.128.202             [2021-01-21 10:23:42]
52.113.207.2               [2021-01-21 11:08:45]
52.113.207.1               [2021-01-21 10:30:24]
52.113.207.0               [2021-01-21 10:38:43]
52.114.158.94              [2021-01-21 10:53:44]
http://eastus-prod-2.notifications.teams.microsoft.com/ (CLNT)  [2021-01-21
10:57:44]
52.114.133.219             [2021-01-21 10:22:33]
52.114.132.128             [2021-01-21 10:27:42]
52.114.132.118             [2021-01-21 10:12:40]
52.114.132.173             [2021-01-21 10:42:43]
52.114.132.134             [2021-01-21 10:30:26]
52.114.132.171             [2021-01-21 10:57:44]
http://presence.teams.microsoft.com/ (CLNT)  [2021-01-21 11:00:54]
52.114.128.90              [2021-01-21 10:11:05]
52.114.133.164             [2021-01-21 10:23:47]
52.114.128.85              [2021-01-21 10:30:25]
52.112.115.29              [2021-01-21 10:30:52]
52.112.115.30              [2021-01-21 11:00:54]
52.114.128.86              [2021-01-21 10:45:53]
Server IP    Uplink           Vlan  Type
0.0.0.0      cablemodem_inet  4086  DHCP (CFG)
```

- `show datapath saas servers`

  Use this command to view the DNS requests.

The following example displays the partial output of the command.

```
(host) #show datapath saas servers
Flags: C - Control Plane installed, D - Data Plane installed
Datapath SAAS Server Entries
Server IP       Port  Proto  App-ID  Flags  Age (sec)
13.107.6.156    0000  0000   1448    CD     38
13.107.136.9    0000  0000   1453    C      1
13.107.6.171    0000  0000   1448    C      18
13.107.21.200   0000  0000   6145    C      18
13.107.5.88     0000  0000   1478    C      59
13.107.42.13    0000  0000   2820    C      28
13.107.6.158    0000  0000   2821    C      25
216.58.217.46   0000  0000   0943    D      44
40.126.26.132   0000  0000   6145    C      29
40.126.26.135   0000  0000   6145    C      3
20.191.46.211   0000  0000   6145    C      17
```

- `show datapath saas fqdn`

  Use this command to view the FQDN for configured SaaS applications.

The following example displays the partial output of the command.

```
(host) #show datapath saas fqdn
Datapath SAAS FQDN Entries
FQDN                              App
platform.linkedin.com             1
live.com                          1
oneclient.sfx.ms                  15
microsoftonline-p.net             1
wns.windows.com                   15
livemeeting.com                   1
azurerms.com                      1
onenote.net                       1
ms.tific.com                      1
view.atdmt.com                    1
microsoftonline-p.com             1
staffhub.uservoice.com            1
```

General Uplink Health

SaaS Express is also a specific type of WAN policy, therefore overall uplink health must also be looked into.

- `show ip health-check`

  Use this command to check the HTTP probe status and which HTTP probes are set. The output also displays all the responses received for the HTTP probes. The **State** column in the output displays if the configuration is **Up** or **Down**. The value in the **MOS** column of the output indicates that higher values of the uplink are the best paths.

The following example displays the output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show ip health-check
IP Health-check Entries
Probe IP       Src Interface  Vpnc IP         State  Probe-Profile
24.23.248.1                                   Up     default
10.127.11.2    vlan 4086      104.36.251.41   Up     data-vpnc
10.127.11.2    vlan 4095      104.36.251.41   Up     data-vpnc,lte-uplink
13.107.128.7   vlan 4086                      Up     saas_skype_teams_pp
100.84.162.17                                 Down   default,lte-uplink
52.52.253.87   vlan 4086                      Up     health-check
52.52.253.87   vlan 4095                      Up     health-check,lte-uplink
10.128.25.106  vlan 4086      44.229.21.219   Up     data-vpnc
10.128.25.106  vlan 4095      44.229.21.219   Up     data-vpnc,lte-uplink
10.128.25.107  vlan 4086      54.185.111.127  Up     data-vpnc
10.128.25.107  vlan 4095      54.185.111.127  Up     data-vpnc,lte-uplink

Latency(ms)  Jitter  Loss(%)  MOS
0.000                0
7.200        0.288   0        4.4
20.500       0.000   0        4.4
11.142       0.500   0        4.4
0.000                0
8.600        0.323   0        4.4
21.000       0.000   0        4.4
18.100       0.194   0        4.4
31.000       0.000   0        4.4
17.500       0.133   0        4.4
29.500       0.000   50       1.0
Total Entries: 11
```

- `show ip health-check verbose`

  Use this command to check the reachability of the server IP and view the HTTP status information. The value in the output helps in understanding if the probe sent from the Branch Gateway is redirected or moved.

The following example displays the partial output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show ip health-check verbose
IP Health-check Entries
Probe IP       Src Interface  Vpnc IP         State  Probe-Profile
24.23.248.1                                   Up     default
10.127.11.2    vlan 4086      104.36.251.41   Up     data-vpnc
10.127.11.2    vlan 4095      104.36.251.41   Up     data-vpnc,lte-uplink
13.107.128.7   vlan 4086                      Up     saas_skype_teams_pp
100.84.162.17                                 Down   default,lte-uplink
52.52.253.87   vlan 4086                      Up     health-check
52.52.253.87   vlan 4095                      Up     health-check,lte-uplink
10.128.25.106  vlan 4086      44.229.21.219   Up     data-vpnc
10.128.25.106  vlan 4095      44.229.21.219   Up     data-vpnc,lte-uplink
10.128.25.107  vlan 4086      54.185.111.127  Up     data-vpnc
10.128.25.107  vlan 4095      54.185.111.127  Up     data-vpnc,lte-uplink

Latency(ms)  Jitter  Loss(%)  MOS
0.000                0
7.500        0.316   0        4.4
18.750       0.000   0        4.4
13.908       9.000   0        4.4
0.000                0
9.900        0.552   0        4.4
23.500       0.000   0        4.4
19.000       0.369   0        4.4
30.750       0.000   0        4.4
17.000       0.357   0        4.4
28.500       0.000   0        4.4
Total Entries: 11
Target IP: 10.128.25.107 is reachable Up: 1 Down: 0
Src intf VLAN: 4095, Vpnc IP: 54.185.111.127
Probe mode: Udp, Probe frequency: 15 seconds
Probe Statistics:
Latest Tx Pkts: 2, Rx Pkts: 2, Pkt Loss: 0 (0.00%), Out of Sequence: 0, Drops: 0
Total Tx Pkts: 264, Rx Pkts: 260, Pkt Loss: 4, Out of Sequence: 0, Drops: 0
```

```
Aggressive Probe: Enabled, Cnt: 2, Reqs: 1
Latency:
Latest Latency: 28.500 ms, RTT: 57.000 ms, Number of Samples: 2
Min/Avg/Max: 24.500/28.500/47.000 ms
Jitter:
Latest Jitter: 0.000 ms, RTT: 0.000 ms, Number of Samples: 0
Min/Avg/Max: 0.031/0.000/1.751 ms
MOS quality: 4.4 (Good)
Available Upload Bandwidth (Mbps): 0
Available Download Bandwidth (Mbps): 0
Bandwidth Utilization (MD<->VPNC): Minimum probe frequency 10 seconds
```

- `show wan threshold-stats`

  Use this command to view which nexthop is selected by the Branch Gateway for the SaaS application.

The following example displays the partial output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show wan threshold-stats
Flags: D - default HC/VPNC stats, h - health-check IP,  v - VPNC, c - Cloud
security, C - custom probe, S - SaaS probe, B - best hop, N - non compliant, P -
used by policy
Pkt-Loss Flags: A - aggressive probe, B - blackout
ThrMask  - Mask of all Threshold profiles, (1 << Threshold ID)
VioT     - Mask of Threshold profiles violated
CompT    - Mask of Threshold profiles compliant
PlMask   - Mask of WAN Policies using the stats, (1 << (Priority - 1))
Hold-T/P - Mask of Threshold profiles and WAN Policies in Hold state
BMask    - Mask of WAN Policies using Best uplink stats in the absence of SaaS stats
Threshold statistics
Probe IP        Vpn IP  Uplink  AppID  State  ThrMask  VioT  CompT  Hold-T/P
104.36.251.41           4086           1      1e             1e
13.107.128.7            4086    32     1      4              4
162.125.7.18            4086    35     1      2              2
23.197.50.58            4086    41     1      2
23.197.50.65            4086    32     1      4              4
96.6.238.97             4086    44     1      4              4
172.217.5.100           4086    33     1      2              2
44.229.21.219           4086           1      1e             1e
54.185.111.127          4086           1      1e             1e
35.165.127.27           4086           1      1e             1e
```

```
52.12.7.145             4086          1      1e             1e
3.235.71.132            4086    49    1      4

PlMask    Vio/Comp  Dnlds  Last Download         Latency(ms)  Jitter(ms)
200000000 93/93     144    Mar  9 00:10:24 2021  6.20/150     0.13/50
1         203/203   49772  Mar  9 09:08:09 2021  11.61/200    2.00/50
8         78/78     7241   Mar  9 09:08:08 2021  123.11/0     13.50/120
200       0/0       2      Mar  9 09:08:11 2021  0.00/0       0.00/120
1         2/2       475    Mar  9 09:08:10 2021  11.07/200    2.50/50
1000      8/8       621    Mar  9 09:08:16 2021  71.56/200    1.50/50
2         0/0       28     Mar  9 09:08:08 2021  38.60/0      3.50/120
          64/64     106    Mar  9 00:10:24 2021  15.40/150    0.07/50
          55/55     80     Mar  9 00:10:25 2021  17.40/150    0.48/50
          64/64     108    Mar  9 00:10:24 2021  15.70/150    0.10/50
          64/64     98     Mar  9 00:10:25 2021  15.80/150    0.14/50
20000     0/0       2      Mar  9 09:07:58 2021  0.00/200     0.00/50

Pkt-Loss(%)  MOS(1-5)  Flags
0.00/1       4.40/0    DvP
0.00/20      4.39/0    SPB
0.00/0       3.79/0    SPB
0.00/0       4.40/0    SPB
0.00/20      4.39/0    SP
0.00/20      4.32/0    SPB
0.00/0       4.36/0    SPB
0.00/1       4.39/0    Dv
0.00/1       4.39/0    Dv
0.00/1       4.39/0    Dv
0.00/1       4.39/0    Dv
0.00/20      4.40/0    SPB
```

- `show datapath wan hits`

  Use this command to validate the controller datapath hits. The hits are incremented when the user is accessing the SaaS configured applications.

The following example displays the output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show datapath wan hits
Datapath SDWAN Policy Entries
Flags: 4 - IPV4, 6 - IPV6,  D - Default,P - PathSteer, T - Threshold, d - DPI
```

```
Index  Source      Destination  Service/Application
1:     any         any          appcategory 32
3:     any         any          appcategory 46
4:     any         any          appcategory 47
6:     netdest 38  netdest 38   any
7:     any         any          any

DSCP          PS-P   P-Ver  PS-B1     B1-Ver   PS-B2   B2-Ver
0  *all_inet         1      all_lte   26c2
0   all_inet         1      all_lte   26c2
0  *all_inet         1      all_lte   26c2
0  *all_inet         1      all_lte   26c2
0  *all_inet         1      all_lte   26c2

PS-F   F-Ver TID   PrbIp   Ver  Flags  Hits   LossCorrection
             2             3ba  PTd4   3237
             2             3bc  PTd4   3228
             2             3bd  PTd4   5658
             3             3bf   PT4     17   FEC Always(loss: 5% ratio: 1:4)
             0             3c0    P4   10178
```

Application Identification

Lastly, the application classification must also be checked.

- `show datapath session dpi table`

  Use this command to validate if the branch controller is classifying the SaaS application and verify if the DPI has classified the respective application.

The following example displays the partial output of the command. The actual CLI output in Aruba Central appears as a single table. In this example, the output is modified to appear in multiple sections.

```
(host) #show datapath session dpi table
Datapath Session Table Entries
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
Q - Real-Time Quality analysis
u - Upstream Real-Time Quality analysis
I - Deep inspect, U - Locally destined
E - Media Deep Inspect, G - media signal
```

```
r - Route Nexthop, h - High Value
A - Application Firewall Inspect
i - Session classified on first packet
J - SDWAN Default Probe stats used as fallback
f - FEC Enabled for the Session
X - SDWAN Exception
B - Permanent, O - Openflow
L - Log, o - Openflow config revision mismatched
Source IP or MAC  Destination IP  Prot SPort DPort Cntr     Prio ToS Age Destination
194.169.14.254    194.169.14.1    1    37164 0     0/0      0    0   2   local
142.142.0.1       194.169.14.254  1    14000 2048  0/0      0    0   2   tunnel 9
194.169.14.254    194.169.14.1    1    13992 0     0/0      0    0   2   tunnel 9
193.168.2.254     142.142.0.2     1    25932 0     0/0      0    0   2   local
194.169.14.254    194.169.14.1    1    37156 0     0/0      0    0   2   local
13.52.136.140     172.16.50.9     17   4500  4500  0/0      0    48  0   local
142.142.0.4       40.87.19.190    6    50580 443   0/0      0    0   2   local
142.142.0.4       52.206.67.231   6    64265 443   0/0      0    0   1   local
193.168.2.254     142.142.0.2     1    25940 0     0/0      0    0   2   local

TAge  Packets    Bytes      AclVer   Int-Flag Sess-Flag2 PktsDpi   UplnkVlan
20    1          28         0        0        10         0         4092
18    1          28         96a      404001   10         0         4092
19    1          28         0        404000   10         0         4092
20    1          28         0        0        0          0         none
21    1          28         0        0        10         0         4092
da39  27235      4139720    0        800000   0          0         4106
19d9  330        24319      96a      200802b5 18         0         4092
3847  5215       402047     96a      20808a5  18         3         4092
20    1          28         0        0        0          0         none

AppID                    AceIdx      Flags            DpiTIdx CPU ID  ASliceId
                 (0   )  0/0     /0  FI               88      1       31
                 (0   )  0/0     /0  FSCI             39      1       31
                 (0   )  0/0     /0  FNI              11a     1       31
                 (0   )  0/0     /0  FI               2c      1       31
                 (0   )  0/0     /0  FI               8       1       31
                 (0   )  0/0     /0  F                c1      1       31
skype_teams_saas (6160)  301/301 /8  SCi              d8      1       31
amazon           (968 )  301/301 /8  SC               106     1       8
                 (0   )  0/0     /0  FI               14a     1       31
```

- `show saas fastdpi-prefix-list`

  Use this command to validate if the Branch Gateway is downloading the list of Microsoft prefixes from the fastdpi service.

The following example displays the partial output of the command.

```
(host) #show saas fastdpi-prefix-list
SAAS FastDpi Prefix-list Table
App-ID  zone          Prefix           Mask             Proto  Port
1       USGovGCCHigh  40.66.16.0       255.255.248.0    0      0
1       USGovGCCHigh  131.253.83.0     255.255.255.192  0      0
1       USGovGCCHigh  131.253.84.64    255.255.255.192  0      0
1       USGovGCCHigh  131.253.84.192   255.255.255.192  0      0
1       USGovGCCHigh  131.253.86.0     255.255.255.0    0      0
1       USGovGCCHigh  131.253.87.144   255.255.255.240  0      0
1       USGovGCCHigh  131.253.87.208   255.255.255.240  0      0
1       USGovGCCHigh  131.253.87.240   255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.0     255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.32    255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.48    255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.96    255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.128   255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.144   255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.160   255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.192   255.255.255.240  0      0
1       USGovGCCHigh  131.253.88.240   255.255.255.240  0      0
1       USGovGCCHigh  13.72.179.197    255.255.255.255  0      0
1       USGovGCCHigh  13.72.183.70     255.255.255.255  0      0
1       USGovGCCHigh  23.103.191.0     255.255.255.0    0      0
1       USGovGCCHigh  23.103.199.128   255.255.255.128  0      0
1       USGovGCCHigh  23.103.208.0     255.255.252.0    0      0
```

Advanced Logs

More information can be obtained from the system logs.

- `show log system all`

  Use this command to view the services created by the policy manager for the configured SaaS applications. Filter the output for *policymgr*. This command also gives information about the HTTP probes sent by the Branch Gateway for the configured SaaS applications. For information about how to filter, see Filtering Commands.

The following example displays the partial output of the command. The actual CLI output in Aruba Central appears in a single row. In this example, the output is modified to appear in multiple rows.

```
(host) #show log system all
Mar  8 16:59:44  policymgr[6838]: <399803> <6838> <ERRS> |policymgr| An
internal system error has occurred at file policymgr_rules.c function
get_links_mask line 899 error Invalid group string:cellular_lte.

Mar  8 17:00:54  policymgr[6838]: <399803> <6838> <ERRS> |policymgr| An
internal system error has occurred at file policymgr_rules.c function
get_links_mask line 899 error Invalid group string:cellular_lte.

Mar  8 17:01:44  policymgr[6838]: <398550> <6838> <ERRS> |policymgr| |uplink|
Unexpected Policymgr runtime error at policymgr_gsm_delete_ip_probe 88 GSM
Delete ip_probe failed for ip:184.26.53.145 src_intf:4086 probe:
saas_gotomeeting_pp, error:error_htbl_key_not_found

Mar  8 17:01:44  policymgr[6838]: <398550> <6838> <ERRS> |policymgr| |uplink|
Unexpected Policymgr runtime error at policymgr_gsm_delete_ip_probe 88 GSM
Delete ip_probe failed for ip:184.26.53.200 src_intf:4086
probe:saas_gotomeeting_pp, error:error_htbl_key_not_found

Mar  8 17:01:44  policymgr[6838]: <398550> <6838> <ERRS> |policymgr| |uplink|
Unexpected Policymgr runtime error at policymgr_gsm_delete_ip_probe 88
GSM Delete ip_probe failed for ip:23.197.50.57 src_intf:4086
probe:saas_adobe_pp, error:error_htbl_key_not_found

Mar  8 17:01:44  policymgr[6838]: <399803> <6838> <ERRS> |policymgr|
An internal system error has occurred at file policymgr_rules.c function
get_links_mask line 899 error Invalid group string:cellular_lte.

Mar  8 17:02:24  policymgr[6838]: <399803> <6838> <ERRS> |policymgr|
An internal system error has occurred at file policymgr_rules.c function
get_links_mask line 899 error Invalid group string:cellular_lte.

Mar  8 17:03:25  policymgr[6838]: <399803> <6838> <ERRS> |policymgr|
An internal system error has occurred at file policymgr_rules.c function
get_links_mask line 899 error Invalid group string:cellular_lte.
```

Configuring Aruba Gateways for Application Visibility and Control

The application visibility and control feature on Aruba Gateways enables administrators to monitor, analyze, and control application usage and bandwidth consumption in their networks. To provide in-depth visibility

and insightful reporting of the applications in use, Aruba Gateways support Deep Packet Inspection (DPI) of applications accessed by the client devices in the SD-WAN network.

Based on application usage, network administrators can configure ACLs to control application access, prioritize mission-critical applications, and improve quality of experience by fine tuning bandwidth allocation per application or application category.

The 90xx series Gateways do not support IP classification, reputation, and geolocation-based filtering.

Aruba Gateways support the following types of application configurations:

- Configuring per-application limits from the list of applications and application categories. For more information, see Configuring Per-Application Limits
- Creating custom applications and application categories. For more information, see Creating Custom Application and Application Categories
- Configuring following types of application visibility and control features:
  - **Firewall Visibility**—Allows Gateways to log all firewall sessions.
  - **Deep Packet Inspection (AppRF)**—Allows Gateways to perform a deep packet of inspection of the application traffic. For more information, see Using Deep Packet Inspection.
  - **Website Content Classification (WebCC)**—Allows administrators to filter URLs based on website categories and security reputation score. When you enable WebCC, you can configure enable filtering websites based on IP reputation and geolocation. For more information, see Filtering URLs Based on Website Content and Reputation.

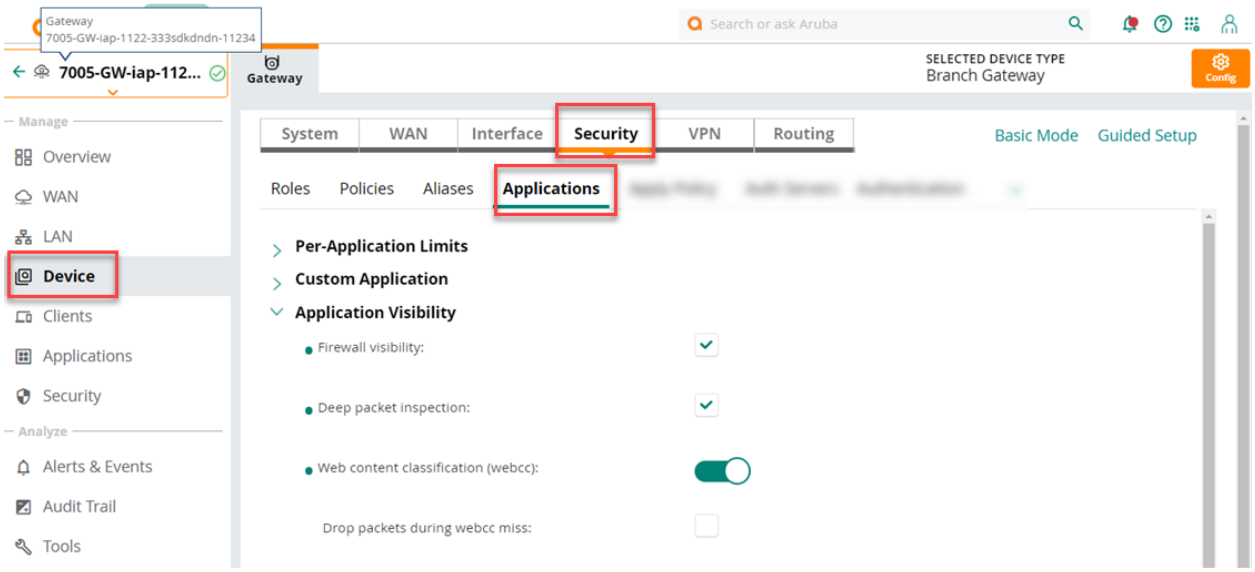
Using Deep Packet Inspection

Aruba Gateways support Deep Packet Inspection (DPI) of applications and application categories used by the connected clients.

The DPI feature enables Gateways to perform the following functions:

- Traffic Inspection and reporting — When DPI is enabled, Gateways perform DPI of application traffic and report it in the Gateway monitoring dashboard. The app library on Gateways includes a list of default applications and application categories on which you can enable deep packet inspection. You can also create a list of custom applications and application categories for DPI.
- Application control—Based on application usage and bandwidth consumption metrics, administrators can configure ACLs per application or application category and throttle bandwidth for mission-critical applications for traffic prioritization and QoS.

Figure 255 *Enabling Deep Packet Inspection in the Gateway Dashboard*



Configuring Per-Application Limits

To configure per-application limits from the default list of applications and application categories, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Switch to **Advanced Mode**.
3. Click **Security** > **Applications** > **Per-Application Limits**.
4. To add a new application, click **+**.
5. Select a **Type** from the drop-down list. The **Application** list displays the default applications available in the DPI library. The **Application category** list displays the default application categories available in the DPI library.
6. Select **Name** of the application or the application category.

7. Enter an **Upstream** value between 256 to 2000000 and select value **Kbit** or **Mbit** from the drop-down list.
8. Enter a **Downstream** value between 256 to 2000000 and select value **Kbit** or **Mbit** from the drop-down list.
9. Click **Save Settings**.

Creating Custom Application and Application Categories

You can add up to 64 custom applications to Aruba Gateway's DPI library. For each custom application, you configure up to 16 ACL rules.

To create a custom application:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Switch to **Advanced Mode**.
3. Click **Security** > **Applications** > **Custom Application**.
4. To add a new application, click **+**.
5. Enter a **Name** for the custom application.
6. Enter an **Application ID** between 1 and 64. The application ID is used to identify the application in the application category during DPI.
7. Select a **Category** from the drop-down list. The application category list displays the default application categories available in the DPI library. To add a new application category, click **+**. You can create up to 32 application categories.
8. (Optional) Click **+** in the **Server name** table and configure the DNS server name and the FQDN URI.
9. (Optional) Click **+** in the **Referer name** table and configure a referrer URL. A referrer is URL data from an HTTP header field that is used for identifying the web link to direct users to a web page.
10. (Optional) Click **+** in the Common Name table and configure a **Common Name**; that is, the SSL certificate Common Name identifies the hostname associated with the certificate. The Common Name typically includes host and domain name. The Common Name must match website address of the application.
11. Click **Save Settings**.

Enabling DPI under Application Visibility

To enable DPI, complete the following steps:

1. To configure a Gateway group or Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Applications**.
3. Click **Application Visibility**.
4. Select the **Deep Packet Inspection** check box.

Configuring Proxy Server on Branch Gateway for DPI

If your network has clients that access web applications through a proxy server, you must configure the proxy server details on Branch Gateways to enable DPI for client traffic and application usage.

To configure proxy server details on Branch Gateway for DPI, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.

d. Under **Manage**, click **Device**.

The gateway device configuration page is displayed.

2. Switch to **Advanced Mode**.
3. Click **Security** > **Applications**.
4. Click **Application Visibility**.
5. Enable the **Application visibility with proxy server**.
6. Enter the HTTP and HTTPS port of the proxy server.
7. Click **Save Settings**.

Monitoring Application Usage

To monitor application usage for Gateway clients:

1. To monitor application usage for a Gateway group or Gateway, complete either one of these steps:
   - To view application usage for a Gateway group:
     a. In the **Network Operations** app, set the filter to a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Applications** > **Visibility**.
   - To view application usage for a gateway:
     a. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.
2. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.
3. Under **Manage**, click **Applications** > **Visibility**.

For more information on application graphs and usage metrics, see Gateway > Applications > Visibility.

Configuring Security Policies for Application Access Control

For more information, see Configuring ACLs for Deep Packet Inspection.

Configuring Bandwidth Contracts Per Applications

To configure bandwidth contract, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click **Config**.

        The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
    a. Set the filter to **Global** or a group containing at least one Branch Gateway.
    b. Under **Manage**, click **Devices** > **Gateways**.
       A list of gateways is displayed in the List view.
    c. Click a gateway under **Device Name**.
       The dashboard context for the gateway is displayed.
    d. Under **Manage**, click **Device**.
       The gateway device configuration page is displayed.

2. Switch to **Advanced Mode**.
3. Click **Security** > **Applications**.
4. Expand **Per-Application Limits**.
5. To add an application or application category to a bandwidth contract, click **+** in the table The **Add Application Limit** section is displayed.
6. Select the application bandwidth type from the **Type** drop-down list.
7. Select the name of the bandwidth contract from the **Name** drop-down list.
8. Enter values in Kbits or Mbits in the **Upstream** and **Downstream** fields.
9. Click **Save Settings**.

Filtering URLs Based on Website Content and Reputation

Aruba Gateways enhance branch security by providing real-time web content and reputation filtering. The Website Content Classification feature on Branch Gateways allows you to classify website content based on reputation and take measures to block malicious sites.

Aruba Gateways use Webroot BrightCloud Security Services to fetch information on website content classification, and geolocation of IPs. The IP reputation database contains known IP addresses associated with various malicious activities or threats such as botnet, DOS, and spam sources. The geolocation IP database contains the geographical location of the IP address from where the traffic is received or to which the traffic is sent. This allows the Branch Gateways to provide geolocation and reputation filtering as a part of the security suite.

When a new session is received, the source and destination IPs are fetched and both these IP addresses are looked up on the BrightCloud server to retrieve the information about the reputation and geolocation of the IPs. If the table lookup succeeds, then the session is marked as classified and subjected to IP classification based firewall policies. If the table lookup fails, IP classification query message is sent to the control plane to have the classification for these IP addresses downloaded from Webroot's Brightcloud service.

The 90xx series Gateways do not support IP classification, reputation, and geolocation-based filtering.

Enabling Web Content Classification

To enable WebCC, complete the following steps:

1. To configure a gateway group or gateway device, complete either one of these steps:
    - To configure a Branch Gateway group or VPNC group, complete the following steps:
        a. Set the filter to a group containing at least one Branch Gateway.
           The dashboard context for a group is displayed.

b. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. Click **Security** > **Applications**.
3. Click **Application Visibility**.
4. For enabling traffic analysis for WebCC, select the **Web content classification (WebCC)** check box.
5. Click **Save Settings**.

Configuring Security Policies for Filtering Websites and IP Addresses

For more information, see Configuring ACLs for Web Content Classification.

Dropping Unclassified Web Content

To drop the packets that do not match any web content category or reputation levels in the Branch Gateway's internal web content cache, complete the following task:

1. To configure a gateway group or gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Applications**.
3. Click **Application Visibility**.

4. For website URL filtering, turn on the **Web Content Classification (WebCC)** toggle switch.
5. Select the **Drop packets during webcc miss** check box.
6. Click **Save Settings**.

Configuring Redirect URLs for Blocked Sessions

To configure a URL to redirect the users when they access blocked sessions, complete the following tasks:

1. To configure a Gateway group or Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Applications**.
3. Click **Application Visibility**.
4. For website URL filtering, select the **Web Content Classification (WebCC)** check box.
5. Specify a URL to which the users should be redirected when they access blocked session in the **URL to redirect blocked session** field.
6. Click **Save Settings**.

Configuring IP Reputation and Filtering

IP reputation policies can be applied to Branch Gateways to prevent traffic from or to malicious websites.

Before configuring this feature, ensure that you configure the WebCC or Web reputation policies. For more information, see Configuring ACLs for Web Content Classification.

To enable IP reputation and filtering, complete the following tasks:

1. To configure a gateway group or gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. Click **Security** > **Applications**.
3. Click **Application Visibility**.
4. For website URL filtering, turn on the **Web Content Classification (WebCC)** toggle switch.
5. Enable **IP classification and reputation**.
6. To deny incoming traffic from malicious IP addresses, select the **Deny inbound connections from malicious IP address**.
7. To deny outgoing traffic to malicious IP addresses, select the **Deny outbound connections to malicious IP address**.
8. To allowlist any trusted IP address or a range of IP addresses that may be misclassified as malicious IP addresses, complete the following tasks:
   a. Click **+** from the **IP ADDRESS** table under the **Allowedlist IP addresses** field.
   b. Enter the IP address to be allowlisted in the **IP address** field. If you want to allowlist a range of IP addresses, enter the starting IP address of the range in this field.
   c. Enter the ending IP address of the range to be allowlisted in the **End IP address** field.
   d. Specify any description of the IP address or the IP address range in the **Description** field.

The IP addresses included in this table are considered trusted IP addresses even if they are classified as malicious IP address by the IP reputation database.

   e. Click **Save Settings**.

Configure Geolocation-Based Filtering

The Geolocation filtering policies allow you to filter traffic based on the geographic location of the source or destination IP addresses. You can configure these policies to permit or deny outgoing or incoming traffic from specific countries.

To enable geolocation-based filtering, complete the following tasks:

1. To configure a gateway group or gateway device, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

     The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. Click **Security** > **Applications**.
3. Click **Application Visibility**.
4. For website URL filtering, turn on the **Web Content Classification (WebCC)** toggle switch.
5. Enable **Geo location**.
6. Click **+** in the **GeoLocation** table to add a new geolocation rule.
7. In the **New GeoLocation Rule** section, configure the following parameters:
   - **Action**—Select the action as **Permit** or **Deny**.
   - **Direction**—Select the direction as **To** or **From**.
   - **Country**—Select the required country for which you want to apply this rule.
   - **Log**—Select the check box to enable logging for this rule.
8. Click **Save Settings**.

Monitoring Application Traffic

For website traffic visibility:

1. To configure a gateway group or gateway device, complete either one of these steps:
   - To view a Gateway group:
     a. In the **Network Operations** app, use the filter to select **Groups**.
     b. Under **Manage**, click **Applications** > **Visibility**.
   - To view a gateway:
     a. In the **Network Operations** app, use the filter to select the gateway.

For more information on application graphs and usage metrics, see Gateway > Applications > Visibility.

Enforcing a Common Security Policy for Wired and Wireless Users

The Aruba SD Branch solution supports dynamic segmentation of the branch network based on device profiles. The solution also supports diverting client traffic from selected devices to Branch Gateways.

If your SD Branch has Aruba Switches deployed and provisioned to function along with the Branch Gateways, your network administrators can configure common set of security policies for wired and wireless clients on the ClearPass server and use Branch Gateway as policy enforcement points to inspect every communication in the branch.

The **Tunneled Node** feature on Aruba switches allows wired traffic entering a switch port to be routed to Branch Gateway through the GRE tunnel. An Aruba switch can also initiate a GRE tunnel with the Branch

Gateway from its management IP address associated to an underlay VLAN that is different from the user VLANs.

To allow policy enforcement for the wired traffic, the port-based tunnels must be configured and the IP address of the Branch Gateway must be set as a primary tunneled node on the switches. For more information on the configuration procedure, see the *HPE ArubaOS-Switch Management and Configuration Guide*.

Configuring Firewall Policies and ACLs

To secure your branch, you must configure a policy with a set of ACLs and apply these policies to user roles or user-facing VLAN interfaces.

For an SD Branch setup, the general recommendation is to set the WAN-facing ports as trusted and LAN-facing ports as untrusted. Although WAN-facing ports are trusted, Aruba recommends that you apply a restrictive firewall policy to the WAN interfaces.

As LAN-facing ports are untrusted, it is very important to secure your branch by applying a AAA profile to the VLANs configured for the LAN interfaces. When a AAA policy is applied, SD-WAN Gateways assign the user roles based on the role preferences configured in a AAA profile.

Firewall Policies for SD Branch

The SD Branch solution supports identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for the WAN network. You can configure firewall policies on Branch Gateways to define user access to network, set priority queue for Quality of Service (QoS), and assign bandwidth contracts.

A firewall policy identifies specific characteristics about a data packet and performs one of the following actions:

- Firewall-type action such as permitting or denying the packets.
- Administrative action such as logging the packets.
- QoS action such as setting 802.1p bits or placing the packet in a priority queue.

Types of ACLs

Aruba Central allows you to configure the following types of ACLs on Branch Gateways.

- **Standard ACLs**—Permit or deny any traffic based on the source IP address of the packet. Standard ACLs can be either named or numbered, with valid numbers in the range of 1–99 and 1300–1399. Standard ACLs use a bit-wise mask to specify the portion of the source IP address to be matched.
- **Extended ACLs**—Permit or deny any traffic based on source or destination IP address, source or destination port number, or IP protocol. Extended ACLs can be named or numbered, with valid numbers in the range 100–199 and 2000–2699.
- **MAC ACLs**—Filter the traffic on a specific source MAC address or range of MAC addresses. MAC ACLs can be either named or numbered, with valid numbers in the range of 700–799 and 1200–1299.
- **Ethertype ACLs**—Filter the traffic based on the Ethertype field in the frame header. Ethertype ACLs can be either named or numbered, with valid numbers in the range of 200–299.These ACLs can be used to permit IPs while blocking other non-IP protocols, such as IPX or AppleTalk.
- **Session ACLs**—Restrict all services from specific hosts and subnets. Rules with this ACL are applied to all traffic on the Branch Gateway regardless of the ingress port or VLAN.
- **Route ACLs**—Forward all packets to a device defined by an IPsec map, a next hop list, a tunnel or a tunnel group.

Configuring Aliases for Firewall Policies

Aliases allow you to name your network ports, protocols, and services in a simple yet understandable way. When configuring multiple ACLs, you can use a common alias instead of providing details of the network ports, protocols, and services each time.

Creating a Network Alias

A network alias defines a TCP, UDP, or IP protocol and a list or range of ports supported by that service. You can use a network alias when specifying a network service for multiple session ACLs.

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Aliases**.
3. Click **+** to create a network alias.
4. Enter a name and description for this alias.
5. Select the **Invert** check box.
6. Click **Save Settings**.
7. Under **Destination** click + to add a new user rule.
8. Select **Network** from the **Rule type** drop-down list.
9. Enter a IPv4 address and Network mask.
10. Click **Save Settings**.

Creating a Service Alias

To create a service alias:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.

b. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. Click **Security** > **Aliases**.
3. Click **+** to create a service alias.
   a. Enter a value in the **Service name** field.
   b. In the **Protocol** drop-down list, select either **TCP** or **UDP**, or select **protocol** and enter the IP protocol number and **Application level gateway (alg)** of the protocol for which you want to create an alias.
   c. In the **Port type** drop-down list, specify whether you want to define the port by a contiguous range of ports, or by a list of non-contiguous port numbers.
      - If you selected **range**, enter the starting and ending port numbers in the **Starting port** and **End port** fields, respectively.
      - If you selected **list**, enter a comma-separated list of port numbers in the **Port list** field.
   d. To limit the service alias to a specific application, select one of the following service types from the **Application Level Gateway (alg)** drop-down list:
      - ftp: Service is FTP
      - tftp: Service is TFTP
      - dns: Service is DNS
      - dhcp: Service is DHCP
      - sip: Service is SIP
      - sips: Service is Secure SIP
      - svp: Service is SVP
      - sccp: Service is SCCP
      - rtsp: Service is RTSP
      - vocera: Service is VOCERA
      - noe: Service is Alcatel NOE
      - h323: Service is H323
      - jabber: Service is Jabber
      - facetime: Service is Facetime
4. Click **Save Settings**.

Creating a Firewall Policy for Network Services

To create a firewall policy, complete the following procedure:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Policies**.
3. Click **+** to create a new policy.
4. Select a policy type from the **Policy type** drop-down list. You can select **Session**, **Ethertype**, **MAC**, **Route**, **Extended**, or **Standard**.
5. Enter the policy name in the **Policy name** field.
6. Click **Save Settings**.

Configuring Access Rules

To configure access rule, complete the following procedure:

1. From the list of policies, select the policy that you created and click **+** in the **Policy <policy name>** table.
2. Select the **Access Control** option in the **Rule Type** field and click **OK**.
3. To add a rule to restrict packet flow or permit access to network or services, configure the following parameters:

Table 265: *Firewall Policy Rule Parameters*

Parameter	Description
IP version	Specifies the IP version that the policy applies to. Select IPv4.
Source (required)	▪ Source of the traffic, which can be one of the following: ▪ **Any**—Acts as a wildcard and applies to any source address. ▪ **User**—Refers to the traffic from the wireless client. ▪ **Host**—Refers to the traffic from a specific host. When this option is selected, specify the IP address of the host. ▪ **Network**—Refers to the traffic that has a source IP from a subnet of IP addresses. When this option is selected, specify the IP address and network mask of the subnet.

Table 265: *Firewall Policy Rule Parameters*

Parameter	Description
	■ **Alias**—Refers to using an alias for a host or network. ■ **Local IP**—Refers to the local IP address. ■ **User Role**—Refers to the user role to be assigned.
Destination (required)	Destination of the traffic.
Service/app (required)	Type of traffic, which can be one of the following: ■ **Any**—This option specifies that this rule applies to any type of traffic. ■ **TCP**—Using this option, you configure a range of TCP ports to match for the rule to be applied. ■ **UDP**—Using this option, you configure a range of UDP ports to match for the rule to be applied. ■ **Service**—Using this option, you use one of the pre-defined services (common protocols such as HTTPS and HTTP) as the protocol to match for the rule to be applied. ■ **Protocol**—This option specifies the routing protocol. ■ **Application**—This option specifies the application name. ■ **App Category**—This option specifies the category of the application. ■ **Web Category/Reputation**—This option specifies the name of the web content category or the predefined web content reputation level.
Action (required)	The action that you want the Branch Gateway to perform on a packet that matches the specified criteria. ■ **Deny**—Denies traffic not matching this rule. ■ **Permit**—Permits the traffic matching this rule. ■ **Redirect**—This option redirects the traffic to a GRE tunnel. This option is used primarily to redirect all guest traffic to a GRE tunnel and then to a DMZ router or switch. ■ **Destination NAT**—Redirects traffic to the configured IP address and destination port. An example of this option is to redirect all HTTP packets to the captive portal port on the Branch Gateway as used in the predefined policy called captive portal. This action functions in tunnel or decrypt-tunnel forwarding mode. User should configure the NAT pool in the Branch Gateway. ■ **Source and Destination NAT**—This option performs both source and destination NAT on packets matching the rule. This action forwards packets from the source network to the destination network and re-marks them with destination IP of the target network. This action functions in tunnel or decrypt-tunnel forwarding mode. User should configure the NAT pool in the Branch Gateway. ■ **Source NAT**—Performs network address translation on packets matching the rule. The options available are: ◦ **NAT Pool**—When this option is selected, you must to select a NAT pool. This action functions in the tunnel or decrypt-tunnel forwarding mode. ◦ **VLAN**—When this option is selected, you must select a VLAN ID. The source IP address of the network changes to the IP address of the VLAN (NAT pool is automatically configured). ■ **Route Source NAT**—Routes traffic based on source address. ■ **Route Destination NAT**—Routes traffic based on destination address.

Table 265: *Firewall Policy Rule Parameters*

Parameter	Description
DSCP (optional)	Option to re-tag the traffic with the specified DSCP tag in the IP header of the packet that matches this rule when it leaves the Branch Gateway.
Time Range	You can allow or deny access during specific time range. You can either create an **absolute** time range with a single fixed start and end date and time; or a **periodic** (recurring) time range that starts and ends at a specified time on a weekday, weekend, or selected day.
802.1p Priority (optional)	When this parameter is enabled, the value of 802.1p priority bits are marked in the frame of a packet matching this rule when it leaves the Branch Gateway. 0 represents the lowest priority (background traffic) and 7 represents the highest priority (network control).
Options	Select the required options: ■ **Log**—Logs a match to this rule. This is recommended when a rule indicates a security breach, such as a data packet on a policy that is meant only to be used for voice calls. ■ **Mirror**—Mirrors session packets to datapath or remote destination. ■ **Blacklist**—Automatically blacklists a client that is the source or destination of the traffic matching this rule. This option is recommended for rules that indicate a security breach where the blacklisting option can be used to prevent access to clients that are attempting to breach the security. ■ **Disable Scanning**—Disable AP scanning other channels.
Queue (optional)	The queue in which a packet matching this rule should be placed. Select **High** for higher-priority data, such as voice, and **Low** for lower-priority traffic.
Position	The position of the rule in the **Policy <policy name>** table, where 1 is first and default is last.

Configuring ACLs for Deep Packet Inspection

Branch Gateways support AppRF, Aruba's custom-built layer 7 firewall capability. It consists of an onboard Deep Packet Inspection (DPI) service that allows creating firewall policies based on the types of application and application categories.

You can configure ACLs to restrict user access to an application or application category. You can also define traffic-shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth-monopolizing applications on a guest role within an enterprise.

Creating ACLs for Application Access Control

To create ACL rules for Deep Packet Inspection on Branch Gateways, complete the following procedure:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.

     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.

     c. Click **Config**.

        The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. Click **Security** > **Policies**.
3. Click **+** to create a new policy.
4. Enter the policy name in the **Policy name** field.
5. From the list of policies, select the policy you just created and click **+**.
6. Select one of the following options from the **Service/app** drop-down list.
   - **Application**—To allow or deny access to a specific application.
   - **Application Category**—To allow or deny access to a specific application category.
7. Specify an action.
8. Click **Save Settings**.

Configuration Example

This example shows a DPI rule along with a layer 3 or layer 4 rule with forwarding action in the same ACL. Both ACL policies can be applied to a single user role.

- Rule 1
  - source: any
  - destination: any
  - service or application: application facebook
  - action: permit
  - DSCP value: 45
- Rule 2
  - source: any
  - destination: any
  - service or application: application YouTube
  - action: deny
- Rule 3
  - source: any
  - destination: any
  - service or application: application category peer-to-peer
  - action: deny
- Rule 4
  - source: any
  - destination: any

- service or application: TCP 23
- action: permit

- Rule 5
  - source: network 40.1.0.0/16
  - destination: any
  - service or application: TCP 80
  - action: permit
  - DSCP: 60

Configuring ACLs for Web Content Classification

The WebCC feature in Branch Gateways allows your network administrators to analyze the website usage by clients. Branch Gateways classify the usage pattern based on web categories and website reputation scores; it allows your network administrators to take appropriate measures to prevent malicious malware, spyware, or adware by blocking dangerous websites.

To configure an ACL rule for website content classification, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Policies**.
3. Click **+** to create a new policy. Select a policy type from the **Policy type** drop-down list.
4. Enter the policy name in the **Policy name** field.
5. From the list of policies, select the policy you just created and click **+**.
6. In the **Rules of this Role only** section, perform the steps:
7. Select **Web Category/Reputation** from the **Service/app** drop-down list:
   a. From the **Web reputation** drop-down list, select one of the following reputation scores based on your requirement:
      - **high-risk**—These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads.

- **low-risk**—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
- **moderate-risk**—These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
- **suspicious**—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
- **trustworthy**—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.

b. From the **Action** drop-down list, select **Deny** to not allow user to access this web category; else, select **Permit** to allow user to access the web category.
c. For **DSCP**, enter a value.
d. From the **Time range** drop-down list, select a suitable time range during which you want the policy to be active or valid. Alternatively, you can also create a new time range by clicking **the +** icon.
e. From the **802.1p priority** drop-down list, select a priority from 1-7.
f. For **Options**, select **Log, Mirror**, and **Blacklist**, or any other option that is applicable.

8. Click **Save Settings**.

Configuring Global Firewall Parameters

The Aruba Gateways support stateful firewall for stateful inspection of packets. Stateful firewalls provide an additional layer of security by tracking the state of network connections and using the state information from previous communications to monitor and control new communication attempts. To protect your network from external attacks and unauthorized communication attempts, you can configure match conditions and packet filtering criteria for the Aruba Gateways.

To configure global firewall parameters for protection against external attacks, complete the following procedure:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **Security** > **Firewall**.
7. Configure the parameters described in Table 266 as per your network requirements.
8. Click **Save Settings**.

Table 266: *Firewall Parameters*

Parameter	Description
Monitor ping attack	Number of ICMP pings per 30 seconds, which if exceeded, can indicate a DoS attack. A valid range is 1-16384 pings per 30 seconds. Recommended value is 120.
Monitor TCP SYN attack rate	Number of TCP SYN messages per 30 seconds, which if exceeded, can indicate a DoS attack. A valid range is 1-16384 pings per 30 seconds. Recommended value is 960.
Monitor IP sessions attack	Number of TCP or UDP connection requests per 30 second, which if exceeded, can indicate a DoS attack. A valid range is 1-16384 requests per 30 seconds. Recommended value is 960.
Monitor/police non-gratuitous ARP attacks	Enable monitoring and policing non-gratuitous ARP attacks and configure the following parameters: ■ **Monitor/police non-gratuitous ARP attack rate**—Specify the number of ARP packets (other than Gratuitous ARP packets) per 30 seconds, which if exceeded, can indicate a DoS attack. A valid range is 1-16384 packets per 30 seconds. Recommended value is 960. ■ **Monitor/police non-gratuitous ARP attack action**—Select an action to be taken upon detection of ARP attacks. The options are **Blacklist** and **Drop**.
Monitor/Police Gratuitous ARP Attack rate (per 30 seconds)	Number of gratuitous ARP packets per 30 seconds, which if exceeded, can indicate DoS attack. A valid range is 1-16384 packets per 30 seconds. Recommended value is 50.
Monitor/police gratuitous ARP attack action	The action to be taken upon detection of ARP attacks. The options are **Blacklist** and **Drop**. The default value is **Drop**.
Monitor/police CP attack rate	Rate limit for control plane traffic policing. The recommended value is 3000 frames per 30 seconds.
Deny inter user bridging	Prevents the forwarding of layer 2 traffic between wired or wireless users. You can configure user role policies that prevent layer 3 traffic between users or networks but this does not block layer 2 traffic. This option can be used to prevent traffic from being forwarded.
Deny inter user traffic	Denies traffic between untrusted users by not allowing layer 2 and layer 3 traffic.
Deny source routing	Permits firewall to reject and log packets with the specified IP options loose source routing, strict source routing, and record route.
Deny all IP fragments	Drops all IP fragments. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support representative.
Enforce TCP handshake before allowing data	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option must be disabled when you have mobile clients on the network as enabling this option may affect mobility.

Table 266: *Firewall Parameters*

Parameter	Description
Prohibit IP spoofing	Enables detection of IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, source and destination IP and MAC addresses are checked for each ARP request or response. Traffic from a second MAC address using a specific IP address is denied, and the entry is not added to the user table. Possible IP spoofing attacks are logged and an SNMP trap is sent. This is enabled by default.
Prohibit RST replay attack	Closes a TCP connection in both directions if a TCP RST is received from either direction, this option is disabled by default. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support representative.
Log all received ICMP errors	Enables logging of received ICMP errors. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support representative.
Allow tri-session with DNAT	Allows a three-way session when performing destination NAT. This option must be enabled when the Branch Gateway is not the default gateway for wireless clients. This option is typically used for captive portal configuration.
AMSDU configuration	Enables handling AMSDU traffic from clients.
Session idle timeout	Sets the time, in seconds, for a non-TCP protocol such as UDP or a non-established TCP session to be idle before it is removed from the session table. Specify a value in the range of 16-300 seconds. An established TCP session is maintained in the session table until a RST or FIN flag is sent or up to 15 minutes of being idle. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support representative.
Disable FTP server	Disables the FTP server. Enabling this option prevents FTP transfers. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support representative.
GRE call ID processing	Creates a unique state for each PPTP tunnel. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support representative.
Optimize duplicate address detection frames	Enables optimization of duplicate address detection frames with respect to IPv4 gratuitous ARPs.
Stall detection	Enable this to detect if there is any hardware issue with the forwarding engine and to take necessary mitigating steps. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support

Table 266: *Firewall Parameters*

Parameter	Description
	representative.
Immediate freeback	Enables immediate freeback of hardware buffers from datapath to the interface. **NOTE:** Do not enable this option unless instructed to do so by an Aruba Support representative.
Stateful ICMP processing	Enables stateful ICMP processing for all kinds of ICMP traffic. This option is used to selectively control different kinds of ICMP traffic through ACLs.
Mcast RED	Enables the multicast random early detection algorithm parameters.
Per-packet logging	Enables logging of every packet if logging is enabled for the corresponding session rule. By default, one event is logged per session. If you enable this option, each packet in the session is logged.
Prohibit ARP spoofing	Detects and prohibits ARP spoofing. When this option is enabled, possible address resolution protocol (arp) spoofing attacks are logged and an SNMP trap is sent.
Prevent DHCP exhaustion	Enables verification DHCP client hardware address against the packet source MAC address. This command checks the frame's source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. Enabling this feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.
Only allow local subnets in user table	Adds only IP addresses, which belong to a local subnet, to the user table.
Session-tunnel FIB	Enable session-tunnel-based forwarding. Enable this parameter only during maintenance window or off-peak production hours.
Multicast automatic shaping	Enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used.
Enforce bw contracts for broadcast traffic	Applies bandwidth contracts to local subnet broadcast traffic.
Enforce TCP sequence numbers	Enforces the TCP sequence numbers for all packets.
Public-access mode	Enables public access mode for all packets.
Rate limit CP untrusted ucast traffic (pps)	Indicates the rate limit value of untrusted unicast traffic. The range is 1-65535 packets pps.

Table 266: *Firewall Parameters*

Parameter	Description
Rate limit CP untrusted mcast traffic (pps)	Indicates the rate limit value of untrusted multicast traffic. The range is 1-65535 pps.
Rate limit CP trusted ucast traffic (pps)	Indicates the rate limit value of trusted unicast traffic. The range is 1-98304 pps.
Rate limit CP trusted mcast traffic (pps)	Specifies the trusted multicast traffic rate limit. The range is 1-65535 pps.
Rate limit CP route traffic (pps)	Indicates the rate limit value of route traffic that needs ARP requests. The range is 1-65535 pps.
Rate limit CP session mirror traffic (pps)	Indicates the rate limit value of session mirrored traffic forwarded to the Aruba Gateway device. The range is 1-65535 pps.
Rate limit CP VRRP traffic (pps)	Indicates the rate limit value of VRRP traffic that hits the control plane. The range is 1-65535 pps.
Rate limit CP ARP traffic (pps)	Indicates the rate limit value of ARP traffic that hits the control plane. The range is 1-65535 pps.
Rate limit CP l2 protocol/other traffic (pps	Indicates the rate limit value of other L2 traffic that hits the control plane. The range is 1-65535 pps.
Rate limit CP auth process traffic (pps)	Indicates the rate limit value of the traffic that is forwarded to the authentication process. The range is 1-65535 pps.
Rate limit CP IKE traffic (pps)	Indicates the rate limit value of IKE traffic that hits the control plane. The range is 1-65535 pps.
Jumbo frames processing	Enables Jumbo frames processing for data frames that are larger than 1500 bytes. You can specify a value in the **Jumbo MTU[1789-9216] bytes** field. The The range is 1789-9216 bytes. The default value is 9216 bytes.
Mark management frames	Enables marking of management frames.
Trust client QoS	Uses the DSCP set by client to prioritize the RTP traffic.

Advanced Monitoring Parameters

Table 267: *Advanced Monitoring*

Parameter	Description
App Performance Monitoring	Enables application performance monitoring.
DHCP Performance Monitoring	Enables DHCP and DNS server performance monitoring.

Configuring User Roles for Clients

A client device in an Aruba user-centric network is associated with a user role that determines the access privileges, bandwidth contract assignments, and frequency of client authentication.

A client device is assigned a user role by several methods. The following list shows the role assignment preferences for a branch network:

1. Initial user role—The initial user role or VLAN for unauthenticated clients is configured in the AAA profile.
2. User-derived role—The user role can be derived from user attributes when a client connects to an AP. You can configure access rules to assign a user role to the clients that match a specific criteria. For example, you can configure a rule to assign the role **VoIP-Phone** to any client that has a MAC address that starts with bytes *xx:yy:zz*. The user-derived roles are applied before client authentication.
3. Default user role—The user role can be the default user role configured for an authentication method, such as 802.1X or VPN. For each authentication method, you can configure a default role for the clients that successfully authenticate based on the specified authentication method.
4. Server-derived role—The user role can be derived from attributes returned by the authentication server and certain client attributes. If the client authenticates through an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication, or on client attributes such as SSID (even if the attribute is not returned by the server). Server-derived roles are applied after client authentication.
5. VSA-Derived Role—Many NAS vendors, including Aruba, use vendor-specific attributes to provide features that are not supported in standard RADIUS attributes. The Aruba VSAs allow deriving user roles and VLAN for the clients that authenticate to the RADIUS server. A role derived from a VSA takes precedence over other types of user roles.

Refer to the following topics to know how to configure User Roles for clients:

- Creating a Role
- Assigning a Policy to a Role
- Assigning User Roles in AAA Profiles
- Configuring a Default Role Based on Authentication Methods

Creating a Role

To create a user role, complete the following procedure:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
2. Click **Security** > **Roles**.
3. Click **+** from the **Roles** table to create a new role.

4. Enter a name for the new role and click **Save Settings**.
5. To add access rules, click **+** under **RULES of this Role only** and configure access rules.
6. Click **Save Settings**.

Assigning a Policy to a Role

To add a policy to a role:

1. Select the role name from the **Roles** table.
2. Click **+** under the **Policies** tab.
3. Select the **Add an existing policy** option.
4. Select a policy type from the **Policy type** drop-down list. Select the policy type as **Route** to apply PBR policies.
5. Select a policy from the **Policy name** drop-down list.
6. Click **Save Settings**.
7. (Optional) If the user role contains more than one firewall policy, use the up and down arrows to assign priorities to each policy. The higher the position of the policy on the list, the higher its priority.

Assigning User Roles in AAA Profiles

AAA profiles define user roles for unauthenticated clients (initial role) as well as the default user role for MAC and 802.1X authentication.

To assign user roles in a AAA profile:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **AAA Profiles**.
3. Click **+** to create a new role.
4. Select a profile under **AAA Profiles**.
5. Select the default profile or a user-defined AAA profile.
6. Select the desired user role for unauthenticated users from the **Initial Role** drop-down list.

7. Select the desired user role for users who have completed 802.1X authentication from the **802.1X Authentication Default Role** drop-down list.
8. Select the desired user role for clients who have completed MAC authentication from the **MAC Authentication Default Role** drop-down list.
9. Click **Save Settings**.

Configuring a Default Role Based on Authentication Methods

You can configure a default role for the clients that authenticate using the specified authentication that method. To configure a default role for an authentication method, complete the following procedure:

1. To configure a Branch Gateway group or the Branch Gateway for which you want to configure a default role for a specific authentication method, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **AAA Profiles**.
3. Click **+** to create a new role.
4. To configure the default user role for MAC or 802.1X authentication, select the **AAA Profiles** tab.
5. Select an AAA profile under **AAA Profiles** and select the desired user role for **MAC Authentication Default Role** or **802.1X Authentication Default Role**.
6. To configure the default user role for other authentication methods, select the **L2 Authentication** or **L3 Authentication** tab.
   a. Select the authentication type (Stateful 802.1X for L2 Authentication, Captive Portal or VPN Authentication for L3 Authentication).
   b. Select the profile.
   c. Enter the user role for **Default Role**.
7. Click **Save Settings**.

Configuring Bandwidth Contracts

Aruba Central allows you to configure application specific bandwidth contracts for WLAN and WAN clients. By default, bandwidth contracts for applications are applied on a per-role basis.

You can also configure an exclude list to exclude applications or application categories on which a generic user or role bandwidth-contract is not applied. Use the exclude list option to prioritize mission-critical applications over other user traffic. An enterprise may have well known applications such as Microsoft Exchange, SAP, Oracle, accounting and finance applications, and other enterprise resource planning or customer relationship management applications.

Instead of enumerating bandwidth limits for each application individually on a per-user or per-role basis, you can configure a single bandwidth contract to limit all non-mission-critical applications. You can then exclude all mission-critical applications by placing them in an exclude list. This way, mission-critical applications will not be rate-limited.

Assigning Bandwidth Contracts to User Roles

To configure bandwidth contract, complete the following procedure:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Roles**.
3. Select a role name from the **Roles** table and select the **Bandwidth** tab.
4. To add an application or application category to a bandwidth contract, click **+** under **Per-Application Limits for This Role**.
   a. Select the application bandwidth type from the **Type** drop-down list.
   b. Select the name of the bandwidth contract from the **Name** drop-down list.
   c. Enter values in Kbits or Mbits in the **Upstream** and **Downstream** fields.
   d. Click **Submit**.
5. To add an exception, click **+** under **Per-Application Limit Exceptions for This Role**.
   a. Enter the name of the application or application category.
6. Click **Save Settings**.

Configuring Global Bandwidth Contracts for Applications

To configure bandwidth contract, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Applications**.
3. Expand **Per-Application Limits**.
4. To add an application or application category to a bandwidth contract, click **+** under **Global Per-Application Limits** . The **Add Application Limit** section is displayed.
5. Select the application bandwidth type from the **Type** drop-down list.
6. Select the name of the bandwidth contract from the **Name** drop-down list.
7. Enter values in Kbits or Mbits in the **Upstream** and **Downstream** fields.
8. Click **Save Settings**.

Ensure that you expand **Application Visibility** section and enable **Deep Packet Inspection**.

Configuring Authentication Profiles

The Aruba SD Branch solution supports multiple types of authentication methods. Based on your network goals, security requirements, user types, and the types of client devices, you can configure an AAA profile with a specific authentication method that is suitable for your Layer 2 and Layer 3 security infrastructure.

For example, you can choose to configure an authentication profile with 802.1X or MAC authentication, and configure an authentication server or server group to allow role assignment to client devices.

See the following topics for more information how to set up authentication sources and profiles.

- Configuring RADIUS Authentication Server on Aruba Gateways
- Configuring Other External Authentication Servers on Aruba Gateways
- Configuring Authentication Survivability on a Branch Gateway
- Configuring Server Groups
- Creating a AAA Profile

Configuring RADIUS Authentication Server on Aruba Gateways

To add a RADIUS authentication server, complete the following procedure:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:

- To configure a Branch Gateway group or VPNC group, complete the following steps:
  a. Set the filter to a group containing at least one Branch Gateway.
     The dashboard context for a group is displayed.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the **List** view.
  c. Click **Config**.
     The configuration page is displayed for the selected group.
- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. Click **Security > Auth Servers**.
3. Click **+** under **All Servers**.
4. Enter a name for the new server.
5. Enter the IP address for the new server.
6. To configure a RADIUS server, select **RADIUS** as the server type.
7. In the **All Servers** table, select the name of the new RADIUS server and configure parameters described in Table 268.

Table 268: *RADIUS Server Configuration Parameters*

Code	Description
Name	Name of the RADIUS server.
IP address / hostname	IP address or FQDN of the authentication server. The maximum supported FQDN length is 63 characters. Default: N/A
Secure radius	Enable this option to secure communication between the RADIUS server and the Branch Gateway. Specify values for the following parameters: ■ **Secure auth port**—The destination port for RADIUS over TLS. By default, the value is set to 2083. ■ **Radsec trusted CA name**—The CA certificate that is uploaded as a Trusted CA if the Radsec server uses a certificate signed by a CA. ■ **Radsec server cert name**—The server certificate that is uploaded. ■ **Radsec client cert**—The client certificate sent to the Radsec server.
Auth port	Authentication port of this server. The default value is 1812.

Table 268: *RADIUS Server Configuration Parameters*

Code	Description
Acct port	Accounting port of this server. The default value is 1813.
Shared key	Shared secret between the Branch Gateway and the authentication server. The maximum length is 128 characters.
Retype key	Retype shared secret key.
Timeout	Maximum time, in seconds, that the Branch Gateway waits before timing out the request and resending it. The default value is 5 seconds.
Retransmits	Maximum number of retries sent to the server by the Branch Gateway before the server is marked as down. The default value is 3.
NAS ID	NAS identifier to use in RADIUS packets.
NAS IP	The NAS IP address to be sent in RADIUS packets from that server.
Use MD5	Use MD5 hash of cleartext password.
Enable	Enable the use of IPv4 address for the server.
Lowercase MAC addresses	Send MAC address with lowercase in the authentication and accounting requests to this server.
Use IP address for calling station ID	Enables using the IP address as the calling station ID.
MAC address delimiter	Send MAC address with the following delimiters in the authentication and accounting requests of this server: ■ colon: Send MAC address as XX:XX:XX:XX:XX:XX ■ dash: Send MAC address as XX-XX-XX-XX-XX-XX ■ none: Send MAC address as XXXXXXXXXXXX ■ oui-nic: Send MAC address as XXXXXX-XXXXXX
Service-type of FRAMED-USER	Send the service-type as FRAMED-USER instead of LOGIN-USER. For more information, see RADIUS Service-Type Attribute on page 176.
CPPM credentials	If you are using ClearPass Policy Manager as the RADIUS server, provide user credentials for ClearPass Policy Manager server.
CALLED STATION ID	
Station ID type	Select any of the following options to configure called station ID: ■ **MAC Address** — Uses the MAC address as the called station ID. ■ **AP group** — Uses the host name of the Instant AP as the called station ID. ■ **AP MAC address** — Uses the MAC address of the Instant AP as the called station ID. ■ **AP name** — Uses the host name of the Instant AP as the called station ID. ■ **IP address** — Uses the IP address of the Instant AP as the called station ID. ■ **VLAN ID** — Uses the VLAN ID of as the called station ID.

Table 268: *RADIUS Server Configuration Parameters*

Code	Description
Station ID delimiter	Select a character such as **Colon** or **Dash** as the delimiter for the string.
Include SSID	Select the check box to append the SSID name to the called station ID.

8. Click **Save Settings**.

Configuring an RFC 3576 Server

You can configure a RADIUS server to send user disconnect, CoA, and session timeout messages as described in RFC 3576, "Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)."

To configure an RFC 3576 server, complete the following procedure:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:

- To configure a Branch Gateway group or VPNC group, complete the following steps:
  a. Set the filter to a group containing at least one Branch Gateway.
     The dashboard context for a group is displayed.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the **List** view.
  c. Click **Config**.
     The configuration page is displayed for the selected group.
- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. Click **Security**> **Auth Servers**.
3. Click **+** under **All Servers**.
4. Select **RFC 3576** from the **Type** drop-down list.
5. Enter the IP address for the new server.
6. Enter the server authentication key into the **Key** and **Retype key** fields.
7. Click **Save Settings**.

Configuring Other External Authentication Servers on Aruba Gateways

This section describes how to configure external authentication servers:

Configuring an LDAP Server

To configure an LDAP server, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Auth Servers**.
3. Under **All Servers**, click the **+** icon to add a new server.
4. Set the **Type** to **Ldap** and click **Submit**.
5. From the **All Servers** list, select the server to edit properties.
6. Configure the parameters described in the following table:

Table 269: *LDAP Server Configuration Parameters*

Parameter	Description
Host	IP address of the LDAP server.
Admin-dn	Distinguished name for the admin user who has read or search privileges across all the entries in the LDAP database (the user does need write privileges, but can search the database, and read attributes of other users in the database).
Admin-passwd	Password for the admin user.
Re-type admin-passwd	Retype the password for the admin user for confirmation.
Allow clear-text	Allows clear text (unencrypted) communication with the LDAP server. Default: disabled
Auth port	Port number used for authentication. Default: 389
Base-dn	Distinguished Name of the node that contains the entire user database.
Filter	A string search for users in the LDAP database. The default filter string is: **(objectclass=*)**.

Table 269: *LDAP Server Configuration Parameters*

Parameter	Description
Key attribute	A string search for an LDAP server. For Active Directory, the value is sAMAccountName. Default: sAMAccountName
Timeout	Timeout period of an LDAP request, in seconds. Default: 20 seconds
Enable	Option to enable or disable the server. Default: enabled
Preferred connection type	Preferred type of connection between a Branch Gateway and the LDAP server. The default order of connection type is: 1. ldap-s 2. start-tls 3. clear-text The Branch Gateway first attempts to contact the LDAP server using the preferred connection type, and only attempts to use a lower-priority connection type if the first attempt is not successful. **NOTE:** If you selected **clear-text** as the preferred connection type, you must also enable the **allow-cleartext** option.
Maximum number of non-admin connections	Configure the maximum number of non-admin connections to the server. Default: 4
Chase referrals	Chase referrals anonymously.

7. Select the **Enable** check box to activate the authentication server.
8. Click **Submit**.

Configuring a TACACS+ Server

To configure a TACACS+ server, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.

c. Click a gateway under **Device Name**.

The dashboard context for the gateway is displayed.

d. Under **Manage**, click **Device**.

The gateway device configuration page is displayed.

2. Click **Security** > **Auth Servers**.
3. Under **All Servers**, click the **+** icon to add a new server.
4. Set the **Type** to **Tacacs**.
5. Enter the server **Name** and its **IP address**.
6. Click **Submit**.
7. From the **All Servers** list, select the server to configure server parameters.
8. Configure the parameters described in the following table:

Table 270: *TACACS+ Server Configuration Parameters*

Parameter	Description
Host	IP address of the server.
Key	Shared secret to authenticate communication between the TACACS+ client and server.
Retype key	Retype the shared secret for confirmation.
TCP port	TCP port used by server.
Retransmits	Maximum number of times a request is retried. Default: 3
Timeout	Timeout period for TACACS+ requests (in seconds). Default: 20 seconds
Mode	Option to enables or disable the server. Default: enabled
Session authorization	Option to enable or disable session authorization. Session authorization turns on the optional authorization session for admin users. Default: disabled

Configuring a Windows Server

To configure a Windows server, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

     The dashboard context for a group is displayed.

     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the **List** view.

     c. Click **Config**.

     The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
    a. Set the filter to **Global** or a group containing at least one Branch Gateway.
    b. Under **Manage**, click **Devices** > **Gateways**.
    A list of gateways is displayed in the List view.
    c. Click a gateway under **Device Name**.
    The dashboard context for the gateway is displayed.
    d. Under **Manage**, click **Device**.
    The gateway device configuration page is displayed.

2. Click **Security** > **Auth Servers**.
3. Under **All Servers**, click the **+** icon to add a new server.
4. Set the **Type** to **Windows**.
5. Enter the server **Name** and its **IP address** fields, respectively.
6. Click **Submit**.
7. From the **All Servers** list, select the server to configure server parameters.
8. Configure the parameters described in the following table:

Table 271: *Windows Server Configuration Parameters*

Parameter	Description
Host	IP address of the server.
Mode	Option to enable or disable the server. Default: enabled
Windows Domain	Name of the Windows Domain assigned to the server.

Configuring Authentication Survivability on a Branch Gateway

Authentication survivability is required for all sites where authentication transactions traverse a WAN. It's primary function is to prevent remote link failures between a Gateway device and an authentication server that is either in the cloud or a data center. However, if the connectivity between the Gateway and the authentication server is lost for a limited amount of time, this feature ensures that the known users can securely join the network even if the authentication server is unavailable.

To configure authentication survivability on a Branch Gateway, complete the following procedure:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
    - To configure a Branch Gateway group or VPNC group, complete the following steps:
        a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
        b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
        c. Click **Config**.
        The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
    a. Set the filter to **Global** or a group containing at least one Branch Gateway.
    b. Under **Manage**, click **Devices** > **Gateways**.
       A list of gateways is displayed in the List view.
    c. Click a gateway under **Device Name**.
       The dashboard context for the gateway is displayed.
    d. Under **Manage**, click **Device**.
       The gateway device configuration page is displayed.

2. Click **Security > Auth Servers.**
3. Click the **Authentication Survivability** drop-down and slide the toggle switch next to **Enable authentication survivability**.
4. Select a value within the range of 1 to 7 days from the **Local cache lifetime** drop-down to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again.
5. From the **CA Certificate** drop-down, select the client's CA certificate to be configured as Trusted CA cert on the Gateway device. You can add multiple CA certificates in this field.
6. From the **CA Certificate** drop-down, select the client's CA certificate to be configured as Trusted CA cert on the Gateway device. You can add multiple CA certificates in this field.
7. From the **Authentication server certificate** drop-down, select a server certificate used by the local survival server to terminate EAP-TLS for 802.1X authentication.
8. Click **Save Settings**.

Authentication Survivability is supported in deployments where the SD-WAN gateway is used as an authenticator.
Authentication Survivability is not supported in deployments where the SD-WAN gateway is used for stateful 802.1x authentication

Configuring Server Groups

You can create server groups to distinguish authentication servers and for the ease of use. For example, you can configure a server group based on the following criteria:

- User authentication—Servers that authenticate client devices.
- Management authentication—Servers that authenticate management users such as the Branch Gateway admin.
- Accounting—Servers that support accounting.

Accounting is supported only with RADIUS and TACACS servers.

To add a server group:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
    - To configure a Branch Gateway group or VPNC group, complete the following steps:
        a. Set the filter to a group containing at least one Branch Gateway.
           The dashboard context for a group is displayed.

b. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
c. Click **Config**.
   The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. Click **Security** > **Auth Servers**.
3. Under **Server**, click the **+** icon to add a new server.
4. Enter the **Name** of the server group.
5. Click **Submit**.
6. From the **Server Groups** list, select a server group and assign the servers.
7. Click **Save Settings**.

Creating a AAA Profile

To configure a AAA profile:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Security** > **Role Assignment (AAA Profiles)**.
4. Select **AAA** under **AAA Profiles**.

5. Click **+** under **AAA Profile: New Profile** to define AAA profile settings.
6. Enter a name for the profile in the **Profile name** field, then configure the AAA profile parameters described in Table 272.

Table 272: *AAA Profile Parameters*

Parameter	Description
Initial role	Assigns role for the unauthenticated users. The default role for unauthenticated users is **logon**.
MAC authentication default role	Assigns role after the client device completes MAC authentication. The default role for MAC authentication is the **guest** user role.
802.1X authentication default role	Assigns role after the client device completes 802.1X authentication.
Download role from CPPM	Allows Aruba Gateways to download roles from Clear Pass Policy Manager.
Set username from dhcp option 12	Assigns a user name from DHCP option 12.
l2 authentication fail through	When MAC authentication fails and if 802.1X authentication method is configured, client devices are assigned roles after they complete 802.1x authentication.
Multiple server accounting	Enables SD-WAN Gateways to send accounting messages to all the servers configured in the server group in a sequential order.
User idle timeout	Configures a session time out value for inactive user sessions. A value of 0, deletes the user immediately after disassociation from the wireless network. Valid range is 30-15300 in multiples of 30 seconds. Specifying a value overrides the global settings configured in the AAA timers.
RADIUS roaming accounting	Creates an accounting session for each client. The records in the session contain the same set of RADIUS attributes as compared to the timer-based RADIUS Interim-Update Accounting record, except the statistics attributes.
RADIUS interim accounting	Enables Branch Gateway to send Interim-Update messages with current user statistics to the server at regular intervals. This option is disabled by default, allowing the Branch Gateway to send only start and stop messages to the RADIUS accounting server.
RADIUS acct-session-id in access-request	An accounting ID for the start and stop record of the session. This option is disabled by default.
User derivation rules	Specifies a profile from which the user role or VLAN is derived.
Reauthenticate wired user on VLAN change	Enable this feature to keep users authenticated when they roam from the wired side of the network. This feature is disabled by default.

Parameter	Description
Device type classification	Allows SD-WAN Gateways to parse user-agent strings and attempt to identify the type of device connecting to the AP.
Enforce DHCP	Allows clients to obtain IP from DHCP before associating to an AP. Enable this option when you create a user rule that assigns a specific role or VLAN based upon the client device's type.
PAN firewalls Integration	Requires IP mapping at Palo Alto Networks firewalls.
Apply ageout mechanism on bridge mode wireless clients	Enable this feature for the bridge entry to not age out as long as the wireless client is associated with the AP. The bridge entry is deleted only when the wireless client is deleted. This feature is disabled by default.

7. Click **Save Settings**.
8. Assign AAA policy to VLAN interfaces.

Configuring Authentication Timers

To set an authentication timer, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Advanced**.
3. Click **Authentication Timers**.

4. Configure the timers as described in Table 273:

Table 273: *Authentication Timers Parameters*

Timer	Description
User idle timeout	Maximum period after which a client is considered idle if there is no wireless traffic from the client. The timeout period is reset if there is wireless traffic. If there is no wireless traffic in the timeout period, the client is aged out. Once the timeout period has expired, the user is removed. If the keyword **seconds** is not specified, the value defaults to minutes at the command line. Range: 1–255 minutes (30–15300 seconds) Default: 5 minutes (300 seconds)
Authentication server dead time (min)	Maximum number of minutes after which the Branch Gateway considers an unresponsive authentication server to be *out of service*. This timer is only applicable if there are two or more authentication servers configured on a Branch Gateway. If there is only one authentication server configured, the server is never considered out of service, and all requests are sent to the server. If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as **DOWN** for the dead time. Range: 0–50 minutes Default: 10 minutes
Logon user lifetime (min)	Maximum time, in minutes, for which all unauthenticated clients are allowed to remain logged on. Range: 0–255 minutes Default: 5 minutes
User interim stats frequency	Sets the timeout value (in minutes or seconds) for user statistics and reporting. Range: 300–600 seconds, or 5–10 minutes Default: 600 seconds

5. Click **Save Settings**.

L2 Authentication

Wi-Fi networks have multiple authentication methods available for use. Each method depends on the network goals, security requirements, user types, and client types that access the network. Authentication is typically separated into two models, Layer 2 and Layer 3. These models can be combined for additional authentication.

The following sections describe the different L3 authentication methods:

- 802.1X Authentication
- MAC Authentication
- Stateful 802.1X Authentication

802.1X Authentication

802.1X is an IEEE standard that provides an authentication framework for WLANs. 802.1X uses the EAP to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework that are suitable for wireless networks include EAP-TLS, PEAP, and EAP-TTLS. These

protocols allow the network to authenticate the client while also allowing the client to authenticate the network.

This section describes the following topics:

- Understanding 802.1X Authentication
- Configuring 802.1X Authentication
- Performing Advanced Configuration Options for 802.1X

Understanding 802.1X Authentication

802.1X authentication consists of three components:

- The *supplicant*, or client is the device attempting to gain access to the network. You can configure the Aruba user-centric network to support 802.1X authentication for wired users and wireless users.
- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants.
- The *Branch Gateway* acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type must be consistent between the authentication server and supplicant, and is transparent to the Branch Gateway.

The authentication server provides a database of information required for authentication, and informs the authenticator to deny or permit access to the supplicant.

The 802.1X authentication server is typically an EAP-compliant RADIUS server which can authenticate either users (through passwords or certificates) or the client computer.

An example of an 802.1X authentication server is the IAS in Windows (see http://technet.microsoft.com/enus/library/cc759077(WS.10).aspx).

In Aruba user-centric networks, you can terminate the 802.1X authentication on the Branch Gateway. The Branch Gateway passes user authentication to its internal database or to a backend non-802.1X server. This feature, also called AAA FastConnect, is useful for deployments where an 802.1X EAP-compliant RADIUS server is not available or required for authentication.

Supported EAP Types

The following is the list of supported EAP types:

- PEAP — PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with the server. The PEAP authentication creates an encrypted SSL or TLS tunnelbetween the client and the authentication server. The exchange of information is encrypted and stored in the tunnel to ensure that the user credentials are kept secure.
- EAP-GTC—The EAP-GTC type uses clear text method to exchange authentication controls between the client and the server. Since the authentication mechanism uses the one-time tokens (generated by the card), this method of credential exchange is considered safe. In addition, EAP-GTC is used in PEAP or TTLS tunnels in wireless environments. The EAP-GTC is described in RFC 2284.
- EAP-AKA—The EAP-AKA authentication mechanism is typically used in mobile networks that include UMTS and CDMA 2000. This method uses the information stored in the SIM for authentication. The EAP-AKA is described in RFC 4187.
- EAP-FAST—The EAP-FAST is an alternative authentication method to PEAP. This method uses the PAC for verifying clients on the network. The EAP-FAST is described in RFC 4851.
- EAP-MD5—The EAP-MD5 method verifies MD5 hash of a user password for authentication. This method is commonly used in a trusted network. The EAP-MD5 is described in RFC 2284.
- EAP-POTP—The EAP type 32 is supported. Complete details are described in RFC 4793.

- EAP-SIM—The EAP-SIM uses GSM SIM for authentication and session key distribution. This authentication mechanism includes network authentication, user anonymity support, result indication, and fast reauthentication procedure. Complete details about this authentication mechanism is described in RFC 4186.
- EAP-TLS—The EAP-TLS uses PKI to set up authentication with a RADIUS server or any authentication server. This method requires the use of a client-side certificate for communicating with the authentication server. The EAP-TLS is described in RFC 5216.
- EAP-TLV—The EAP-TLV method allows you to add additional information in an EAP message. Often this method is used to provide more information about an EAP message such as status information or authorization data. This method is always used after a typical EAP authentication process.
- EAP-TTLS—The EAP-TTLS method uses server-side certificates to set up authentication between clients and servers. The actual authentication is, however, performed using passwords. Complete details about EAPTTLS is described in RFC 5281.
- LEAP— LEAP uses dynamic WEP keys and mutual authentication between the client and the RADIUS server.
- ZLXEAP—ZoneLabs EAP is an EAP method that has been allocated EAP Type 44 by IANA. For more information, visit http://tools.ietf.org/html/draft-bersani-eap-synthesis-sharedkeymethods-00#page-30.

Configuring Authentication with a RADIUS Server

For an overview of the parameters that you need to configure on authentication components when the authentication server is an 802.1X EAP-compliant RADIUS server, see Configuring 802.1X Authentication on page 1.

The supplicant and the authentication server must be configured to use the same EAP type. The Branch Gateway does not need to know the EAP type used between the supplicant and authentication server.

For the Branch Gateway to communicate with the authentication server, you must configure the IP address, authentication port, and accounting port of the server on the Branch Gateway. The authentication server must be configured with the IP address of the RADIUS client, which is the Branch Gateway in this case. Both the Branch Gateway and the authentication server must be configured to use the same shared secret.

Additional information on EAP types supported in a Windows environment, Microsoft supplicants, and authentication servers, is available at http://technet.microsoft.com/en-us/library/cc782851(WS.10).aspx.

The client communicates with the Branch Gateway through a GRE tunnel to form an association with an AP and to get authenticated in the network. Therefore, the network authentication and encryption configured for an ESSID must be the same on both the client and the Branch Gateway.

Configuring Authentication Terminated on Branch Gateway

User authentication is performed either via the Branch Gateway's internal database or a non-802.1X server. For an overview of the parameters that you need to configure on 802.1X authentication components when802.1X authentication is terminated on the Branch Gateway (AAA FastConnect), see Configuring 802.1X Authentication on page 1.

In a scenario where the supplicant is configured for EAP-TLS or EAP-PEAP.

- EAP-TLS is used with smart card user authentication. A smart card holds a digital certificate which, with the user-entered PIN, allows the user to be authenticated on the network. EAP-TLS relies on digital certificates to verify the identities of both the client and the server.

  EAP-TLS requires that you import server and CA certificates onto the Branch Gateway (for more information see, Configuring 802.1X Authentication on page 1). The client certificate is verified on the

Branch Gateway (the client certificate must be signed by a known CA) before the username is checked on the authentication server.

- EAP-PEAP uses TLS to create an encrypted tunnel. Within the tunnel, one of the following "inner EAP" methods is used:
  - EAP-GTC: Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of an LDAP or RADIUS server as the user authentication server. You can also enable caching of user credentials on the Branch Gateway as a backup to an external authentication server.
  - EAP-Microsoft MS-CHAPv2: Described in RFC 2759, this EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the backend authentication server.

If you use the internal database of the Branch Gateway for user authentication, you need to add the names and passwords of the users to be authenticated. If you use an LDAP server for user authentication, you need to configure both the LDAP server and the user IDs and passwords on the Branch Gateway. If you use a RADIUS server for user authentication, you need to configure the RADIUS server on the Branch Gateway.

Configuring 802.1X Authentication

On the Branch Gateway, use the following steps to configure a wireless network that uses 802.1X authentication:

1. Configure the VLANs to which the authenticated users will be assigned.
2. Configure policies and roles. You can specify a default role for users who are successfully authenticated using 802.1X. You can also configure server derivation rules to assign a user role based on attributes returned by the authentication server; server-derived user roles take precedence over default roles.

The Policy Enforcement Firewall Virtual Private Network module provides identity-based security for wired and wireless users and must be installed on the Branch Gateway. The stateful firewall allows user classification based on user identity, device type, location, and time of day to provide differentiated access for different classes of users.

3. Configure the authentication server(s) and server group. The server can be an 802.1X RADIUS server or, if you use AAA FastConnect, a non-802.1X server or the internal database of the Branch Gateway. If you use EAP-GTC within a PEAP tunnel, configure an LDAP or RADIUS server as the authentication server. If you use EAP-TLS, import server and CA certificates on the Branch Gateway.
4. Configure the AAA profile:
   a. Select the 802.1X default user role.
   b. Select the server group you previously configured for the 802.1X authentication server group.
5. Configure the 802.1X authentication profile.
6. Configure the virtual AP profile for an AP group or for a specific AP:
   a. Select the AAA profile you previously configured.
   b. In the SSID profile, configure the WLAN for 802.1X authentication.

Configuring a new instance of an 802.1X authentication profile in the WebUI:

1. Configure a Branch Gateway group or a Branch Gateway:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
   - To configure a Branch Gateway, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Security** > **L2 Authentication**.
4. In the L2 Authentication table, select **802.1X Authentication Profile**.
5. Click **+** in the **802.1X Authentication Profile: New Profile**.
6. Change the settings described in the following table and click **Save Settings**.
7. Enter a name for the new profile in the **Profile Name** field.

Table 274: *802.1X Authentication Profile WebUI Parameters*

Parameter	Description
Max Authentication Failures	Number of times a user can try to log in with wrong credentials after which the user is blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. Range: 0-5 failures. Default: 0 failure. **NOTE:** This option may require a license.
Enforce Machine Authentication	Select the Enforce Machine Authentication option to require machine authentication. This option is also available on the Basic settings tab. **NOTE:** This option may require a license.
Machine Authentication Default Machine Role	Default role assigned to the user after 802.1X authentication. The default role for this setting is the guest role.
Machine Authentication Cache Timeout	The timeout, in hours, for machine authentication. The allowed range of values is 1- 1000 hours, and the default value is 24 hours.

Table 274: *802.1X Authentication Profile WebUI Parameters*

Parameter	Description
Blacklist on Machine Authentication Failure	Select this check box to blacklist a client if machine authentication fails. This setting is disabled by default.
Machine Authentication Default User Role	Default role assigned to the user after completing only machine authentication. The default role for this setting is the *guest* role.
Interval between Identity Requests	Interval, in seconds, between identity request retries. Range: 1-65535 seconds. Default: 5 seconds.
Quiet Period afterFailed Authentication	The enforced quiet period interval, in seconds, following failed authentication. Range: 1-65535 seconds. Default: 30 seconds.
Reauthentication Interval	Interval, in seconds, between reauthentication attempts. Range: 60-864000 seconds. Default: 86400 seconds (1 day).
Use Server provided Reauthentication Interval	Select this option to override any user-defined reauthentication interval and use the reauthentication period defined by the authentication server.
Multicast Key RotationTime Interval	Interval, in seconds, between multicast key rotation. Range: 60-864000 seconds. Default: 1800 seconds.
Unicast Key RotationTime Interval	Interval, in seconds, between unicast key rotation. Range: 60-864000 seconds. Default: 900 seconds.
Authentication ServerRetry Interval	Server group retry interval, in seconds. Range: 2-65535 seconds. Default: 5 seconds.
Authentication ServerRetry Count	Maximum number of authentication requests that are sent to server group. Range: 0-5 requests. Default: 3 requests.
Framed MTU	Sets the framed MTU attribute sent to the authentication server. Range: 500-1500 bytes. Default: 1100 bytes.
Max number of requestssent during an Auth attempt	Maximum number of times ID requests are sent to the client. Range: 1-10 retries. Default: 3 retries.

Table 274: *802.1X Authentication Profile WebUI Parameters*

Parameter	Description
Maximum Number of Reauthentication Attempts	Number of times a user can try to log in with wrong credentials after which the user is blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a value from 0-5 to blacklist the user after the specified number of failures. **NOTE:** If changed from its default value, this option may require a license.
Maximum number oftimes Held State can be bypassed	Number of consecutive authentication failures which, when reached, causes the Branch Gateway to not respond to authentication requests from a client while the Branch Gateway is in a held state after the authentication failure. Before this number is reached, the Branch Gateway responds to authentication requests from the client even while the Branch Gateway is in its held state. (This parameter is applicable when 802.1X authentication is terminated on the Branch Gateway, also known as AAA FastConnect.) The allowed range of values for this parameter is 0-3 failures, and the default value is 0.
Dynamic WEP KeyMessage Retry Count	Set the Number of times WPA or WPA2 key messages are retried. Range: 1-5 retries. Default: 3 retries.
Dynamic WEP Key Size	The default dynamic WEP key size is 128 bits, If desired, you can change this parameter to 40 bits.
Interval between WPA/WPA2 Key Messages	Interval, in milliseconds, between each WPA key exchanges. Range: 1000-5000 ms. Default: 1000 ms.
Delay between EAP Successand WPA2 Unicast Key Exchange	Interval, in milliseconds, between EAP-Success and unicast key exchanges. Range: 0-2000 ms. Default: 0 ms (no delay).
Time interval afterwhich the PMKSA will be deleted	The time interval after which the PMKSA cache is deleted. Time interval in Hours. Range: 1-2000. Default: 8.
WPA/WPA2 Key MessageRetry Count	Number of times WPA or WPA2 key messages are retried. Range: 1-5 retries. Default: 3 retries.
Multicast Key Rotation	Select this check box to enable multicast key rotation. This feature is disabled by default.
Unicast Key Rotation	Select this check box to enable unicast key rotation. This feature is disabled by default.
Reauthentication	Select the Reauthentication check box to force the client to do a 802.1X reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.) If the user fails to reauthenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1X-authenticated users, then the reauthentication timer per role overrides this setting. **NOTE:** This option is disabled by default.

Table 274: *802.1X Authentication Profile WebUI Parameters*

Parameter	Description
Opportunistic KeyCaching	By default, the 802.1X authentication profile enables a cached PMK which is derived through a client and an associated AP. This key is used when the client roams to a new AP. This allows clients faster roaming without a full 802.1X authentication. Uncheck this option to disable this feature. **NOTE:** Make sure that the wireless client (the 802.1X supplicant) supports this feature. If the client does not supportthis feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the Branch Gateway can be out of sync with the key of the client.
Validate PMKID	This parameter instructs the Branch Gateway to check the PMK ID sent by the client. When you enable this option, the client must send a PMK ID in the associate or reassociate frame to indicate that it supports OKC or PMK caching; otherwise, full 802.1X authentication takes place. **NOTE:** This feature is optional, since most clients that support OKC and PMK caching do not send the PMK ID in their association request.
Use Session Key	Select this check box for the Branch Gateway to use a RADIUS session key as the unicast WEP key.
Use Static Key	Select this check box for the Branch Gateway to use a static key as the unicast/multicast WEP key.
xSec MTU	Displays the size of the MTU for xSec.
Termination EAP-Type	If you enable termination, click either EAP-PEAP or EAP-TLS to select a EAP method.
Termination Inner EAP-Type	If you use EAP-PEAP as the EAP method, specify one of the following inner EAP types: ■ **eap-gtc**: Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the Branch Gateway as a backup to an external authentication server. ■ **eap-mschapv2**: Described in RFC 2759, this EAP method is widely supported by Microsoft clients.
Token Caching	If you select EAP-GTC as the inner EAP method, you can select the Token Caching check box to enable the Branch Gateway to cache the username and password of each authenticated user. The Branch Gateway continues to reauthenticate users with the remote authentication server. However, if the authentication server is unavailable, the Branch Gateway will inspect its cached credentials to reauthenticate users. This option is disabled by default.
Token Caching Period	If you select EAP-GTC as the inner EAP method, you can specify the timeout period, in hours, for the cached information. The default value is 24 hours.
CA-Certificate	Click the **CA-Certificate** drop-down list and select a certificate for client authentication. The CA certificate needs to be loaded in the Branch Gateway before it will appear on this list.
Server-Certificate	Gateway will use to authenticate itself to the client.

Table 274: *802.1X Authentication Profile WebUI Parameters*

Parameter	Description
	NOTE: By default, the **default-self-signed** certificate is used as server certificate.
TLS Guest Access	Select **TLS Guest Access** to enable guest access for EAP-TLS users with valid certificates. This option is disabled by default.
TLS guest role	Click the TLS Guest Role drop-down list and select the default user role for EAP-TLS guest users. This option may require a license.
Ignore EAPOL-STARTafter authentication	Select Ignore EAPOL-START after authentication to ignore EAPOL-START messages after authentication. This option is disabled by default.
Handle EAPOL-Logoff	Select Handle EAPOL-Logoff to enable handling of EAPOL-LOGOFF messages. This option is disabled by default.
Ignore EAP ID duringnegotiation	Select Ignore EAP ID during negotiation to ignore EAP IDs during negotiation. This option is disabled by default.
WPA-Fast-Handover	Select this option to enable WPA-fast-handover on phones that support this feature. WAP fast-handover is disabled by default.
Check certificate common name against AAA server	If you use client certificates for user authentication, enable this option to verify that the common name of the certificate exists in the server. This parameter is enabled by default in the default-cap and default-rap VPN profiles, and disabled by default on all other VPN profiles.

MAC Authentication

This section describes how to configure MAC-based authentication on the VPN Concentrator using the WebUI.

Use MAC-based authentication to authenticate devices based on their physical MAC address. Although this not the most secure and scalable method, MAC-based authentication implicitly provides an additional layer of security to authenticate devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest. For example, if clients are allowed access to the network through station A, then one method of authenticating station A is MAC-based. Clients may be required to authenticate themselves using other methods depending on the network privileges required.

MAC-based authentication can also be used to authenticate Wi-Fi phones as an additional layer of security to prevent other devices from accessing the voice network using what is normally an insecure SSID.

Before configuring MAC-based authentication, you must configure the following options:

- User role—The user role that will be assigned as the default role for the MAC-based authenticated clients.

  Configure the default user role for MAC-based authentication in the AAA profile. If derivation rules exist or if the client configuration in the internal database has a role assigned, these values take precedence over the default user role.
- Authentication server group—The authentication server group that the Branch uses to validate the clients. The internal database can be used to configure the clients for MAC-based authentication.

Configuring the MAC Authentication Profile

To configure MAC-based authentication, perform the following steps:

1. In the **Network Operations** app, complete either of the following steps:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.

     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
   - To configure a Branch Gateway, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the List view.

     c. Click a gateway under **Device Name**.

        The dashboard context for the gateway is displayed.

        The gateway device configuration page is displayed.
2. Click **Security** > **L2 Authentication**.
3. In the **MAC Authentication Profile: New Profile** section, click **+** to create a new profile.
4. Enter a profile name in the **Profile name** text box.
5. Click **Save Settings**.

Parameter	Description
Profile name	Name of the MAC authentication profile.
Delimiter	Delimiter used in the MAC string: ■ colon specifies the format XX:XX:XX:XX:XX:XX ■ dash specifies the format XX-XX-XX-XX-XX-XX ■ none specifies the format XXXXXXXXXXXX ■ oui-nic specifies the format XXXXXX-XXXXXX Default: none **NOTE:** This parameter is available for the aaa authentication-server radius command.
Case	The case (upper or lower) used in the MAC string. Default: lower
Max authentication failures	Number of times a station can fail to authenticate before it is blacklisted. A value of zero disables blacklisting. Default: zero (0)
Reauthentication	Select the Reauthentication check box if you want to enable Reauthentication. Default: disable.
Reauthentication interval	Time duration between reauthentication attempts. Configure a value in the range of 60–86400. Reauthentication timer is configured in terms of seconds.
Use server provided reauthentication interval	Select the Use server provided reauthentication interval check box to use the interval provided by the server. Default: disable.

Stateful 802.1X Authentication

The VPN Concentrator supports Stateful 802.1X authentication. This feature allows the VPN Concentrator to learn the identity and role of a user connected to an AP, and is useful for authenticating users to networks with APs from multiple vendors. When an 802.1X-capable access point sends an authentication request to a RADIUS server, the VPN Concentrator inspects this request and the associated response to learn the authentication state of the user. It then applies an identity-based user role through the Policy Enforcement Firewall.

When configuring 802.1X authentication for clients on non-Aruba APs, you must specify the group of RADIUS servers that performs user authentication and assign roles to users who successfully complete authentication. When the user logs off or shuts down the client machine, VPN Concentrator notes the deauthentication message from the RADIUS server and changes the user's role from the specified authenticated role back to the login role.For details on defining a RADIUS server used for stateful 802.1X authentication, see Configuring RADIUS Authentication Server on Aruba Gateways.

To configure the Stateful 802.1X Authentication:

1. In the **Network Operations** app, complete either of the following steps:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
   - To configure a Branch Gateway, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.

        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.

        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Security** > **L2 Authentication**.
4. Under the **L2 Authentication** tab, select **Stateful 802.1X Authentication**.
5. Select the role assigned to stateful 802.1X authenticated users from the **Default Role** drop-down list.
6. Specify the **Timeout** period for authentication requests, between 1 and 20 seconds. The default value is 10 seconds.
7. Select the **Enable** check box to enable stateful 802.1X authentication.
8. Click **Server Group** under **L2 Authentication** > **Stateful 802.1X Authentication** to configure server groups to be used for stateful 802.1X authentication.
9. Select the server groups from the **Server Group** drop-down list.
10. To enable authentication fail through and load balancing, select the check boxes for **Fail Through** and **Load Balance**.
11. Click **Save Settings**.

L3 Authentication

The following sections describe the different L3 authentication methods:

- Captive Portal Authentication
- VIA Authentication on page 1229
- VPN Authentication

Captive Portal Authentication

Captive portal is one of the methods of authentication supported by ArubaOS. A captive portal presents a web page which requires user action before network access is granted. The required action can be simply viewing and agreeing to an Acceptable Usage Policy, or entering a user ID and password which must be validated against a database of authorized users.

You can configure captive portal for guest users, where no authentication is required, or for registered users who must be authenticated against an external server or the internal database of the Branch Gateway.

While you can use captive portal to authenticate users, it does not provide for encryption of user data and should not be used in networks where data security is required. Captive portal is most often used for guest access, access to open systems (such as public hot spots), or as a way to connect to a VPN.

The following sections present the procedure for configuring the captive portal authentication profile.

To configure captive profile authentication parameters:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **L3 Authentication**.
3. Select **Captive Portal Authentication** profile.
   a. Click **+** to create a new Captive Portal Authentication Profile, enter the name of the profile.
   b. You can enable user login and guest login, and configure other captive portal profile parameters

as described in Table 275.

c. Click **Save Settings**.

Table 275: *Captive Portal Authentication Profile Parameters*

Parameter	Description
Default Role	Role assigned to the Captive Portal user upon login. When both user and guest logon are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the guest role. Default: guest
Default Guest Role	Role assigned to guest. Default: guest
Redirect Pause	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link. Default: 10 seconds
User Login	Enables Captive Portal with authentication of user credentials. Default: Enabled
Guest Login	Enables Captive Portal logon without authentication. Default: Disabled
Logout popout window	Enables a pop-up window with the Logout link for the user to logout after logon. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station reloads. Default: Enabled
Use HTTP for authentication	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captive portal policy to allow HTTP traffic. Default: disabled (HTTPS is used)
Logon wait minimum wait	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter. Default: 5 seconds
Logon wait maximum wait	Configure parameters for the logon wait interval. Default: 10 seconds
Logon wait CPU utilization threshold	CPU utilization percentage above which the Logon wait interval is applied when presenting the user with the logon page. Default: 60%
Max Authentication failures	Maximum number of authentication failures before the user is denylisted. Default: 0
Show FQDN	Allows the user to see and select the FQDN on the login page. The FQDNs shown are specified when configuring individual servers for the server group used with captive portal authentication. Default: Disabled
Authentication	Select the PAP, CHAP or MS-CHAPv2 authentication protocol.

Parameter	Description
Protocol	**NOTE:** Do not use the CHAP = option unless instructed to do so by an Aruba representative.
Login Page	URL of the page that appears for the user logon. This can be set to any URL. Default: `/cgi-bin/login?cmd=authenticate` or `/cgi-bin/login?cmd=login`
Welcome Page	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL. Default: /auth/welcome.html
Show Welcome Page	Displays the configured welcome page before the user is redirected to their original URL. If this option is disabled, users are redirected to the web URL immediately after they log in. Default: Enabled
Proxy server configuration	Configure captive portal to work with proxy Web servers. Enter the address and port details of the proxy server.
Add gateway IP in redirection URL	Sends the IP address of the Branch Gateway in the redirection URL when external captive portal servers are used. An external captive portal server can determine the Branch Gateway from which a request originated by parsing the 'switchip' variable in the URL. Default: Disabled
Add user vlan in the redirection URL	Sends the user VLAN ID in the redirection URL when external captive portal servers are used.
Add a gateway interface in the redirection URL	Sends the interface IP address of the Branch Gateway in the redirection URL when external captive portal servers are used. An external captive portal server can determine the Branch Gateway from which a request originated by parsing the 'switchip' variable in the URL.
Allow only one active user session	Allows only one active user session at a time. Default: Disabled
White List	To add a netdestination to the captive portal whitelist, enter the destination host or subnet, then click **Add.** The netdestination will be added to the whitelist. To remove a netdestination from the whitelist, select it in the whitelist field, then click **Delete**. If you have not yet defined a netdestination, use the CLI command **netdestination** to define a destination host or subnet before you add it to the whitelist. This parameter requires a PEFNG license.
Black List	To add a netdestination to the captive portal blacklist, enter the destination host or subnet, then click **Add**. The netdestination will be added to the blacklist. To remove a netdestination from the blacklist, select it in the blacklist field, then click **Delete**. If you have not yet defined a netdestination, use the CLI command **netdestination** to define a destination host or subnet before you add it to the blacklist.
Show Acceptable Use Policy Page	Show the acceptable use policy page before the logon page. Default: Disabled

Parameter	Description
User idle timeout	The user idle timeout value for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.
Redirect URL	URL to which an authenticated user will be directed. This parameter must be an absolute URL that begins with either **http://** or **https://**.
URL Hash Key	If a redirection URL is defined, enter a URL Hash Key to hash the redirect URL using the specified key. This parameter enhances security for the ClearPass Guest login URL so that ClearPass Policy Manager can trust and ensure that the client MAC address in the redirect URL has not been tampered with by anyone. Default: Disabled.

VIA Authentication

For detailed information on the Aruba VIAsolution, see Configuring Support for Aruba VIA Service on page 1389

Configuring VIA Authentication Profile

The VIA authentication profile defines the authentication server group used and the default role assigned to the authenticated users. Multiple authentication profiles can be created. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile.

The VIA authentication profile is a critical part of VIA configuration and it is used for these purposes:

- To determine the authentication server for the XAUTH authentication phase of IKEv1 and EAP authentications of IKEv2.
- To determine the authentication server for the VIA web authentication. The VIA authentication profile is an integral part of the VIA web authentication, which determines the authentication sever used for VIA bootstrap process and for authenticating users on the VIA installer download page of the VPNC. For more information on VIA web authentication, see Configuring VIA Web Authentication.

To configure a VIA authentication profile, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

        The dashboard context for a group is displayed.

     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.

     c. Click **Config**.

        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the List view.

c. Click a gateway under **Device Name**.

   The dashboard context for the gateway is displayed.

d. Under **Manage**, click **Device**.

   The gateway device configuration page is displayed.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Security > L3 Authentication**.
4. Select **VIA Authentication**.
5. Click **+** to create a new VIA authentication profile or select an existing profile. You can also use the predefined **default** VIA authentication profile.
6. After selecting the required profile, select the role that you defined for the VIA users in the **Default role** field. For more information on configuring the other parameters for this profile, see Table 276.
7. Select the required server group for authentication from the appropriate server group option under the selected profile. The server group options are **RADIUS Accounting Server Group**, **RFC 3576 Server**, and **Server Group**. Optionally you can configure the following options for the selected server group:
   - **Fail through**—Enables the fail through option for the server group.
   - **Load balance**—Enables load balancing among the servers for authentication requests.
8. Save the changes.

Table 276: *VIA Authentication Profile Parameters*

Parameter	Description
Default Role	Select the role that you want to be assigned as the default role for the client when authenticating using this profile. By default, the default-via-role is assigned.
Max Authentication failures	Maximum number of authentication failures allowed for the client. Allowed range is 1-10 and the default value is 0.
Description	Description of the authentication profile.
Check certificate common name against AAA server	Select this option to check for certificate common name against the AAA server. Default: enabled.
Client-certificate based authentication for VIA Profile download	Select this option to enable client-certificate based authentication for VIA Profile download. By default, this is disabled.
Authentication protocol	Select the authentication protocol to be used. The default value is PAP.
Download Role from CPPM	Select this option to download the default role from ClearPass Policy Manager, if the default role is not defined.

Configuring VIA Connection Profile

The VIA connection profile is a collection of all the configurations required by a VIA client. The VIA connection profile contains all the details required for the VIA client to establish a secure IPsec connection to the VPNC. A VIA connection profile also defines other optional parameters. Such optional parameters can be client auto-login, split-tunnel settings, and Content Security Services (CSS) settings. You can configure multiple VIA connection profiles.

A VIA connection profile is always associated to a user role, and all users that belong to that role use the configured settings. When a user authenticates successfully to a server in an authentication profile, the VIA client downloads the VIA connection profile that is attached to the role assigned to that user.

Table 277 summarizes the various parameters of a VIA connection profile .

To configure a VIA connection profile, complete the following steps:

1. In the **Network Management** app, use the filter to select a VPNC group or VPNC.
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security > L3 Authentication**.
3. Select **VIA Connection**.
4. Click **+** to create a new VIA connection profile or select an existing profile. You can also use the predefined **default**VIA connection profile.
5. After selecting the required profile, configure the various VIA connection profile parameters as described in Table 277
6. Save the changes.

Table 277: *VIA Connection Profile Parameters*

Parameter	Description
VIA servers	This parameter has the following fields: ■ **Addr**—Add the public IP or DNS hostname of the VPNC. This is the host name or IP address that the users enter as the remote server information on the VIA client. ■ **Internal IP**—Add the IP address of any of the internal VLAN interfaces of the VPNC. This IP address should not be reachable from the public Internet. The VIA client uses this IP address to determine whether or not the user is connected to a trusted network. ■ **Description**—Add a human-readable description of the VIA server. **NOTE:** More than one VIA server can be added to the list.

Parameter	Description
Client auto-login	Enabling client auto-login makes the VIA client detect untrusted network and connect automatically. If you disable auto-login, VIA stays idle after it comes up and the user has to manually click **Connect** to establish a VPN connection even though an untrusted network is detected. Default: enabled
VIA authentication profiles to provision	This VIA authentication profile is used to determine the authentication server used for the IKE authentication process. If more than one VIA authentication profile is added to this list, the users can choose the VIA authentication profile to be used during IKE authentication. If no VIA authentication profile is defined, the users are authenticated against the server group that is specified by the default VIA authentication profile (predefined).
Allow client to auto-upgrade	This parameter allows the VIA client to automatically upgrade if a newer version of VIA is available on the VPNC. By default this is enabled.
VIA tunneled networks	When split-tunneling is enabled, the VIA client tunnels traffic to the VPNC for all the network destinations (IP address and netmask) listed in this parameter. All other network destinations are bridged appropriately on the client. If split-tunnel is disabled, all the traffic is tunneled to the VPNC irrespective of the destination.
Enable split tunneling	When enabled, all traffic to the VIA tunneled networks goes through the VPNC and the rest is bridged directly on the client. If split-tunnel is disabled, all the traffic is tunneled to the VPNC irrespective of the destination.
Allow client-side logging	This parameter determines whether client side logging is allowed or not. If enabled, VIA client collects logs that can be sent to the support email address for troubleshooting. Default: Enabled
VIA IKEv2 Policy	This IKE policy is used for IKEv2 connections by the VIA client. Remember that IKEv2 using PSK is not supported for VIA. For more information on configuring IKE policies, see Configuring IKE Policies.
VIA IKE Policy	This IKE policy is used for IKEv1 connections by the VIA client. This policy determines whether IKEv1 phase 1 authentication uses PSK or certificates. For more information on configuring IKE policies, see Configuring IKE Policies.
Use windows credentials	This parameter determines whether the Windows credentials are used automatically to login to VIA. If enabled, the single sign-on feature can be utilized by remote users to connect to internal resources. Default: Enabled
Enable IKEv2	This parameter enables or disables IKEv2.
Use suite b cryptography	This parameter enables or disables Suite B cryptographic methods.
IKEv2 authentication method	This parameter indicates the IKEv2 client authentication method. It can be one of these settings: l user-cert l EAP-TLS l EAP-MSCHAPv2 Remember that EAP termination on the VPNC is not supported.
VIA IPSec v2 crypto map	This IPsec map is used by IKEv2 VIA client to connect to the VPNC.

Parameter	Description
VIA IPSec crypto map	This IPsec map is used by IKEv1 VIA client to connect to the VPNC.
Allow user to save passwords	This parameter determines whether the users can save the passwords entered in VIA or not. If this is enabled, the user credentials that were able to successfully establish a VIA connection are saved securely until VIA is uninstalled or until IKE authentication fails with stored credentials. If this option is disabled, VIA prompts for credentials every time it establishes a connection. If secure tokens such as the RSA tokens are used for authentication, disable this option to prompt the user for a password/token for each connection attempt. By default, this is enabled.
Enable supplicant	This parameter enables the supplicant mode.
Enable FIPS module	This parameter enables the VIA FIPS module.
Auto-launch supplicant	This parameter automatically connects to the configured WLAN network.
Lockdown all settings	This parameter locks all the configuration options available on the end-user VIA client. If this option is enabled, a VIA user can only connect, disconnect or send logs. Diagnostics such as traceroute and ping can still be used, but no settings can be changed. **NOTE:** This option is available in VIA 2.1 and later versions.
Domain suffix in VIA authentication	This parameter enables domain suffix in VIA authentication.
Enable Controllers load balance	This parameter enables load balancing of VIA clients by randomly choosing a VPNC from the list of available VIA VPNCs that can be used for connection. This feature does not take the existing load of the VPNC into account. **NOTE:** This option is available in VIA 2.1 and later versions.
Enable domain pre-connect	This parameter enables pre-connection to the domain. By default, this is enabled.
VIA banner message reappearance timeout(minutes)	This parameter configures the timeout value in minutes for reappearance of VIA login banner message. The default value is 60 minutes.
VIA client network mask	This network mask is set on the client after the VPN connection is established. The default value is 255.255.255.255.
Validate server certificate	If enabled, the VIA client validates the server certificate presented by the VPNC during the IPsec process. Remember that to validate the server certificate, the CA that signed the VPNC certificate should be a trusted CA in the client certificate store. By default, this is enabled.
VIA client DNS suffix list	This is the DNS suffix that is set on the client after the VPN connection is established.

Parameter	Description
OCSP cert verification enabled	This parameter enables OCSP certificate verification.
In EAP/IKE, action taken when OCSP cert verification result is unknown	This parameter accepts the certificate when OCSP certificate verification result is unknown for EAP/IKEs.
VIA domain name profile	This parameter allows you to add VIA domain name profiles.
Destination traffic to be blocked	This parameter allows you to configure the IP address and netmask of the destination traffic for blocking.
Block-destination-traffic-selector (on/off)	This parameter enables or disables the blocking of destination traffic.
VIA max session timeout	This parameter defines the maximum time, in minutes, allowed before the VIA session is disconnected. Default: 1440 min
VIA logon script	This parameter specifies the name of the logon script that must be executed after VIA establishes a secure connection. The logon script must reside on the client computer.
VIA logoff script	This parameter specifies the name of the logoff script that must be executed after VIA tears down a secure connection. The logoff script must reside on the client computer.
VIA support e-mail address	This is the support email address to which VIA users send client logs using the VIA client. For information on sending VIA logs using the VIA client, see Chapter 8: Establishing VIA connection.
Maximum reconnection attempts	This parameter defines the maximum reconnection attempts by the VIA client. If the reconnection attempt is exceeded, the VIA client becomes idle. However, if the connection attempt fails due to an IKE authentication failure error, then the user is prompted to reenter username and password. Default: 3
VIA external download URL	The VIA installer can be hosted on an external server other than the VPNC for download by the VIA client during VIA upgrades and by the end users. If the VIA installer is hosted on an external server, this parameter should be configured to redirect the VIA clients to the external URL for the upgrade process. If this parameter is not configured, the VIA clients automatically go to https:// <VPNC IP address or FQDN >/via for upgrades.
Allow user to disconnect VIA	This feature determines whether the users can disconnect VIA or not. Remember that a user with administrative rights to a laptop can always uninstall VIA or disable the service running on the laptop. For users with restricted access to the laptops, disabling this feature ensures that users cannot disconnect VIA. By default, his is enabled.
Content security gateway URL	When split-tunnel mode is enabled, traffic to external websites is inspected by the CSS.

Parameter	Description
Comma separated list of HTTP ports to be inspected (apart fromdefault port 80)	Traffic to the specified list of ports is verified by the CSS provider.
Certificate criteria	Certificate criteria expressed in key-value pairs where keys can be certificate attributes, or certificate OIDs. Multiple key-value pairs can be combined with semi-colon.
Enable content security services	This parameter enables the CSS. The CSS requires the CSS licenses.
Keep VIA window minimized	When this feature is enabled, the VIA client is minimized to the system tray during the connection phase. This feature is applicable only for VIA clients installed on Microsoft Windows laptops. Default: disabled
Block traffic until VPN tunnel is up	This parameter allows blocking of traffic until VPN tunnel is up.
Block traffic rules	This parameter configures the VIA allowlist traffic rules. Specify the IP address, netmask and description for the traffic rules.
User idle timeout	User idle timeout value. Allowed range is 30-15300 seconds in multiples of 30 seconds.
VIA client mtu value	MTU value for the VIA client. Allowed range is 576-5120 bytes. The default value is 1452 bytes.

Attaching the VIA Connection Profile to User Role

VIA connection profile that the VIA client has to download should be attached to the user role to be assigned to the user. When a user goes through the authentication phase it is placed on a role which has a certain connection profile associated. Suppose, the users authenticating to the VIA authentication profile are assigned the **default-via-role**. To assign a specific connection profile to these users, attach the connection profile to the **default-via-role**.

To attach the VIA connection profile to a user role, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. Click **Security > Roles**.
5. Select the role to which you want to associate a VIA connection profile and select the **More** tab.
6. Expand **VPN** and select the required VIA connection profile from the **VIA connection profile** drop-down list.
7. Save the changes.

Configuring VIA Web Authentication

The VIA web authentication is a list of VIA authentication profiles. The web authentication list allows the users to login to the VIA download page <https://<VPNC IP address>/via> to download the VIA client. To successfully login to the VIA download page, the users must authenticate successfully against the VIA authentication profile in the list. If more than one VIA authentication profile is configured in the web authentication list, the users can view the list and select one authentication profile before authenticating to the VIA installer download page.

The web authentication list is also used during the initial user authentication process that determines the VIA user role. The Branch Gateway has a default web authentication list to which multiple VIA authentication profiles can be added. Additional VIA web authentication lists cannot be created.

To configure the VIA web authentication list, add one or more VIA authentication profiles to the default web authentication list and order them according to the priority. Configuring more than one VIA authentication profile in the VIA web authentication list allows the users to use the backup authentication server when the primary server becomes unavailable temporarily.

To configure the VIA web authentication profile, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - For a Branch Gateway group, in the **Network Operations** app, use the filter to select **Groups**.
   - For a Branch Gateway in the **Network Operations** app, use the filter to select the gateway.
2. Under **Manage**, click **Devices** > **Gateways**.
3. Click the Config configuration icon. The gateway configuration page is displayed.
4. Select **VIA Web Authentication** > **default**.
5. Click **+** to add a VIA authentication profile in the **VIA authentication profiles** table.
6. Save the changes.

VPN Authentication

Wireless networks can use VPN connections to further secure wireless data from attackers. A VPNC is used to terminate all VPN connections from both wired and wireless clients.

VPN Authentication Profiles

VPN authentication profiles identify an authentication server, the server group to which the authentication server belongs to, and a user-role for authenticated VPN clients. There are three predefined VPN authentication profiles: **default**, **default-cap**, **default-hp-switch**, **default-iap**, and **default-rap**. These different profiles allow you to use different authentication servers, user roles, and IP pools for VPN, remote AP, switches, Instant AP, and campus AP clients.

Table 278: *Predefined Authentication Profile settings*

Parameter	Description	default	*rap	*cap	*hp-switch	*iap
Default Role	The role that is assigned to the authenticated users.	default-vpn-role	default-vpn-role	sys-ap-role 0	default-vpn-role	default-vpn-role

Parameter	Description	default	*rap	*cap	*hp-switch	*iap
Maximum allowed authentication failures	The number of contiguous authentication failures before the station is denylisted.	0 (feature is disabled)	0 (feature is disabled)	0 (feature is disabled)	0 (feature is disabled)	0 (feature is disabled)
Check certificate common name against AAA server	When enabled, this feature verifies that the certificate's common name exists in the server.	disabled	enabled	enabled	enabled	enabled
Export VPN IP address as a route	When enabled, this feature causes any VPN client address to be exported to OSPF using IPC. **NOTE:** The **Framed-IP-Address** attribute is assigned the IP address as long as the any server returns the attribute. The **Framed-IP-Address** value always has a higher priority than the local address pool.	enabled	enabled	enabled	enabled	enabled

Parameter	Description	default	*rap	*cap	*hp-switch	*iap
User idle timeout	The user idle timeout value for this profile. Specify the idle timeout value for the client in seconds. Valid range is 0-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.	disabled	N/A	N/A	disabled	disabled
PAN firewalls Integration	Requires IP mapping at Palo Alto Networks firewalls.	disabled	disabled	disabled	disabled	disabled

To modify the default VPN authentication profile via the WebUI:

1. In the **Mobility Conductor** node hierarchy, navigate to the **Configuration > System > Profiles** page.
2. In the **All Profiles** list, expand **Wireless LAN > VPN Authentication** and select the **default** VPN authentication profile.
3. From the **Default Role** drop-down list, select the default user role for authenticated VPN users.
4. (Optional) Set **Max Authentication failures** to an integer value. The default value is 0, which disables this feature.
5. (Optional) If you use client certificates for user authentication, select the **Check certificate common name against AAA server** check box to verify that the certificate's common name exists in the server. This parameter is enabled by default in the **default-cap** and **default-rap** VPN profiles, and is disabled by default on all other VPN profiles.
6. (Optional) Enabling **PAN Firewall Integration** requires IP mapping at Palo Alto Networks firewalls.
7. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.
10. In the **All Profiles** list, select the **Server Group** entry below the **Wireless LAN > VPN Authentication > Default** profile.
11. From the **Server Group** drop-down list, select the server group to be used for VPN authentication.
12. Click **Submit**.
13. Click **Pending Changes**.
14. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Applying Policies to Gateway Interfaces

After configuring the firewall policies, ACLs, and AAA profiles, you need to apply the appropriate policies on the WAN and LAN interfaces of the Aruba Gateways.

NOTE

For trusted (WAN) interfaces, apply the firewall policies directly. For untrusted (LAN) interfaces, assign AAA profiles (role assignment policies) to the VLANs.

This section includes the following topics that describe how to apply policies on appropriate ports and VLAN interfaces of the Aruba Gateways:

- Applying Policies for VLANs on Access Ports
- Applying Policies for VLANs on Trunk Ports
- Applying Route ACLs for VLAN Interfaces
- Assigning AAA profile to VLAN Interfaces for Role Assignment

Applying Policies for VLANs on Access Ports

Complete the following procedure to apply a firewall policy for a trusted VLAN on access port:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Apply Policies**.
3. To apply a firewall policy, select an access port from **Interface table**.
4. Under the **POLICY** column, select the policy to be applied from the drop-down list.

NOTE

You can apply firewall policies only for trusted VLAN interfaces.

5. Save the changes.

Applying Policies for VLANs on Trunk Ports

Complete the following procedure to apply firewall policies for trusted VLANs on trunk port:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security** > **Apply Policies**.
3. Click **Edit Policies** from the **POLICY** column of **Interface table** for the trunk port on which you want to apply a firewall policy. The **Interface > <port-number>** table appears which lists all the VLANs configured for the selected trunk port.
4. Select any trusted VLAN from the **Interface <port-number>** table for which you want to apply a firewall policy.

You can apply firewall policies only for trusted VLAN interfaces.

5. Under the **POLICY** column, select the policy to be applied from the drop-down list.
6. Save the changes.
7. Repeat *step 6* to *step 8* to apply policies for multiple VLANs.

Applying Route ACLs for VLAN Interfaces

Complete the following procedure to apply Route ACLs for the configured VLAN interfaces:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
    a. Set the filter to **Global** or a group containing at least one Branch Gateway.
    b. Under **Manage**, click **Devices** > **Gateways**.
       A list of gateways is displayed in the List view.
    c. Click a gateway under **Device Name**.
       The dashboard context for the gateway is displayed.
    d. Under **Manage**, click **Device**.
       The gateway device configuration page is displayed.

2. Click **Security** > **Apply Policies**.
3. From the **VLANs** table, select the VLAN for which you want to apply a route ACL.
4. Under the **ROUTE ACL** column, select the ACL to be applied from the drop-down list.
5. Save the changes.

Assigning AAA profile to VLAN Interfaces for Role Assignment

Complete the following procedure to apply a AAA profile on a VLAN interface for role assignment:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
    - To configure a Branch Gateway group or VPNC group, complete the following steps:
        a. Set the filter to a group containing at least one Branch Gateway.
           The dashboard context for a group is displayed.
        b. Under **Manage**, click **Devices** > **Gateways**.
           A list of gateways is displayed in the **List** view.
        c. Click **Config**.
           The configuration page is displayed for the selected group.
    - To configure a Branch Gateway or VPNC, complete the following steps:
        a. Set the filter to **Global** or a group containing at least one Branch Gateway.
        b. Under **Manage**, click **Devices** > **Gateways**.
           A list of gateways is displayed in the List view.
        c. Click a gateway under **Device Name**.
           The dashboard context for the gateway is displayed.
        d. Under **Manage**, click **Device**.
           The gateway device configuration page is displayed.
2. Click **Security** > **Apply Policies**.
3. From the **VLANs** table, select the VLAN for which you want to apply a AAA profile.
4. Under the **ROLE ASSIGNMENT** column, select the AAA profile to be applied to the VLAN interface from the drop-down list.
5. Save the changes.

SD-Branch Redundancy

Administrators can set up a redundancy scheme in SD-Branches and data centers to provide a highly available and an always-on network. The data center, VPNC, and Branch Gateway failover redundancy features allow network administrators to significantly reduce the downtime and client traffic disruptions.

Data Center Redundancy

The SD-WAN solution supports active-standby or active-active VPNC configuration at the data center. Any of the Aruba 7200 Series controllers can be configured to function as a VPNC at the data center or headquarters to aggregate data traffic from branches.

Administrators can configure primary and redundant VPNCs in active-active mode to allow some Branch Gateways to terminate on one VPNC and the remaining on the second VPNC.

For example, if you have data centers on the East and West Coasts, half of the branch sites could connect to the data center on the West Coast as primary and that on the East Coast as backup. The remaining sites could connect to the East Coast data center as primary and that on the West Coast as backup. This architecture reduces downtime during VPNC failures as only half of the sites need to switch to the backup VPNC.

VRRP Redundancy

The Virtual Router Redundancy Protocol (VRRP) is used to create various redundancy solutions, such as pairs of Aruba Gateways acting in active-backup mode or in primary-standby mode by using a virtual IP address. When the primary device becomes unavailable, a backup SD-WAN Gateway comes up as the primary device with the virtual IP address. All network elements (APs and other devices) are configured to access individual virtual IP addresses of respective VLANs, thereby providing a transparent redundant solution to your network.

VRRP eliminates a single point of failure by providing a mechanism to elect a VRRP conductor device. If VRRP preemption is disabled and all Aruba Gateways share the same priority, the first device that comes up is elected as the VRRP conductor. However, if VRRP preemption is enabled and all devices share the same priority, the device with the highest IP address becomes the VRRP conductor.

To avoid routing loops during overlay negotiation with the hubs, Branch Gateways automatically suppress route advertisements for subnets that do not have the VRRP state as Conductor.

To know how to configure redundant gateways for high availability, see Configuring Redundant Gateways for High Availability.

Configuring Redundant Gateways for High Availability

To configure a Gateway pair for high availability, complete the following steps:

- Configuring Peer Aruba Gateways and Transport VLAN for WAN Redundancy
- Configuring DHCP State Synchronization
- Configuring VRRP for LAN Redundancy

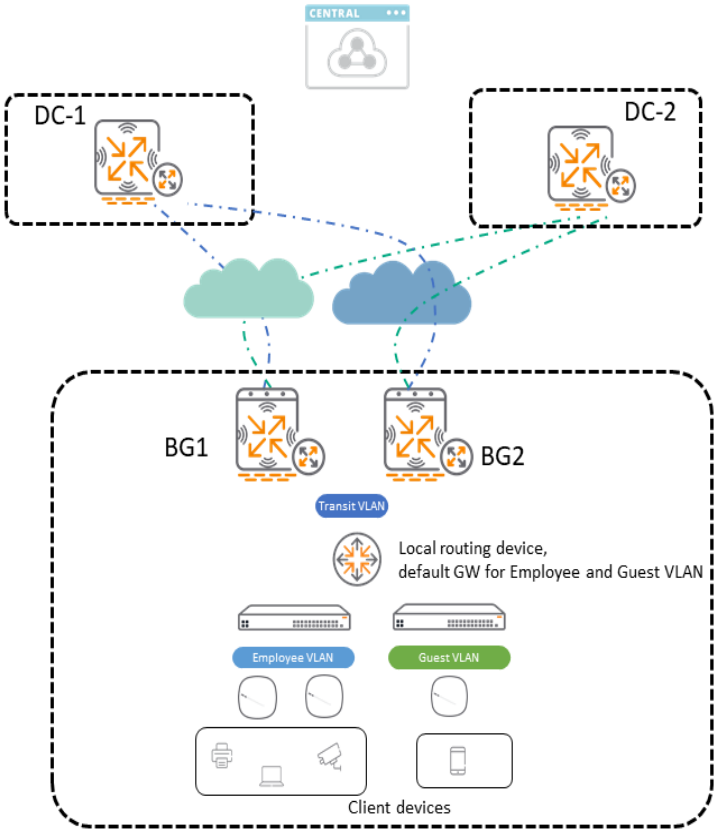
Configuring Peer Aruba Gateways and Transport VLAN for WAN Redundancy

Aruba SD-Branch solution allows to establish a virtual link between redundant Aruba Gateways to share the WAN interfaces. This virtual link is a GRE tunnel that is automatically established between Branch Gateways when peer Aruba Gateways and transport VLAN are configured.

Aruba provides Layer 3 redundancy between a peer Branch Gateway and a default Branch Gateway to which the clients in that site are connected. These two Branch Gateways have a dynamic or a static routing set up to get reachability information. Routing information is redistributed over the SD-WAN overlay to communicate to the VPNCs that these subnets are not directly attached. The **Site ID** determines that the Branch Gateways are installed at the same site. This allows path computation to take place, set the auto-cost and maintain the symmetry of traffic flows through the overlay. When redistributing routes on a VPNC

or Branch Gateway to upstream routing devices, path selection can be influenced by the options available through the respective protocol. For example, interface cost when using OSPF in the branch site. The following image illustrates this feature:

Figure 256 *Layer 3 Redundancy for high availability*



When the virtual link is established, Branch Gateways share uplink interfaces with their peers. Peer Aruba Gateways use uplink interfaces from the other Aruba Gateways only if WAN ports are configured with different uplink VLANs.

Note the following guidelines for configuring Peer Aruba Gateways and Transport VLAN for WAN Redundancy:

- It is recommended not to configure the same SD-WAN Gateway as the Conductor for some VLANs and as Backup for some other VLANs.
- Peer Aruba Gateways use uplink interfaces from the other Aruba Gateways only if WAN ports are configured with different uplink VLANs.

To set up the communication between the peer Aruba Gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the gateway device is displayed.

4. Under **Manage**, Click **Device**.

   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **High Availability**. The **Redundancy** configuration page is displayed.
7. In the **WAN Redundancy** section, enter the **Site ID** to which the gateways belong.
8. Enter the peer SD-WAN Gateway IP address in the **Peer gateway IP address** field to enable Branch Gateway redundancy with uplink sharing.
9. Select the VLAN ID from the **VLAN ID connecting to peer gateway** field to configure the transport VLAN for communication between the redundant Aruba Gateways.
10. Save the changes.
11. Repeat steps 1-6 on the configured peer SD-WAN Gateway to enable uplink load sharing.

Configuring DHCP State Synchronization

State synchronization is achieved through a combination of DHCP failover profile, pool scope, and NTP server. The pool scope under the DHCP database is similar for both peers. Users have no control over the failover profile and they are automatically added to the DHCP database when a virtual Branch Gateway link is successfully established between the Branch Gateway peers.

To configure DHCP state synchronization, configure a corporate NTP server at the group level. For more information, see Configuring System Information on Aruba Gateways.

Ensure that you create the same DHCP scope on both Aruba Gateways. Exclude VLAN interface IP addresses from the pool address range. To view the pool address range, execute the 'show ip dhcp database' command and ensure that the range is same across peers.
Normal functioning of a DHCP server is dependent on NTP clock synchronization and network (virtual link) connectivity between Branch Gateway peers in a high availability (HA) setup. Ensure that both the peers are connected and functioning.

The DHCP high availability and failover mechanism for two Branch Gateway peers work differently as explained in the following states:

- **Peer down state**—This state occurs during boot up where one peer comes up first and gets provisioned while the second peer takes time to come up. In this scenario, the first peer invokes peer down timer for 60 seconds and waits for the second peer to come up. If connectivity to second peer is not established in 60 seconds, then the first peer acts in standalone mode claiming the full DHCP lease range keeping a reduced lease time of five minutes. This approach avoids any boot time setbacks and limits IP address conflicts to five minutes when peers have connectivity issues with network or each other. Once the second peer is commissioned and connectivity to the first peer is established, the peers start operating in High Availability mode with configured lease times.
- **Connectivity down state**—This state occurs when two peers successfully establish a connection with each other and share a DHCP pool lease range but lose connectivity due to a hardware failure or network issues.

For example, consider a scenario where Peer A and Peer B successfully establish connection with each other and share a DHCP pool of 10 leases. Peer-A owns five leases and Peer B owns the remaining five. Peer-A hands out four leases to its clients and Peer-B hands out four leases to its clients. A hardware failure causes Peer B to go down and they lose connectivity with each other. As Peer A is aware of the total two free leases both of them owned before Peer B went down, Peer A renews the eight leases (four owned and leased by each peer) until it re-establishes connection with Peer B. Peer-A hands out the ninth lease (one free lease left that it owned at the time of connectivity loss) to its new client. During the time of their connectivity down

state, neither Peer A nor Peer B will hand out the 10th lease (one free lease left for Peer-B) . The DHCP high availability and failover mechanism takes extreme precautions to stop any silo operation, conflict, or duplicate IP address grant. Once the connectivity is restored, Peer B will be able to hand out the tenth lease to its client.

Configuring VRRP for LAN Redundancy

Before you begin configuring VRRP redundancy, obtain the following network information:

- VLAN ID for the two Aruba Gateways on the same layer 2 network.
- Virtual IP address to be used for the VRRP instance.

To configure VRRP redundancy, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **High Availability**. The **Redundancy** configuration page opens.
7. Click **+** to add a new virtual router in the **Virtual Router Table**. The **New Virtual Router** section is displayed.
8. Select the IP version from the **IP Version** drop-down list.
9. Select the VLAN on which you want to configure VRRP from the **VLAN** drop-down list.
10. Set **Admin State** to **UP**.
11. Specify the priority value in the **Priority** field. For a backup SD-WAN Gateway, use the default priority value of 100. For the primary SD-WAN Gateway, use a priority value higher than the default value, such as 110.
12. Configure the other VRRP parameters as described in Table 279.
13. Save the changes.
14. Repeat steps 1-10 to configure VRRP on the other device in the primary and backup redundant pair.

Ensure to reload the device whenever you modify the Conductor VRRP configuration under Conductor Redundancy to avoid any configuration errors.

Table 279: *VRRP Configuration Parameters*

Parameter	Description
ID	The ID uniquely identifies a VRRP instance. For ease of administration, specify VLAN ID as the ID.
Description	Description of the VRRP instance.
IP version	The IP version. Select IPv4.

Table 279: *VRRP Configuration Parameters*

Parameter	Description
Authentication Password	Password to authenticate VRRP peers in their advertisements.
Retype authentication password	Reconfirm the password, if configured.
IP address	This is the virtual IP address that is owned by the elected VRRP conductor. Ensure that the same IP address and VRRP ID is configured on each member of the redundant pair.
Priority	Priority level of the VRRP instance for the device. This value is used in the election mechanism for the conductor. When configuring VRRP on a standby device, use the default priority value of 100. For a conductor device, use a higher priority value such as 110.
Advertisement interval (secs)	This is the interval, in seconds, between successive VRRP advertisements sent by the current conductor. The default interval time is recommended. Default: 1 second
Hold time (secs)	This is the hold time, in seconds. The default interval time is recommended. Default: 45 seconds
Enable router Pre-emption	Enables a device to take over the role of conductor if it detects a lower priority device that is currently acting as conductor.
Pre-emption delay (secs)	Specifying a value enables the delay timer. The timer is triggered when the VRRP state moves out of backup or init state to become a conductor. This is applicable only if you enable router pre-emption. When the timer is triggered, it forces VRRP to wait for a specified period of time, so that all the applications are ready before coming up. This prevents the APs from connecting to the SD-WAN Gateway before the SD-WAN Gateway can accept the connection. In the meantime, if there is an advertisement from another VRRP, the VRRP stops the timer and does not transition to conductor.
Admin state	Administrative state of the VRRP instance. To start the VRRP instance, change the admin state to **UP**.
VLAN	VLAN on which the VRRP protocol runs.
Tracking conductor up-time	Perform VRRP priority tracking based on how long the device has been the conductor. This feature is designed to ensure that a conductor is allowed to take and maintain control of the VRRP if it has been up for a certain amount of time in minutes (0-1440). This prevents a common issue where a device that is periodically going up and down assumes the role of primary conductor. Configuring this parameter is optional.
Tracking conductor up-time priority	The additional priority given to the conductor after it has been up for the time interval defined by the **Tracking Conductor Up-time** parameter. Configuring this parameter is optional.
Tracking VRRP conductor state ID	Perform tracking based on the UP or DOWN state of another VRRP conductor by specifying the VRRP ID of the conductor to be tracked. Configuring this parameter is optional.

Table 279: *VRRP Configuration Parameters*

Parameter	Description
Tracking VRRP conductor state priority	The priority taken away from a VRRP conductor if it is in a DOWN state. The priority levels are returned to their previous state when the VRRP conductor comes back up. Configuring this parameter is optional.
Tracking VLAN	Perform VRRP priority tracking based on the UP or DOWN state of a VLAN. Click **+** below the **Tracking VLAN** table and specify the following values: VLAN Id: ID of the VLAN to be tracked. Subtract: Priority level to be subtracted from the device's VRRP priority if the tracked VLAN goes down. Configuring this parameter is optional.
Tracking interface	(Optional) Perform VRRP priority tracking based on the UP or DOWN state of a specific interface. Click **+** below the **Tracking Interface** table and specify the following values: Interface: Interface Port to be tracked. Subtract: Priority level to be subtracted from the device's VRRP priority if the tracked interface goes down. Configuring this parameter is optional.

Configuring Aruba Gateways for Certificate-Based Authentication

Certificates provide a secure way of authenticating devices and eliminate the need for less secure password-based authentication. In certificate-based authentication, digital certificates are used to identify a user or device before granting access to a network or application.

Digital certificates use PKI that requires a private-public key pair. A digital certificate is associated with a private key, known only to the certificate owner, and a public key. A certificate encrypted with a private key is decrypted with its public key. For example, party A encrypts its certificate with its private key and sends it to party B. Party B decrypts the certificate with the public key of party A.

Server certificates and the digital certificates issued by a CA validate the identities of servers and clients. For example, when a client connects to a server for the first time, or the first time since its previous certificate has expired or been revoked, the server requests that the client transmit its authentication certificate and verifies it. Clients can also request and verify the authentication certificate of the server.

Branch devices use digital certificates for authenticating a client's access to user-centric network services such as VPN, the device UI or CLI. Branch Gateways include a server certificate by default for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Adding Certificates to Certificate Store in Aruba Central

The **Global Settings > Certificates** page in the Aruba Central UI allows you to add certificates to the Central's certificate store. If the certificates are added in the Aruba Central's certificate store, you can import or map the certificates required for SD-WAN configuration.

For more information on adding certificates to Aruba Central, see Certificates.

Installing Certificates

To enable branch devices to use certificate-based authentication, you must install the certificates loaded in the Aruba Central's certificate store on branch devices.

Installing Certificates for Server Authentication

To install certificates for web server, captive portal, or VIA server authentication, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **System** > **Certificates**.
3. Click **Server Certificates**.
4. Under **Captive portal certificate**, select a certificate for captive portal server authentication.
5. Under **Configure SSL/TLS protocol**, select a security protocol. By default, all TLS protocols are selected.
6. Under **VIA server certificate**, select a certificate for VIA server authentication.
7. Click **System** > **Admin**.
8. Click **Admin Authentication Options**.
9. Under **WebUI Authentication** > **Server certificate**, select a certificate for server authentication.
10. Click **Save Settings**.

Installing Certificates for VPN Clients

To install a certificate for VPN client authentication, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.

b. Under **Manage**, click **Devices** > **Gateways**.

A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. Click **System** > **Certificates** > **Certificates for VPN Clients**.
   - To add a CA certificate, click **+** in the **CA Certificate Assigned for VPN Clients** table.
   - To add certificate group, click **+** in the **Certificate Groups for VPN Clients** table.

   The **Add New Certificate** table is displayed at the bottom of the page.
3. Select the certificate to add from a list of certificates uploaded in the Aruba Central's certificate store.
4. Click **Save Settings**.

Configuring Revocation Checkpoint

The Certificate Revocation feature enables the Aruba Gateways to perform real-time certificate revocation checks using OCSP server, or traditional certificate validation using the CRL client.

OCSP (RFC 2560) is a standard protocol that consists of an OCSP client and an OCSP responder. This protocol determines revocation status of a given digital public-key certificate without downloading the entire CRL.

CRL is the traditional method of checking certificate validity. A CRL provides a list of certificate serial numbers that have been revoked or are no longer valid. CRLs let the verifier check the revocation status of the presented certificate while verifying it. CRLs are limited to 512 entries.

When configured as an OCSP responder, the Aruba Gateways provide revocation status information to applications that use CRLs.

Ensure that the required OCSP signer and responder certificates are available in the Aruba Central certificate store.

Configuring Revocation Checkpoint Using OCSP

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

     The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the **List** view.

c. Click **Config**.

The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.

  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.

  The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

  The gateway device configuration page is displayed.

2. Click **System** > **Certificates** > **Revocation Checkpoint**.
3. In the **Revocation Checkpoint** table, click **+** to add the record for which you want to configure the revocation checkpoint. The **Add Revocation Checkpoint** section is displayed.
4. From the **Name** drop-down list, select the CA cert for which you want to configure the revocation check point.
5. Select **ocsp** from the **Revocation method 1** drop-down list as the primary check method.
6. Specify the OCSP server URL in the **OCSP URL** field.
7. Optionally, select a backup check method (**crl**) from the **Revocation method 2** drop-down list.
   a. Select the **Enable OCSP responder** check box to configure the SD-WAN Gateway as an OCSP responder for the selected CA certificate.
   b. Select the required OCSP signer certificate from the **OCSP signer cert** drop-down list.
   c. Select the required OCSP responder certificate from the **OCSP responder cert** drop-down list.
8. Optionally, you can configure one of the following actions to be taken when the configured server is unreachable:
   - **Fail-Over**—Fails over to the revocation method 2, if configured.
   - **Allow Cert**—Allows the certificate.
   - **Revoke Cert**—Revokes the certificate.
9. Save the changes.

Configuring Revocation Checkpoint Using CRL

To configure the SD-WAN Gateway as an OCSP responder for providing revocation status information using CRL, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.

     The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.

     A list of gateways is displayed in the **List** view.
     c. Click **Config**.

     The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
    a. Set the filter to **Global** or a group containing at least one Branch Gateway.
    b. Under **Manage**, click **Devices** > **Gateways**.
       A list of gateways is displayed in the List view.
    c. Click a gateway under **Device Name**.
       The dashboard context for the gateway is displayed.
    d. Under **Manage**, click **Device**.
       The gateway device configuration page is displayed.

2. Click **System** > **Certificates** > **Revocation Checkpoint**.
3. Optionally, if you want to globally enable the OCSP responder service on the SD-WAN Gateway, complete the following steps:
    a. Click the **Enable OCSP responder** option to enable the OCSP responder service on the Aruba Gateways.
       Enable OCSP responder is a global option that enables or disables the OCSP responder service on the Aruba Gateways. By default, it is disabled.
    b. Select the OCSP signer certificate to be used to sign OCSP responses for this revocation checkpoint from the **OCSP certificates** drop-down list.
4. In the **Revocation Checkpoint** table, click **+** to add the record for which you want to configure the revocation checkpoint. The **Add Revocation Checkpoint** section is displayed.
5. From the **Name** drop-down list, select the CA certificate for which you want to configure the revocation check point.
6. Select **crl** from the **Revocation method 1** drop-down list as the primary check method.
7. Select the CRL that you want to use for this revocation checkpoint from the **CRL location** drop-down list. The CRLs listed are files that have already been imported onto the Aruba Gateways.
8. Optionally, select a backup check method as follows:
    a. Select **ocsp** from the **Revocation method 2** drop-down list.
    b. Specify the OCSP server URL in the **OCSP URL** field.
9. If you want to override the global OSCP responder settings and configure specific settings for the selected CA certificate, complete the following tasks:
    a. Select the **Enable OCSP responder** check box to configure the SD-WAN Gateway as an OCSP responder for the selected CA certificate.
    b. Select the required OCSP signer certificate from the **OCSP signer cert** drop-down list.
    c. Select the required OCSP responder certificate from the **OCSP responder cert** drop-down list.
10. Optionally, you can configure one of the following actions to be taken when the configured server is unreachable:
    - **Fail-Over**—Fails over to the revocation method 2, if configured.
    - **Allow Cert**—Allows the certificate.
    - **Revoke Cert**—Revokes the certificate.
11. Save the changes.

Configuring Aruba Gateways for SNMP-Based Reporting

The Aruba Gateways support versions 1, 2c, and 3 of SNMP for reporting purposes. For SNMP-based data collection and management, configure the following SNMP parameters:

Table 280: *SNMP Parameters*

Field	Description
Host Name	Host name of the Gateway.
System Contact	Name of the person who acts as the System Contact or administrator for the Gateway.
System Location	String to describe the location of the Gateway.
If you are using SNMPv3 to obtain values from the Gateway, you can configure the following parameters:	
User name	A string representing the name of the user.
Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: ■ MD5: HMAC-MD5-96 Digest Authentication Protocol ■ SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used.
Privacy protocol password	If messages sent on behalf of this user can be encrypted or decrypted with DES, the (private) privacy key for use with the privacy protocol.
Enable Trap Generation	Enables generation of SNMP traps to configured SNMP trap receivers. Refer to the list of traps in the "SNMP traps" section below for a list of traps that are generated by the Branch Gateway.

Community String for SNMPv1 and SNMPv2

Community strings are used to authenticate requests for SNMP versions before version 3. This is needed only when using SNMP v2c and is not needed if using version 3.

SNMP Trap Receivers

This table contains information on a trap receiver. This host needs to be running a trap receiver to receive and interpret the traps sent by the Branch Gateway. Configure the following for each host or trap receiver:

- **IP address**: This is the IP address of the new trap receiver.
- **SNMP version**: The SNMP version can be 1, 2c, or 3.
- **Security string**: Choose from the community strings that was created for SNMPv1 and SNMPv2.
- **Type**: Trap or Inform (SNMPv2c or SNMPv3 only)
- **Engine ID**: (SNMPv3 only)
- **UDP port**: This is the port on which the trap receiver is listening for traps. The default is the UDP port number 162. This is optional, and will use the default port number if not modified by the user.

Configuring Captive Portal IP Redirect Address

You can now configure a redirect IP address to redirect Gateway clients on the Captive Portal VLAN.

To configure captive portal redirect address, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Security** > **Advanced**.
4. Click **Captive Portal**.
5. Select the **Captive portal redirect IP** check box.
6. Enter an IP address to redirect captive portal clients.
7. Click **Save Settings**.

Viewing Gateway Configuration Status

Aruba Central provides an audit dashboard to review configuration changes for the devices provisioned in UI and template groups. The **Configuration Audit** menu option is available for all types of devices provisioned in Aruba Central.

To access the Gateway **Config Audit** page:

1. In the **Network Operations** app, use the filter to select a gateway.
   Summary of the selected gateway is displayed.
2. Under **Manage**, click **Device**.
   The selected gateway's configuration page is displayed.
3. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
4. Click **Config Audit** tab.

Managing Configuration Overrides

Aruba Central supports two levels of configuration hierarchy:

- Group level—When you configure a set of parameters at the group level, all other gateways provisioned in that group inherit the configuration updates.
- Device level—In certain cases, your deployment topology may require you to modify the system configuration of a specific device provisioned in a group. In such cases, you can modify the parameters at the device level. The final configuration for such devices will include the configuration applied at the group level and the overrides applied at the device level.

  If a configuration parameter is modified both at the group and device levels, the configuration applied at the device level takes precedence.

  Aruba recommends that you configure most of the provisioning parameters at the group-level unless a device-specific override is required. For SD-Branch deployments, Aruba recommends that you configure the following features and parameters at the device-level:
  - Gateway hostname
  - Loopback Interface addresses
  - OSPF and BGP router IDs
  - Local DHCP pools
  - Gateway peer configuration
  - Manual override of firewall aliases
  - Uplink configuration inherited from Zero Touch Provisioning
  - Bulk configuration imported from a CSV file

Configuration Overrides

When a configuration parameter is modified both at the group and device levels, Aruba Central marks this configuration difference as an override. For such parameters, Aruba Central displays a green bullet icon. On clicking this icon, you can view the details of the override and also remove the override if required.

Important Points to Note

Note the following points:

- Configuration overrides are applicable to only those parameters which can be modified at both group and device levels.
- Aruba Central does not display the configuration override indicator (green bullet icon) for the following UI fields:
  - All password fields in the UI—For example, SNMPv3 user credentials (**System** > **SNMP**).
  - Configuration parameters that are already configured at the group level, but are not available for device-level edits—For example, the **IP address** UI field in the **System** > **Logging** > **Syslog Servers** > **Add New Syslog Server** page.
  - Configuration parameters that must be applied only at device-level— For example, hostname (**System** > **General** > **Basic Info**), SNMP hostname (**System** > **SNMP** > **Hostname)**, System contact and System location (**System** > **SNMP**), and other such configuration parameters. The device-specific parameters are configured only at the device level. Hence, the override option is not applicable to these fields.

Limitations

Due to feature limitations in this release, Aruba Central does not display the configuration override bullet icon for the following UI elements:

- Parameters with multiple UI elements in a row. For example, the **Auth Protocols** field in the **VPN** > **IKEV1** page.
- Cascading UI elements that are displayed after selecting another UI element, such as a toggle switch or check box.

  For example:
  - The **Advertise VLANs to all hubs** toggle switch that appears when **Overlay mode** is **Manual** in the **VPN** > **SD-WAN Overlay** page.
  - The **DPD** toggle switch and its associated parameters on the **VPN** > **DPD** page.
- Some drop-down lists with options for selecting an IP address or VLAN interface; For example, the **IPv4 Address** drop-down under **System IP Address** in the **System** > **General** page.
- Parameters in the tables displayed on the **Security** > **Auth Servers** and **System** > **Admin** > **Admin Authentication Servers** pages.

Configuring Aruba Gateways for Syslog Message Collection

This section outlines the steps required to configure logging on an SD-WAN Gateway.

For each category or subcategory of message, you can set the logging level or severity level of the messages to be logged.

The following table summarizes these categories:

Table 281: *Software Modules*

Code	Description
network	Network messages
all	All network messages
packet-dump	Protocol packet dump messages
mobility	Mobility messages
dhcp	DHCP messages
system	System messages
all	All system messages
configuration	Configuration messages
messages	Messages
snmp	SNMP messages
webserver	web server messages
security	security messages

Code	Description
all	all security messages
aaa	AAA messages
firewall	firewall messages
packet-trace	packet trace messages
mobility	mobility messages
vpn	VPN messages
dot1x	802.1X messages
ike	IKE messages
webserver	web server messages
wireless	wireless messages
all	all wireless messages
captive-portal	captive portal user messages
vpn	VPN messages
dot1x	802.1x messages
radius	RADIUS user messages

For each category or subcategory, you can configure a logging level. The following table describes the logging levels in the order of its severity, that is, from most severe to least severe.

Table 282: *Logging Levels*

Code	Description
emergency	captive portal user messages
alert	VPN messages
critical	802.1x messages
errors	RADIUS user messages
warning	warning messages
notice	Significant events of a non-critical and normal nature.
informational	Messages of general interest to system users.
debug	Messages containing information useful for debugging.

The default logging level for all categories is Warning. You can also configure IP address of a syslog server to which the Branch Gateway can direct these logs.

Configuring Logging Levels

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. Click **System** > **Logging**.
6. Click **+** in the **Syslog Servers** section to add a logging server.
7. Add the logging server to the list of logging servers. Update the followings fields:
   - **IP address**
   - **Category**
   - **Logging facility**
   - **Logging level**
   - **Format**: Select the logging format from the **Format** drop-down list. The ArcSight CEF is a log management standard that uses a standardized logging format so that data can easily be collected and aggregated for analysis by an enterprise management system.

Ensure that the syslog server is enabled and configured on this host.

8. Click **Save Settings**.

To select the types of messages you want to log, select **Logging Levels.**

1. Select the category or subcategory to be logged.
2. To select the severity level for the category or subcategory, select the level from the **Logging Level** drop-down list.
3. Click **Save Settings**.

Chapter 16
Configuring an SD-Branch Network Using the Basic Setup

This section guides you through the steps required to set up your SD-WAN network using the Basic setup.

Before you proceed with the configuration tasks, browse through the recommendations and best practices described in the Aruba SD-Branch Fundamentals Guide and Aruba SD-Branch Security Hardening Guide.

Configuration Checklist

Following is the configuration workflow for the SD-Branch devices in Basic mode:

VPNCs

Following is the basic mode configuration workflow for VPNCs.

- Configuring System IP Address—The system IP configuration is required on each gateway provisioned in Aruba Central.
- Configuring or Renaming Gateway Hostname—Configure or edit a gateway hostname. For offline gateways, the change is reflected in Aruba Central after the gateway goes online.
- Configuring Management User Accounts—Configure a management user with credentials to log in to the local management interface of the device.
- Configuring VLANs for LAN Interfaces—Configure VLAN interfaces for LANs. For the SD-WAN deployment, each Branch Gateway requires VLAN interfaces for LAN. Each VLAN must have a unique VLAN ID assigned to it.
- Configuring Ports for LAN Interfaces—Configure one or more physical ports on the Branch Gateway to be a member of a VLAN.
- Configuring WAN Uplinks and Ports—Configure uplink interfaces by creating WAN-facing VLANs, labeling them as uplink interfaces, and assigning them to the desired uplink ports.
- Configuring Routing Profiles—Configure IPv4 routes to determine how each device must reach Aruba Central and its VPN peers over an intermediate public or private IPv4 network.
- Configuring Overlay Routing Profiles—Configure Overlay Routing for VPNC. VPNCs use the Overlay Agent Protocol (OAP) to automatically build the SD-WAN overlay topology.
- Configuring Route Maps—Configure Routes Maps for VPNC. Route maps allow you to configure a filtering criteria by defining a set of rules or match statements with a permit or deny condition.
- Configuring OSPF—Configure OSPF for VPNC. The OSPF configuration allows advertising branch networks into an OSPF area and enables VPNCs to learn corporate routes.
- Configuring BGP—Configure BGP for VPNC. BGP is a dynamic routing protocol that enables VPNCs to redistribute overlay routes learned from Branch Gateways into BGP and advertise those routes in the data center network.
- Configuring VPN Pools—Configure VPN Pools for a VPNC group. A VPN pool is a pool of IP addresses configured for a device group.

Branch Gateways

Following is the basic mode configuration workflow for Branch Gateways.

- Configuring System IP Address—The system IP configuration is required on each gateway provisioned in Aruba Central.
- Configuring or Renaming Gateway Hostname—Configure or edit a gateway hostname. For offline gateways, the change is reflected in Aruba Central after the gateway goes online.
- Configuring Management User Accounts—Configure a management user with credentials to log in to the local management interface of the device.
- Configuring VLANs for LAN Interfaces—Configure VLAN interfaces for LANs. For the SD-WAN deployment, each Branch Gateway requires VLAN interfaces for LAN. Each VLAN must have a unique VLAN ID assigned to it.
- Specifying the Device Model—Specify a device model for the Branch Gateway group.
- Setting System Clock and Time Zone—Configure the system clock and time zone manually. The system automatically updates the time zone including the relevant Daylight Savings Time (DST) across time zones. You can optionally specify a time zone that is applied to all the gateways in the group. The default time zone is set to GMT.
- Configuring Domain Name System—Configure Domain Name System (DNS) for Branch Gateways. The DNS manages a database that maps domain names to IP addresses and routes your query to the next appropriate server.
- Configuring Management User Accounts—Configure a management user with credentials to log in to the local management interface of the device.
- Configuring VLANs for LAN Interfaces—Configure VLAN interfaces for LANs. For the SD-WAN deployment, each Branch Gateway requires VLAN interfaces for LAN. Each VLAN must have a unique VLAN ID assigned to it.
- Configuring Ports for LAN Interfaces—Configure one or more physical ports on the Branch Gateway to be a member of a VLAN.
- Configuring DHCP for LAN Interfaces—Configure DHCP for LAN interface for a Branch Gateway. A DHCP pool is a set of IP addresses that can be assigned with the client devices associated with the Branch Gateway of a specific branch.
- Configuring WAN Health Check—Configure WAN Health Check for a Branch Gateway. Health check monitoring is critical for forwarding the Internet traffic, ensure that the health check feature is enabled on all Branch Gateway groups.
- Configuring WAN Load Balancing—Configure Load Balancing for a Branch Gateway. The uplink load balancing feature supports both active and standby uplinks, for example, traffic can be load balanced across two wired uplinks, while the backup cellular uplink remains idle and is used when a wired link fails.
- Configuring WAN Uplinks and Ports—Configure uplink interfaces by creating WAN-facing VLANs, labeling them as uplink interfaces, and assigning them to the desired uplink ports.
- Configuring Routing Profiles—Configure IPv4 routes to determine how each device must reach Aruba Central and its VPN peers over an intermediate public or private IPv4 network.
- Configuring VPN Hubs and Routing Profiles—Configure VPN Hubs and Routing Profiles for a Branch Gateway Group.
- Configuring Overlay Routing Profiles—Configure Overlay Routing for VPNC. VPNCs use the Overlay Agent Protocol (OAP) to automatically build the SD-WAN overlay topology.
- Configuring LAN Redundancy for High Availability—Configure LAN Redundancy for Branch Gateway. Before configuring, ensure that you have enabled High Availability on the WAN page and configured peer gateway for redundancy.

- Configuring Policies—Configure the following policies for a Branch Gateway group.
  - Role assignment policy—Policy to determine client access, based on the user roles assigned to a client.
  - Application usage policy—Policy for deep packet inspection of application usage by clients.
  - Traffic steering policy—Policy for dynamically steering client traffic to the best performing uplink.
  - Quality of Service (QoS) policy—Policy for prioritizing critical traffic, prevent excess bandwidth usage, and manage network bottlenecks to prevent packet drops.
  - Security policy—Firewall policy to filter website content.

Configuring System Information on Aruba Gateways

This section describes the procedures for configuring system parameters for Aruba Gateways. Click on the links listed below for more information:

- Configuring or Renaming Gateway Hostname
- Configuring or Renaming Gateway Hostname
- Configuring a Model
- Setting System Clock and Time Zone
- Configuring Domain Name System
- Configuring Management User Accounts

Configuring System IP Address

The system IP configuration should be maintained on each gateway provisioned in Aruba Central. Each Gateway uses one VLAN interface as its system IP address for communicating with network services such as RADIUS, Syslog, TACACS+, and SNMP.

If the system IP address is not assigned to gateways, Aruba Central does not push configuration to gateways, which may lead to configuration discrepancies.
A system reboot is required when you change the system IP address of a gateway.

You can assign a system IP address to gateways using the Basic mode. The **System IP Address** can be configured at the device level for both Branch Gateway and VPNC. At the group level, the configuration can be done for the Branch Gateway group.

Configuring a System IP Address for a Branch Gateway or VPNC

To configure a System IP Address for a device, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
4. Under **Manage**, click **Device**.
   The device configuration page is displayed.
5. Ensure that you are in the **Basic Mode**.

6. Click **System** > **System IP**.
   - Enter the system IP in the textbox.
   - If a system IP address is already set, it is displayed in the **VLAN interface** drop-down list. Select the IP address from the **VLAN interface** drop-down list.
7. Click **Save Settings**.

Configuring a System IP Address for a Branch Gateway Group

To configure a System IP Address for a group, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the group contains at least one Branch Gateway.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **System** > **System IP**.
   - **Define system IP address pool**—Select this option to define an IP address pool for the gateways in the group. You can configure an IP address range by providing the start and end IP addresses. Aruba Central automatically allocates an IP address to each gateway and assigns it to VLAN 4087, which is the system IP address of the device.
   - **Specify static IP addresses later**—Select this option to configure the system IP address at the device level.
6. Click **Save Settings**.

Configuring or Renaming Gateway Hostname

In Basic mode, the hostname can be configured at the device level for both Branch Gateway and VPNC.

To configure a gateway hostname, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.

   The dashboard context for the device is displayed.
4. Under **Manage**, click **Device**.

   The device configuration page is displayed.
5. Ensure that you are in the **Basic Mode**.
6. Click **System** > **Hostname**.
7. Enter a hostname.

If a gateway hostname already exists, you can modify the string. For offline gateways, the change is reflected in Aruba Central after the gateway comes online.

8. Click **Save Settings**.

Specifying the Device Model

In **Basic** mode, you can specify the model at the group level only for Branch Gateway.

To configure the device model, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the group contains at least one Branch Gateway.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **System** > **Model**.

   Select a model from the drop-down list.
6. Click **Save Settings**.

Setting System Clock and Time Zone

In Basic mode, you can set the clock on a Branch Gateway group or VPNC group manually. Alternatively, you can also configure the Aruba Gateways to use an NTP server to synchronize its system clock with a central time source. The system automatically updates the time zone including the relevant Daylight Savings Time (DST) across time zones. This is done to automatically keep the time up-to-date and precise with DST adjustments.

In Basic mode, the timezone can be configured at the group level for Branch Gateways only.

Configuring NTP Server

To configure timezone, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the group contains at least one Branch Gateway.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **System** > **Time**.
6. Click the **+** icon in the **Public NTP Servers** and enter the IPv4 address or the FQDN of the public NTP provider to add the NTP servers to the Branch Gateways in this group.
7. Select the **Burst Mode** check box, if required. It is disabled by default.
   - The **Burst Mode** is a configurable option and not the default behavior for the Branch Gateway, as this option is recommended by some public NTP servers. If an NTP server is unresponsive, the

Burst Mode continues to send frequent queries until the server responds and time synchronization starts.

8. Choose the **timezone** from the drop-down list. The Primary time zones followed by other time zones are listed.
9. Click **Save Settings**.

Configuring Domain Name System

Network devices on the Internet use an IP address to route your request to the site you are trying to reach. Once you connect through a DNS server, it manages a database that maps domain names to IP addresses and routes your query to the next appropriate server.

In Basic mode, the DNS can be configured at the group level for Branch Gateways and VPNCs.

To configure DNS, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the group contains at least one Branch Gateway or VPNC.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **System** > **DNS**.
6. Select one of the following options to configure a DNS server:
   - **Specify DNS servers**—Select this option to configure a DNS server and define the following parameters:
     - Enter a **Domain name**.
     - Click the + icon to add a **Public DNS Server**. You can select one or more DNS service providers from the list or you can select **User Defined** for **Provider** and specify the IPv4 addresses of two or more public DNS name servers.
     - Enter the **IPv4 address** if you have selected **User Defined** for the provider. If you have selected the DNS service providers from the list, the IP address is auto-populated.
     - The **Uplink VLAN** drop-down becomes active when you select **User Defined** for the provider. You can select the VLAN ID from the **Uplink VLAN** drop-down list.
   - **Learn DNS configuration from ISP**—Select this option if you want the gateway to learn the DNS server dynamically from the ISP.

The DNS servers configured here are the ones that the gateway uses to resolve addresses. It must be reachable through the underlay as the device needs it to communicate with the SD-WAN Orchestrator.

7. Click **Save Settings**.

Configuring Management User Accounts for Aruba Gateways

A management user refers to the admin user with credentials to log in to the local management interface of the device.

In **Basic** mode, the user account management can be configured at the group level only for Branch Gateway and VPNC.

To configure the user account management, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the group contains at least one Branch Gateway or VPNC.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **System** > **Management User**.
6. Click the + icon in the **Local Management Users** table.

   The **Add Management User** pop-up is displayed.
7. Enter the user name and password that you want to configure.
8. Select a user role from the **Role** drop-down list. The following options are available:
   - **Super user role**—Administrator user role.
   - **Guest provisioning role**—Administrator role for provisioning guest users.
   - **Read only**—Read-only user role.
9. Click **Save**.
10. To authenticate an admin user using AAA policy, turn on the **AAA authentication** toggle switch.
11. Click the + icon in the **AAA Servers** table to create a AAA server for authenticating device management user.

    The **Add AAA Server** pop-up is displayed.
12. Configure the following parameters:
    - **Name**—Name of the authentication server.
    - **Server IP**—IP address of the authentication server.
    - **AAA authentication**—Enables centralized management user authentication using **RADIUS** or **TACACS** servers. For each AAA server, you must specify the IPv4 address or FQDN of the servers along with the protocol and shared secret.
    - **Key**—Shared key for authenticating a device administrator.
    - **Retype key**—Enter the key again to confirm.
13. Click **Save**.
14. Review the summary page and click **Save Settings**.

Configuring a LAN Interface

As a layer 2 switch, the Branch Gateway requires an external router to route traffic between VLANs. The Branch Gateway can also operate as a layer 3 switch that can route traffic between VLANs.

You can configure one or more physical ports on the Branch Gateway to be a member of a VLAN. Additionally, each wireless client association constitutes a connection to a virtual port on the Branch Gateway, with membership in a specified VLAN. You can place all authenticated wireless users into a single VLAN or different VLANs, depending on your network requirements. You can also configure an IP address and netmask for a VLAN. The IP address is *up* when at least one physical port in the VLAN is up. The VLAN IP

address can be used as a gateway by external devices; packets that are not destined for the Branch Gateway and directed to a VLAN IP address are forwarded according to the Branch Gateway's IP routing table.

For the SD-WAN deployment, each Branch Gateway requires VLAN interfaces for WAN uplinks and LANs. Each VLAN must have a unique VLAN ID assigned to it. By default, the Branch Gateways are pre-configured with the VLAN 4094.

See the following topics for instructions on configuring VLANs:

- Configuring VLANs for LAN Interfaces
- Configuring Ports for LAN Interfaces
- Configuring DHCP for LAN Interfaces
- Configuring WAN Health Check
- Configuring WAN Load Balancing
- Configuring WAN Uplinks and Ports

Configuring VLANs for LAN Interfaces

In Basic mode, the VLANs can be configured at the device or group level for both Branch Gateway and VPNC.

Configuring a LAN Interface for a Branch Gateway

To configure VLAN for LAN interfaces, complete the following steps:

From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, when configuring VLANs for a Branch Gateway, the **IPV4 Address** and **Netmask** fields are optional.

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
4. Under **Manage**, click **Device**.
   The device configuration page is displayed.
5. Ensure you are in the **Basic Mode**.
6. Click **LAN** > **VLANs**.
7. Select the **IP DHCP server** check box for the gateways to act as DHCP servers.
8. Click the **+** icon in the **VLANs** table to add a new VLAN.
9. Enter the **Name**—a unique VLAN name.
10. Enter the **VLAN ID**—a unique VLAN ID.
11. Enter **IPv4 Address**—a unique static IP address for each gateway in the group or a common address for all gateways in the group. This is an optional field.
12. Enter **Netmask**—the subnet mask of the IP address. This is an optional field.

Ensure that this VLAN is not routable, as it will overlap with the other gateways.

13. To configure branch gateways as DHCP server, turn on the **Act as DHCP server** toggle switch and configure the following parameters:
    - **Network**—The network IP address.
    - **Netmask**—The subnet mask of the network.
    - **Default router**—The IP address of the device used by clients if they want to communicate with devices outside of their subnet. Predominantly, this will be the Branch Gateway IP address for the particular VLAN, or the VRRP virtual IP, if configured.
    - **Reserve first**—The first IPv4 address for the CIDR range.
    - **Reserve last**—The last IPv4 address for the CIDR range.
    - **Domain name**—The DNS domain name assigned to branch devices.
    - **DNS server type**—Type of the DNS server. You can use either a public DNS server or add a DNS server by selecting the user-defined DNS option.
        - **DNS server IPv4 addresses**—If you use a **User Defined** DNS server, enter the IP addresses here. You can specify up to eight IP addresses separated by a comma.
        - **DNS Service Provider**—If you use a **Public DNS Service**, select the name of the **DNS service provider** from the list. For example, Google.
14. Turn on the **Enable DHCP relay** toggle switch to relay the incoming DHCP requests to an external DHCP server. Select this option when centralized DHCP servers are deployed to provide addressing to branch devices or if device profiling is performed by services such as Aruba ClearPass.
    a. Click the + icon in the **External DHCP server** table.
    b. Add the IPv4 addresses.
15. Click **Save**.

Configuring a LAN Interface for a Branch Gateway Group

To configure VLAN for LAN interfaces, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group. Ensure that the group contains at least one Branch Gateway.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **LAN** > **VLANs**.
6. Select the **IP DHCP server** check box for the gateways to act as DHCP servers.
7. Click the **+** icon in the **VLANs** table to add a new VLAN.
8. Enter the **Name**—a unique VLAN name.
9. Enter the **VLAN ID**—a unique VLAN ID.
10. Select one of the following **IP addressing mode** from the drop-down list:
    - **Static**—Select this option to use a static IP address. If you want to configure the LAN IP addresses at the device level, leave the IPv4 address and netmask fields empty. You can also set the same static IP/netmask for all the devices in the group.
        - **IPv4 Address**—Enter a unique static IP address for each gateway in the group or a common address for all gateways in the group.

- **Netmask**—Enter the subnet mask of the IP address.

Ensure that this VLAN is not routable, as it will overlap with the other gateways.

- **Dynamic DHCP Pool**—Select this option to assign an IP address from a dynamically carved DHCP pool. To configure an IP address range for dynamic assignment of DHCP IP addresses, configure the following parameters:
  - **DHCP pool start address**—The starting IP address in the DHCP pool that gateways allocate to branch devices.
  - **DHCP pool end address**—The last IP address in the DHCP pool that gateways allocate to branch devices.
  - **Hosts per branch**—The number of hosts per branch. This determines the subnet size that is allocated to each Branch Gateway in the group.
  - **Domain name**—The DNS domain name assigned to branch devices.
  - **DNS server type**—Type of the DNS server. You can use either a **Public DNS Service** or add a DNS server by selecting the **User Defined** DNS option.
    - **DNS server IPv4 addresses**—The IPv4 address of the DNS server. You can specify up to eight IP addresses separated by a comma.
  - **DNS Service Provider**—If you use a **Public DNS Service**, select the name of the DNS service provider from the list. For example, Google.
    To configure a Branch Gateways as DHCP server, turn on the **Act as DHCP server** toggle switch and configure the following parameters:
    - **Network**—The network IP address.
    - **Netmask**—The subnet mask of the network.
    - **Default router**—The IP address of the device used by clients if they want to communicate with devices outside of their subnet. Predominantly, this will be the Branch Gateway IP address for the particular VLAN, or the VRRP virtual IP, if configured.
    - **Reserve first**—The first IPv4 address for the CIDR range.
    - **Reserve last**—The last IPv4 address for the CIDR range.
    - **Domain name**—The DNS domain name assigned to branch devices.
- **DNS server type**—Type of the DNS server. You can use either a public DNS server or add a DNS server by selecting the user-defined DNS option.
- **DNS server IPv4 addresses**—If you use a **User Defined** DNS server, enter the IP addresses here. You can specify up to eight IP addresses separated by a comma.

11. Turn on the **Enable DHCP relay** toggle switch to relay the incoming DHCP requests to an external DHCP server. Select this option when centralized DHCP servers are deployed to provide addressing to branch devices or if device profiling is performed by services such as Aruba ClearPass.
    a. Click the **+** icon in the **External DHCP Server** table.
    b. Add the IPv4 addresses.
12. Click **Save Settings**.

Configuring a LAN Interface for a VPNC or VPNC Group

To configure VLAN for LAN interfaces, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one VPNC.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the VPNC group configuration dashboard.
   - To configure a VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one VPNC.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a VPNC under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **LAN** > **VLANs**.
4. Click + in the **VLANs** table to add a new VLAN.
5. Enter the **Name**—a unique VLAN name.
6. Enter the **VLAN ID**—a unique VLAN ID.
7. Enter **IPv4 Address**—a unique static IP address for each gateway in the group or a common address for all gateways in the group.
8. Enter **Netmask**—the subnet mask of the IP address.

Ensure that this VLAN is not routable, as it overlaps with the other gateways.

9. Click **Save**.

Configuring Ports for LAN Interfaces

In Basic mode, the ports for LAN interfaces can be configured at the device or group level for both Branch Gateway and VPNC.

To configure ports for LAN interfaces, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a Branch Gateway group or VPNC group complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway or VPNC.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the group configuration dashboard.
   - To configure a Branch Gateway or VPNC complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.

2. Ensure you are in the **Basic Mode**.
3. Click **LAN** > **LAN Ports**.
4. To add a LAN port, click the **+** icon in the **New LAN Port / Port Channel** table.
5. Enter a **Name** for the port.
6. Select a port channel or a port from the **Port** drop-down list.
   - If you have selected **Port Channel** for the LAN port, configure the following parameters:
     - **Port channel protocol**—Select a port channel protocol; for example, LACP (Link Aggregation Control Protocol). If you have selected LACP, select the LACP mode as active or passive from the **LACP mode** drop-down list.
     - **Port channel members**—Select the port channel members.
7. Select one of the following **VLAN modes**:
   - **Access**—Select this option to allow the LAN port to carry traffic only for the VLAN to which they are assigned. All transmitted and received traffic on the port is untagged.
   - **Trunk**— Select this option to allow the LAN port to carry traffic for multiple VLANs. If you select the **Trunk** mode, configure a list of allowed VLAN.
     - **Native VLAN**—The untagged VLAN ID for the port or port channel.
     - **Allowed VLAN**—The range of VLAN IDs assigned to the port or port channel including the Native VLAN.
8. Select an **Access VLAN** from the drop-down list.
9. Click **Save**.

Configuring DHCP for LAN Interfaces

In Basic mode, the DHCP can be configured at the device level for Branch Gateway only.

To configure DHCP for LAN interfaces, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one Branch Gateway.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the gateway is displayed.
4. Under **Manage**, click **Device**.

   The gateway device configuration page is displayed.
5. Ensure you are in the **Basic Mode**.
6. Click **LAN** > **DHCP**.
7. To add a DHCP, click + in the **IP Reservation** table.
8. Enter a **Client Name** for the DHCP.
9. Enter the **MAC Address**.
10. Enter the **IPv4 Address**.
11. Click **Save Settings**.

The client name is an identifier to facilitate network administration, it won't have any effect on the device's hostname.

To delete a client, select the client in the **IP reservation** table and click the delete icon.

Configuring WAN Health Checks

The WAN Health Check sends probes to measure WAN availability and latency on selected uplinks. Based on probe response, gateways continue to use the primary uplink or failover to a backup link.

As health check monitoring is critical for forwarding the Internet traffic, ensure that the health check feature is enabled on all Branch Gateway groups. When the health check feature is enabled, the probes are sent through the underlay at regular intervals to verify if the Internet is reachable over the uplink interfaces configured on Gateways. Based on the probe response, the uplink interface is marked as unavailable for the underlay traffic.

When the health check is enabled on a Branch Gateway, it sends five UDP or ICMP probes to a host every 10 seconds. The tunnel health is determined based on the probes received at the host:

1. If a probe is lost, then five probes are sent every two seconds to the host.
2. If a probe is lost in the first two seconds, then the aggressive mode is enabled by default, and 25 probes are sent every two seconds for the next 10 seconds.
3. If the probes do not reach the destination, then the tunnel is torn down hence achieving faster tunnel age-out with minimum packet loss.

When probes are not lost, the Branch Gateway goes back to sending five probes every 10 seconds per uplink.

In Basic mode, WAN health check can be configured at the device or group level for the Branch Gateway only.

Enabling WAN Health Check Probes

To enable WAN health check and configure probe settings, complete the following steps:

1. To configure the WAN health check for a Branch Gateway group or a Branch Gateway, complete either of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **WAN** > **Health Checks**.

4. Turn on the **Enable health checks** toggle to allow the gateway to send UDP or ICMP probes to a host and determine if the path is available to accommodate traffic.
5. Select the **Health check destination** and add the Remote host to which the Branch Gateways can send the health check probes. As part of the SD-WAN solution, Aruba Central provides a globally redundant path quality monitoring service for WAN health checks by default.
   - **User defined**—select this option to use a user defined host that is reachable through the WAN paths outside the VPN tunnel.
     - Enter the **Health check IP address**.
     - If a **User defined** health check destination is selected, provide the **Health check IP address** with the IPv4 address or FDQN of the user defined host.
   - **Aruba cloud**—select this option to use the responder (pqm.arubanetworks.com) provided by Aruba Central.
6. Select the **Health check probe mode**. This is the probe mode to use for connectivity checks. The following probe modes are available:
   - **Ping**—Sends ICMP probes to measure latency and packet loss.
   - **UDP**—Sends UDP Probes through UDP port 4500 to measure latency, packet loss, and jitter.
7. Click **Save Settings**.

Configuring WAN Load Balancing

In Basic mode, the load balancing can be configured at the device or group level for Branch Gateway only.

To enable load balancing mode, complete the following steps:

1. To configure load balancing for a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **WAN** > **Load Balancing**.
4. Select one of the following uplink Load balancing mode:

- **Round robin**—Select this option to sequentially distribute outgoing sessions between WAN links. It is the simplest algorithm to configure and implement but may result in uneven traffic distribution over time.
- **Session count**—Select this option to balance traffic among the uplinks based on the current number of active sessions managed by each link, so that the load for each active uplink stays within 5% of the other active uplinks. For example, if there are two active uplinks with the **Weight** parameter defined as 10 and 20, the active uplink with a weight of 20 will have more sessions assigned.
- **Uplink utilization**—Select this option to distribute traffic between active WAN uplinks based on the utilization % of each active WAN uplink. Uplink utilization considers the link speed to calculate the utilization and allows a maximum percentage of bandwidth threshold to be defined. When the bandwidth threshold exceeds the defined value, the WAN uplink will no longer be considered for session allocation. When you configure WAN ports, you must configure the WAN uplink speed appropriately.

5. Click **Save Settings**.

Configuring WAN Uplinks and Ports for WAN Interface

This section defines uplink interfaces by creating WAN-facing VLANs, labeling them as uplink interfaces, and assigning them to the desired uplink ports.

In Basic mode, the WAN uplinks and ports can be configured at the device level for VPNC at both the device and group level for Branch Gateways.

Configuring a WAN Interface for a Branch Gateway

To configure the WAN interface, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
4. Under **Manage**, click **Device**.
   The device configuration page is displayed.
5. Ensure you are in the **Basic Mode**.
6. Click **WAN** > **WAN Details**.
7. Turn on the **Enable High Availability deployment** toggle switch for LAN redundancy.
   - Select the **Peer gateway** from the list.
   - Enter the **Peer Hostname**.
   - Enter the **Site ID** to which the peer gateway belongs.
8. To add a WAN port, click the **+** icon in the **WAN Uplinks/Ports** table.
   The **New WAN Uplink / Port** pop-up is displayed.
9. Enter a name for the WAN port in the **Uplink** field.
10. Select the type of WAN uplink from the **WAN type** drop-down list. For example, **Internet** or **MPLS**.
11. Configure the **WAN Speed**. By default, the WAN uplink speed is set to 20 Mbps. You can configure a custom value for uplink speed as per your requirement. The allowed range of values is 1–10000 Mbps.

12. Select **Source NAT** to enable NAT for the outbound traffic on the WAN interface.
13. Select the **Use as backup** check box to use the uplink in the standby mode. By default, all uplinks operate as active uplinks.
14. Select an **IP addressing method** from the following options:
    - **Static**—For the static IP addressing method, enter the IP address and subnet mask.
      - Enter **IPv4 Address**—a unique static IP address for each gateway in the group or a common address for all gateways in the group.
      - Enter **Netmask**—the subnet mask of the IP address.
    - **DHCP**—When selected, the IP address from a DHCP pool is assigned for the WAN uplink.
    - **PPPOE**—This is the Point to Point Protocol over Ethernet. When selected, you need to select an authentication type to connect to the ISP.
      - Turn on the **Group credentials** toggle switch.
      - Select an **Authentication type**. If you select Password Authentication Protocol (**PAP**), enter the username and password for PPPoE authentication. If you select Challenge handshake authentication protocol (**CHAP**), enter the user name and CHAP secret for authentication.
15. Select a port from the **Port** drop-down list.
    - If you select **LTE**, the **WAN type** field displays **Cellular**.
    - Select the connection type (**Internal** or **USB**) in the **Cellular type** drop-down list.
16. To apply the default inbound security ACL for WAN ports, select the **Secure with ACL** check box.
17. Click **Save Settings**.

Configuring a WAN Interface for a Branch Gateway Group

To configure the WAN interface, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group. Ensure that the group contains at least one Branch Gateway.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **WAN** > **WAN Details**.
6. Turn on **Enable HA deployment** toggle switch to deploy LAN redundancy.
7. To add a WAN port, click + in the **WAN Uplinks/Ports** table.

   The **Add/Edit WAN Port** pop-up is displayed.
8. Enter a name for the WAN port in the **Uplink** field.
9. Select the type of WAN uplink from the **WAN type** drop-down list. For example, **Internet** or **MPLS**.
10. Configure the **WAN Speed**. By default, the WAN uplink speed is set to 20 Mbps. You can configure a custom value for uplink speed as per your requirement. The allowed range of values is 1–10000 Mbps.
11. To enable NAT for the outbound traffic on the WAN interface, select **Source NAT**.
12. To use the uplink in the standby mode, select the **Use as backup** check box. By default, all uplinks operate as active uplinks.

13. Select an **IP addressing method** from the following options :
    - **Static**—For the static IP addressing method, enter the IP address and subnet mask.
        - Enter **IPv4 Address**—a unique static IP address for each gateway in the group or a common address for all gateways in the group.
    - **DHCP**—When selected, the IP address from a DHCP pool is assigned for the WAN uplink.
    - **PPPOE**—This is the Point to Point Protocol over Ethernet. When selected, you need to select an authentication type to connect to the ISP.
        - Turn on the **Group credentials** toggle switch.
        - Select an **Authentication type**. If you select Password Authentication Protocol (**PAP**), enter the username and password for PPPoE authentication. If you select Challenge handshake authentication protocol (**CHAP**), enter the user name and CHAP secret for authentication.
14. Select a port from the **Port** drop-down list.
    - If you select **LTE**, the **WAN type** field displays **Cellular**.
    - Select the connection type (**Internal** or **USB**) in the **Cellular type** drop-down list.
15. To apply the default inbound security ACL for WAN ports, select the **Secure with ACL** check box.
16. Click **Save Settings**.

Configuring a WAN Interface for a VPNC

To configure the WAN interface, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the List view.
3. Click a VPNC under **Device Name**.

   The device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **WAN** > **WAN Details**.
6. To add a WAN port, click the **+** icon in the **Uplinks** table.

   The **New Uplink** pane is displayed.
7. Enter a name for the WAN port in the **Uplink** field.
8. Select the **Interface VLAN ID** from the drop-down list.
9. Select the type of WAN uplink from the **WAN type** drop-down list. For example, Internet or MPLS.
    - The selection of **Internet** or **MPLS** determines the type of IP address used:
        - Select **Internet** to use a **Public IP** address.
        - Select **MPLS** to use a **Private IP** address.
10. Click **Save Settings**.

Configuring Routing Profiles

Aruba's SD-Branch solution leverages WAN services that interconnect hub and spoke sites to establish VPN tunnels, which encapsulate and forward corporate traffic. Each WAN service is referred to as the underlay network, while the VPN tunnels form the overlay network.

The Branch Gateway and VPNC in an SD-Branch network must have IPv4 routes to determine how each device must reach Aruba Central and its VPN peers over any intermediate public or private IPv4 networks

(underlay routes). Routes are also required to determine which internal networks must be reached by the Aruba Gateways through the overlay VPN tunnels (overlay routes).

In Basic mode, the routing profiles can be configured at the device or group level for both Branch Gateway and VPNC.

Configuring Routing Profiles for a Branch Gateway or Branch Gateway Group

To configure a routing profile on a Branch Gateway or Branch Gateway group:

1. In the **Network Operations** app, select one of the following options:
   - To configure a Branch Gateway group complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the group configuration dashboard.
   - To configure a Branch Gateway complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **SDWAN & Routing** > **Static Routing**.
4. To create a default route, click the **+** icon in the **Default Routes** table:
   - **Type**—Select the default route type; **Next Hop** or **VPNC**.
   - **Next Hop/VPNC**—Enter the IP address of the Next Hop or VPNC.
   - **Uplink**—Select the uplink from the drop-down list.
   - **Cost**—Enter the cost metric of the route.
5. To create a static route, click the **+** icon in the **Static Routes** table and enter the following:
   - **Destination IP**—Enter the destination IP address.
   - **Destination Mask**—Enter the subnet mask of the destination IP address.
   - **Type**—Select the type of route.
     - **Nexthop**—Select this option to configure a nexthop destination.
     - **Blackhole**—Black holes refer to places in the network where incoming or outgoing traffic is discarded (or dropped), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic.
   - **Next Hop**—The IP address for the next hop.
   - **Cost**—The cost metric for the route.
6. Click **Save Settings**.

Configuring Routing Profiles for a VPNC or VPNC Group

To configure a routing profile on a VPNC or VPNC group:

1. In the **Network Operations** app, select one of the following options:
   - To configure a VPNC group complete the following steps:
     a. Set the filter to a group containing at least one VPNC.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the group configuration dashboard.
   - To configure a VPNC complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **SDWAN & Routing** > **Static Routing**.
4. To create a default route, click the **+** icon in the **Default Routes** table:
   - **Next Hop**—Enter the IP address of the Next Hop.
   - **Cost**—Enter the cost metric of the route.
5. To create a static route, click the **+** icon in the **Static Routes** table and enter the following:
   - **Destination IP**—Enter the destination IP address.
   - **Destination Mask**—Enter the subnet mask of the destination IP address.
   - **Type**—Select the type of route.
     - **Nexthop**—Select this option to configure a nexthop destination.
     - **Blackhole**—Black holes refer to places in the network where incoming or outgoing traffic is discarded (or dropped), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic.
   - **Next Hop**—The IP address for the next hop.
   - **Cost**—The cost metric for the route.
6. Click **Save Settings**.

Configuring VPN Hubs and Routing Profiles

In Basic mode, the VPN hubs and routing profiles can be configured at the group level for Branch Gateway only.

To configure VPN hubs and routing profiles, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group. Ensure that the group contains at least one Branch Gateway.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.

4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **DC Preference**.
6. In the **DC Preference** page, click the **+** icon in the **DC Preference** table to add a VPN hub group.
7. Select the **Hub Group** from the drop-down list.
8. Select a primary and secondary VPNC from the drop-down list.
9. Click **Save Settings**.

Configuring Overlay Routing Profiles

In Basic mode, the overlay routing can be configured at the device level for VPNC and the group level for both Branch Gateway and VPNC.

Configuring an Overlay Routing for a Branch Gateway Group

To configure Overlay routing profiles, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group. Ensure that the group contains at least one Branch Gateway.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **Overlay Routing**.
6. Select the VLANs to be advertised in the **Redistribute connected vlans** box to allow Branch Gateways to redistribute connected routes to hubs.
7. To allow Branch Gateways to redistribute static routes, select the **Redistribute static routes** check box.
8. Click **Save Settings**.

Configuring an Overlay Routing for a VPNC Group

VPNCs use the Overlay Agent Protocol (OAP) to automatically build the SD-WAN overlay topology. The OAP allows advertising local routes to the SD-WAN Orchestrator in Aruba Central.

To configure Overlay routing profiles, complete the following steps:

1. In the **Network Operations** app, set the filter to VPNC group. Ensure that the group contains at least one VPNC.

   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click **Config**.

   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **Overlay Routing**.

6. Configure **Redistribution Rules.**

   Redistribution rules allow you to enable the advertising of routing information from the connected, static, OSPF, and BGP interfaces into overlay routing. Routing information from other sources is not automatically redistributed into overlay routing, but need to be configured for each source protocol locally on each Gateway.

   To configure redistributing rules, complete the following steps:

   a. Click **Redistribution**, to open the **Redistribution Rules** table.
   b. To add a redistribution rule, click the **+** icon in the **Redistribution Rules** table.
   c. From the **Source Protocol** drop-down list, select a protocol to be redistributed into the overlay routing. The following options are available:
      - **Static**—To redistribute IP static routes. Select a route map from the **Route Map** drop-down list.
      - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site. If you have selected **Connected**, select the VLAN **1** or **Loopback** interface to which the gateway is connected.
      - **OSPF**—To redistribute routes learned from the OSPF neighbors. Select the OSPF path type from the **Filter** column. The following filter options are available:
        - **Intra Area**—To redistribute routes to the same area from which they originated.
        - **Inter Area**—To redistribute routes to another area in the OSPF domain.
        - **External Type 1**—To redistribute routes as External type 1 which applies external cost to the destination and the costs to reach the boundary router in an Autonomous System.
        - **External Type 2**—To redistribute routes as External type 2 and apply only the external costs to the destination.
      - **BGP**—To redistribute routes using BGP. Select a route map from the **Route Map** drop-down list.
7. Select a route map from the **Route Map** drop-down list.
8. Configure **Data Center Aggregating Routes**.

   For dynamic route summarization and faster calculation of best routing paths, you can configure a route aggregation criteria. The route aggregation feature summarizes multiple routes into a single route advertisement and thus helps in reducing the number of routing tables exchanged between BGP peers.

   To aggregate data center routes, complete the following steps:

   a. Click **Data Center Aggregating Routes**, to open the **DC Aggregate Routes** table.
   b. To allow branch route aggregation, click **Allow branch to branch** check box.
   c. Enter the following details in the **DC Aggregate Routes** table:
      - **IP Address**—Enter a network IP address.
      - **Mask**—Enter the subnet mask.
9. Click **Save Settings**.

Configuring an Overlay Routing for a VPNC

To configure Overlay routing profiles, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.

3. Under **Manage**, click **Device**.

   The gateway device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **Overlay Routing**.
6. To add a redistribution rule, click the **+** icon in the **Redistribution Rules** table.
7. From the **Source Protocol** drop-down list, select the type of routes to redistribute. The following options are available:
   - **Static**—To redistribute IP static routes. Select a route map from the **Route Map** drop-down list.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site. If you have selected **Connected**, select the VLAN interfaces to which the Gateway is connected.
   - **OSPF**—To redistribute routes learned from the OSPF neighbors. If you have selected **OSPF**, select the OSPF path type from the **Filter** column. The following options are available:
     - **Intra Area**—To redistribute routes to the same area from which they originated.
     - **Inter Area**—To redistribute routes to another area in the OSPF domain.
     - **External Type 1**—To redistribute routes as External type 1 which applies external costs to the destination and the cost to reach the boundary router in an Autonomous System.
     - **External Type 2**—To redistribute routes as External type 2 and apply only the external cost to the destination.
   - **BGP**—To redistribute routes using BGP. Select a route map from the **Route Map** drop-down list.
8. Select a route map from the **Route Map** drop-down list.
9. Click **Save Settings**.

Configuring SD-WAN Overlay Routing

In Basic mode, the Route Maps can be configured at the device or group level for VPNC only.

Configuring SD-WAN Overlay for a VPNC or VPNC group

To configure SD-WAN Overlay, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one VPNC.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the VPNC group configuration dashboard.
   - To configure a VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one VPNC.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a VPNC under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **SDWAN & Routing** > **SD-WAN Overlay**.

4. Click the **Enable Overlay Orchestration** toggle switch.
5. Click the **Forward branch internet traffic to a specific Next-Hop router IP using PBR**.
   - Enter the **Next-Hop Router Ipv4 Address**.
   - Enter the **Backup Next-Hop Router IPv4 Address**.
6. Click **Save Settings**.

Configuring Route Maps

In the **Route Maps** tab, you can configure **Community List Rules**, **Prefix Lists**, and **Route Maps**.

In Basic mode, the Route Maps can be configured at the device or group level for VPNC only.

Configuring Community List Rules

The Community List feature allows administrators to configure a set of community attributes to apply on routes exchanged between Aruba Gateways and their peers. The community attribute allows grouping routes with similar properties and is generally used for tagging routes and modifying BGP routing policies.

Configuring Community List Rules for a VPNC or VPNC group

To create a community list, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one VPNC.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the VPNC group configuration dashboard.
   - To configure a VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one VPNC.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a VPNC under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **SDWAN & Routing** > **Route Maps**.
4. Click on the **Community List** accordion.
5. Click the **+** icon in the **Community list rules** table.
6. Enter a **Name** for the community list rule.
7. From the **Action** drop-down list select **Permit** or **Deny**, to match the community specifications.
8. Select a **Well Known Community** from the following options in the drop-down list. Following are the options available:
   - **Internet**—Advertises the prefix to all BGP neighbors.
   - **No-Export**—Does not advertise the prefix to any eBGP neighbor. It advertises the prefix only to iBGP neighbors.
   - **No-Advertise**—Does not advertise the prefix to any peer, iBGP or eBGP neighbor.

- **Local-as**— Does not advertise the prefix outside of the local Autonomous System.

  You can also enter a value for the following types of community strings and click **+** to add.

  - **AS:NN**—The BGP community string in the AS:NN format, where AS refers to the Autonomous System number and NN refers to the network number. The valid range of values is 0-65535.

9. Enter a match in the **Community Value**.
10. Enter the community string in the **AS:NN** format, where AS refers to the Autonomous System number and NN refers to the Network Number. The valid range of values is 0-65535.
11. Click **Save Settings**.

Configuring a Prefix List

A prefix list allows routing systems to determine which routes must be accepted when they peer with other networks. Prefix lists contain one or more ordered entries that are processed sequentially.

Prefix lists can be used as match criteria for applying route map rules on network subnets. For example, if you want to prevent a route for 10.0.0.0/24 from being redistributed, you can define a rule to match the prefix and add it a as match criterion in the BGP redistribution route map.

Configuring a Prefix List for a VPNC or VPNC group

To create a prefix list, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one VPNC.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the VPNC group configuration dashboard.
   - To configure a VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one VPNC.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a VPNC under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Ensure you are in the **Basic Mode**.
3. Click **SDWAN & Routing** > **Route Maps**.
4. Click on the **Prefix List** accordion.
5. Click the **+** icon in the **Prefix Rules** table.
6. Enter a **Name** for the prefix rule.
7. Enter a **Sequence** number.
8. From the **Action** drop-down list select **Permit** or **Deny**, when the traffic matches the condition defined in the prefix rule.
9. Enter the network **address** to which you want to apply the prefix rule.
10. Enter the **Mask** of the network.

11. If you want to define a prefix length parameter and use it as a match criterion for applying rules, enter a value greater than or equal to this value for the **GE** operator. The allowed range of values is 1–32.
12. If you want to define a prefix length parameter and use it as a match criterion for applying rules, enter a value lower than or equal to this value for the **LE** operator. The allowed range of values is 1–32.
13. Click **Save Settings**.

Configuring Route Maps

Route maps allow you to configure filtering criteria by defining a set of rules or match statements with permit or deny condition. A route map includes a series of match statements to determine if a route matches the criteria defined in the statement and then, apply for the permit or deny rule accordingly.

Important Points to Note

The following list includes some of the important points to consider when configuring a route map:

- A route map includes name, sequence number, permit or deny rule, the match, and set statements. The match statements determine the route or the traffic to which the rule must be applied, whereas the set statements allow you to configure attributes or adjust metrics for the route that matches the criteria defined in the match statement.
- The route map rules are applied sequentially; that is, based on the sequence number defined for each entry.
- The route map can use a prefix-list in the match statement to apply the allow or deny rule. For more information on prefix lists, see Configuring a Prefix List.
- Route maps can be attached to the BGP neighbor profiles for the inbound and outbound routes. You can associate route maps for the inbound and outbound traffic when configuring a BGP neighbor profile. When the route map policy is applied to the inbound or outbound BGP route, and if the traffic matches the specified criteria, the attribute set for the match condition is applied. If you do not have a route map attached to the BGP neighbor profile, the BGP neighbor can access all inbound and outbound routes. For more information on BGP neighbor profiles. see Adding BGP Neighbors.

Configuring Route Maps for a VPNC or VPNC group

To configure route maps, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one VPNC.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the VPNC group configuration dashboard.
   - To configure a VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one VPNC.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a VPNC under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.

2. Ensure you are in the **Basic Mode**.
3. Click **SDWAN & Routing** > **Route Maps**.
4. Click on the **Route Map** accordion.
5. To add a route map, click the **+** icon in the **Route Maps** table. The **Add/Edit Route Map** window opens.
6. Enter a **Name** for the route map.
7. Enter a **Sequence number** for the route map. Sequence numbers allow route maps to be executed in order. If you are configuring multiple match clauses or statements, ensure that you define a sequence number to uniquely identify each match statement.
8. From the **Action** drop-down list, select **Permit** or **Deny** when the traffic matches the condition defined in the prefix rule.
9. Configure the **Match** condition for the routes that have a destination network. The match statements define a set of conditions for determining if the route redistribution must be allowed or denied. To add a match statement, click the **+** icon in the **Match** table. You can set match type to any of the following:
   - **IP address**— If you have selected the IP address for match type, select a value from the drop-down list.
   - **Next-hop IP**—If you have selected Next-hop IP for match type, select a value from the drop-down list.
   - **Well known community**—A well-known community allows you to configure one of the following options:
     - **Internet**—Advertises subnets to all BGP neighbors.
     - **No-export**—Does not advertise the prefix to any eBGP neighbor.
     - **No-advertise**—Does not advertise subnets to BGP neighbors.
     - **Local-as**—Prevents sending packets outside the local autonomous system.
   - **Community AS:NN**— The community string is in the AS:NN format, where AS refers to the Autonomous System number and NN refers to the network number. The valid range of values is 0-65535.
   - **Community value**—This allows you to specify a community value string. The valid range of values is 1–4294967295.
   - **Community list**—This allows you to select a community list configured on the Gateway.
   - **Interface VLAN**—Enter the interface VLANs separated by a comma. You can enter up to 10 Interface VLANs. The value you enter must be between 1 to 4095. To know how to configure VLANs, see Configuring VLANs on Aruba Gateways.
   - **OSPF route tag**—You need to enter the tag names separated by a comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.
10. Configure a **Set** of rules or attributes to apply to the BGP traffic that matches the conditions defined in a match statement.

    The **Set** configuration is applicable for VPNC at the device level only and not applicable for group configuration.

    To add a **Set** level attribute, click the **+** icon in the **Set** table and configure the following attributes as per your requirement:
    - **as-path-prepend**—Prepends AS numbers through which the packets have traversed. You can apply the AS path prepending criteria to the BGP traffic to determine the best path.

- **last-as**—Prepends the last AS number to the AS path. The valid range of values is 1–10.
- **Community value**—The BGP community value string. The valid range of values is 1–4294967295.
- **Community AS:NN** for match type, the community string is in the AS:NN format. The valid range of values is 0-65535.
- **Well known community**—A well-known community. You can configure one of the following options:
  - **Internet**—Advertises subnets to all BGP neighbors.
  - **No-export**—Does not advertise the prefix to any eBGP neighbor.
  - **No-advertise**—Does not advertise subnets to BGP neighbors.
  - **Local-as**—Prevents sending packets outside the local autonomous system.
- **Local-as**—Sets a local autonomous system string as an attribute in the routes.
- **metric**—Sets a metric value for determining the preferred path into an Autonomous System. You can define a metric value between 0—4294967295. When a metric value in a route matches this value, the route is advertised.
- **origin**—Sets the origin of the route. The following options are available:
  - **incomplete**—To specify that the route is originated from the exterior routing protocol.
  - **igp**—To specify that the route is originated from an internal routing protocol.
- **OSPF route-type**—Sets the external metric (**External Type-1** or **External Type-2**) attribute of the route.
  - To redistribute as routes as **External type 1** which applies external costs to the destination and the cost to reach the boundary router in an Autonomous System.
  - To redistribute routes as **External type-2** and apply only the external cost to the destination.
- **OSPF route tag**—Sets the tag attribute of the route. Enter the tag names separated by a comma. You can enter up to 10 tags. At least one of these tags has to match to allow route redistribution. The value you enter must be between 0 to 4294967295.

11. Click **Save Settings**.

Configuring OSPF

The OSPF configuration allows advertising branch networks into an OSPF area and enables VPNCs to learn corporate routes. You can configure the **General**, **Interface**, and **Redistribution** settings in this section.

In Basic mode, the OSPF can be configured at the device level for VPNC only.

Enabling OSPF on VPNC

To enable OSPF, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Under **Manage**, click **Device**.
   The gateway device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **OSPF**.
6. Click the **General** accordion.

7. Click the **Enable OSPF** toggle switch to enable OSPF.
8. Select the **Default originate** check box to generate a default external route to OSPF.
9. Enter the **Router ID**. The router ID is the IPv4 address of the gateway used for identifying it as the router in an autonomous system.
10. Set the OSPF **Area ID** for the interface VLAN.
11. Click **Save Settings**.

Configuring Interface

To configure the interface, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Under **Manage**, click **Device**.

   The gateway device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **OSPF**.
6. Click the **Interface** accordion.
7. To add an interface, click the **+** icon in the **VLANs** table.
8. Select an OSPF interface **VLAN** from the drop-down list.
9. Set the OSPF **Area ID** for the interface VLAN.
10. Set the **Cost** for the interface VLAN.
11. Set the **Hello Interval** timer to send messages to neighbors.
12. Click **Save Settings**.

Configuring Redistribution Rules

To configure redistribution rules, complete the following steps:

1. In the **Network Operations** app, set the filter to a group or **Global**. Ensure that the group contains at least one VPNC.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.

   The dashboard context for the gateway is displayed.
4. Under **Manage**, click **Device**.

   The device configuration page is displayed.
5. Ensure you are in the **Basic Mode**.
6. Click **SDWAN & Routing** > **OSPF**.
7. Click **Redistribution**.
8. To add a redistribution rule, click **+** under the **Redistribution Rules** table and configure the following parameters:

a. From the **Source Protocol** drop-down list, select a source type:
   - **Static**—To redistribute IP static routes.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site.
   - **SD-WAN Overlay**—To redistribute routes learned from the SD-WAN overlay network through the Overlay Agent Protocol.
   - **IAP-VPN Overlay**—To redistribute routes that were received from deployments with Instant APs.

b. From the **Route Type** drop-down, select an OSPF route type. Aruba Gateways support propagating OSPF routes as External Type 1 (E1) and External Type 2 (E2) routes.
   - **E1**—The External Type 1 applies external costs to the destination and the cost to reach the boundary router in an Autonomous System.
   - **E2**—The External Type 2 type applies only the external cost to the destination.

c. Optionally, you can select a **Route Map** to associate with the routes.

9. Click **Save Settings**.

Configuring BGP

To support interoperability with an existing network infrastructure, BGP, a dynamic routing protocol enables VPNCs to redistribute overlay routes learned from Branch Gateways into BGP and advertise those routes in the data center network.

In Basic mode, the BGP can be configured at the device level for VPNC only.

Configuring General Settings on a VPNC

To enable BGP, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Under **Manage**, click **Device**.
   The gateway device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **BGP**.
6. Click the **General** accordion.
7. Click the **Enable BGP** toggle switch to enable BGP.
8. Select the **Default originate** check box to generate a default external route to OSPF.
9. Enter the **AS number** to determine if the BGP neighbor is in the same Autonomous System (AS).
10. Enter the **Router ID**. The router ID is the IPv4 address of Gateway used for identifying it as the router in an autonomous system.
11. Click **Save Settings**.

Configuring Neighbors

To configure neighbors, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Under **Manage**, click **Device**.

   The gateway device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **BGP**.
6. Click the **Neighbors** accordion.
7. To add neighbors, click the **+** icon in the **Neighbors** table.
8. Enter the **Peer Address** (IP address) of the neighbor you want to establish communication with.
9. Enter the number of **Remote AS** to which the peer router belongs.
10. Select the **Multi-Hop** check box if you want the gateway to route packets to its remote BGP peer that is more than one hop away.
11. Set the **Update Source** for the Interface or IP address used for the BGP updates in a multi-hop scenario.
12. Select the **Route Map In** value from the drop-down list. This is a per-neighbor routing policy that is applied to information received from the neighbor.
13. Select the **Route Map Out** value from the drop-down list. This is a per-neighbor routing policy that is applied to information sent to the neighbor.
14. Click **Save Settings**.

Advertising Networks to BGP

To advertise networks, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices**, and then click **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Under **Manage**, click **Device**.

   The gateway device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **BGP**.
6. Click the **Networks to Advertise** accordion.
7. To add networks, click the **+** icon in the **Prefixes To Aggregate** table.
8. Select the prefix type as **Network** or **Aggregate** from the **Type** drop-down list.
9. Enter the network IP **Address** that you want to be advertised.
10. Enter the subnet **Mask** for the advertised network.
11. If you select **Aggregate** from the **Type** drop-down list, then select the **Route Map**.
12. Click **Save Settings**.

Configuring Redistribution Rules

To configure Redistribution Rules, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global** or a group containing at least one VPNC.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Under **Manage**, click **Device**.
   The gateway device configuration page is displayed.
4. Ensure you are in the **Basic Mode**.
5. Click **SD-WAN & Routing** > **BGP**.
6. Click the **Redistribution** accordion.
7. To add rules, click the **+** icon in the **Redistribution Rules** table.
8. From the **Source Protocol** drop-down list, select the type of routes to redistribute. The following options are available:
   - **Static**—To redistribute the static routes manually configured on Branch Gateways.
   - **OSPF**—To redistribute the routes learned from an OSPF neighbor.
   - **SD-WAN Overlay**—To redistribute routes learned from the SD-WAN overlay network through the Overlay Agent Protocol.
   - **Connected**—To redistribute routes received from the subnets that are directly connected to a router's interface at the hub site.
   - **IAP-VPN Overlay**—To redistribute routes that were received from micro-branch deployments with Instant APs.
9. Optionally, you can select a route map to associate with the routes.
10. Click **Save Settings**.

Configuring LAN Redundancy for High Availability

Before you proceed, ensure that you have enabled High Availability on the WAN page and configured the peer gateway for redundancy. For the configuration details, see the Configuring WAN Uplinks and Ports for WAN Interface page.

In Basic mode, LAN Redundancy can be configured only at the device level for a Branch Gateway.

Configuring a LAN Redundancy for a Branch Gateway

To configure LAN redundancy, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.
   The dashboard context for the device is displayed.
4. Under **Manage**, click **Device**.
   The device configuration page is displayed.
5. Ensure you are in the **Basic Mode**.
6. Click **Redundancy** > **VRRP**.
7. Click the **+** icon in the **VRRP Interfaces** table and configure the following parameters:
   - **VLAN ID**—VLAN ID for which you want to set up the redundant gateway.
   - **IP Address on Local**—The IP address of the VLAN on the local gateway.

- **IP Address on Peer**—The IP address of the VLAN on the peer gateway.
- **Virtual IP**—The virtual IP of the VLAN.
- **Conductor** —The designated active gateway of the redundant pair.

8. Click **Save Settings**.

Configuring VPN Pools

A VPN pool refers to a pool of IP addresses configured for a device group. The system IP addresses for the SD-WAN Gateways are assigned from the gateway pool when a device joins the group.

In Basic mode, VPN pools can be configured only at the group level for a VPNC group.

Creating VPN Pools for a VPNC Group

To create a gateway pool for a device group, complete either of the following steps:

1. In the **Network Operations** app, set the filter to VPNC group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **VPN** > **VPN Pools**.
6. Click the **+** icon in the **Address Pools** table to add a pool.
7. In the **Pool name** field, enter a name for the new pool.
8. In the **Start IP address** field, enter the first IP address of the IP address range.
9. In the **End IP address** field, enter the last IP address of the IP address range.
10. Select the **IAP-VPN pool** from the drop-down list.
11. Click **Save Settings**.

Configuring Policies for a Branch Gateway Group

In the **Policies** tab, you can configure the following types of policies for a Branch Gateway group:

- Role assignment policy—Policy to determine client access based on the user roles assigned to a client.
- Application usage policy—Policy for deep packet inspection of application usage by clients.
- Traffic steering policy—Policy for dynamically steering client traffic to best performing uplink.
- QoS policy—Policy to prioritize critical traffic, prevent excess bandwidth usage and manage network bottlenecks to prevent packet drops.
- Security policy—Policy to filter website content.

Configuring a Role Assignment Policy

Configure this policy to determine client access based on the user roles assigned to a client.

In Basic mode, the role assignment policies can be configured at the group level for Branch Gateways only.

Configuring a Role Assignment Policy for a Branch Gateway Group

To configure a role assignment policy, complete the following steps:

1. In the **Network Operations** app, set the filter to a Branch Gateway group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **Policies** > **Roles**.
6. Click the **+** icon to add a user role in the **Roles** table. The policies that are associated with this role are configured in subsequent steps.
7. Click the **+** icon in the **Role Assignment** table. The **Role Assignment** pop-up appears.
8. Select a VLAN ID to which this role needs to be applied, from the **VLAN ID** drop-down list.
9. Select a role from the **Initial role** drop-down list. This is the default user role that is assigned to the clients connecting through this VLAN.
10. To enable authentication, turn on the **Authentication** toggle switch.
11. Select the **Default authentication role** from the drop-down list.
12. Select one of the following authentication modes:
    - **MAC authentication**—Select this check box to assign a role after a client device completes MAC authentication. The default role for MAC authentication is the **guest** user role.
    - **802.1X authentication**—Select this check box to assign a role after a client device completes 802.1X authentication. You can also enable MAC authentication to allow clients to complete 802.1X authentication when MAC authentication fails and vice-versa.
13. Configure primary and backup authentication servers. This defines them as Authentication, Accounting, and CoA (RFC3676) servers.
14. To add a AAA server, click the **+** icon in the **Select AAA Servers** table and configure the following parameters:
    - **Name**—The server name.
    - **Server IP**—The IP address or FQDN of the server.
    - **Password**—The password to use for authentication.
    - **Retype Password**—Confirm password.
15. Click **Save** in the Role Assignment window.
16. Click **Save Settings**.

Configuring Applications

Configure this policy for deep packet inspection of application usage by clients.

In Basic mode, the application policies can be configured at the group level for Branch Gateways only.

Configuring Applications Policies for a Branch Gateway Group

To define applications, and other security aliases, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **Policies** > **Applications**.
   The list of applications and application categories available for Branch Gateways to create a policy appears.
6. Click the **+** icon in the **Applications** table to add an application or the application category with the server name and the corresponding domain URI. Configure the following parameters in the **Add/Edit Application** window:
   - **Name**—Enter the name of the application.
   - **Category**—Enter the application category.
   - In the **Servers** table, click the + icon to add the server name and the URI that the application uses.
   - Click **Save**.
7. To create a network alias, click + in the **Network Aliases** table and configure the following parameters:
   - **Name**—Enter the name of the network alias.
   - **Description**—Enter description text for the alias.
   - **Invert**—Select this check box if you want to apply the firewall rules to all the destinations except the one configured in the alias.
   - **User Rules**—Click **+** to add user rules. The following rule types are available:
     - **Host**—Allows you to configure a rule for a specific host IP address.
     - **Name**—Allows you to configure a rule for a specific domain name.
     - **Range**—Allows you to configure a rule for a range of IP addresses.
     - **Network**—Allows you to configure a rule for a specific network IP address and subnet mask.
     - **Override VLAN**—Allows you to configure a rule for overriding a specific VLAN.
8. Click **Save**.
9. To create a service alias, click the **+** icon in the **Service Aliases** table and configure the following parameters in the **Add/Edit Service Alias** window:
   - Enter a value in the **Service name** field.
   - In the **Protocol** drop-down list, select one of the following options:
     - **TCP**
     - **UDP**
     - **Protocol**
   - If you select **Protocol**, enter the IP protocol number in the **Protocol number** field.
   - If you select **UDP** or **TCP**, in the **Port type** drop-down list, select one of the following options:
     - **Range**—If you select a **range** to provide a contiguous list of ports, enter the starting and ending port numbers in the **Start port** and **End port** fields, respectively.
     - **List**—If you select **List**, enter a comma-separated list of port numbers in the **Port list** field.

- To limit the service alias to a specific application, select a service type from the **ALG** (Application Level Gateway) drop-down list.

10. Click **Save** in the **Add/Edit Service Alias** window.
11. Click **Save Settings**.

Configuring a Traffic Steering Policy

A dynamic path steering policy serves as a global policy that determines paths for the outgoing corporate and Internet traffic. The DPS policy is configured for dynamically steering client traffic to the best performing uplink.

In Basic mode, the DPS policies can be configured at the group level for Branch Gateways only.

Configuring a Traffic Steering Policy for a Branch Gateway Group

To configure a traffic steering policy, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **Policies** > **DPS**.
   The list of default traffic policies appears.
6. Click the **+** icon in the **Policies** table.
7. Select **DPS** or **SAAS** in the **Policy Type** drop-down list.
8. If you have selected **SAAS**, select the **Application** in the drop-down list.
9. If you have selected **DPS**, enter the name of the policy.
10. Click **Save**.

Configuring a QoS Policy

Quality of service (QoS) policy allows you to prioritize critical traffic, prevent excess bandwidth usage, and manage network bottlenecks to prevent packet drops.

In Basic mode, the QoS policies can be configured at the group level for Branch Gateways only.

Configuring a QoS Policy for a Branch Gateway group

To configure a QoS policy, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.

5. Click **Policies** > **QoS**.

   The list of roles appears. You can review the bandwidth contracts, and QoS priorities assigned for each role or application.
6. To edit the QoS for a user role, select the user role in the **Roles** table. Click the **+** icon in the **QoS for <selected role name>** table and configure the following parameters:
   - **Type**—Select the policy type as Application or Application Category from the drop-down list. Enter the **Application** or **Application category** based on the policy type that is selected.
   - **QoS Profile**—Select one of the following from the drop-down list for the QoS profile:
     - **Realtime**—Select this option if the policy applies to realtime, delay-sensitive data transmission such as audio and video conferencing.
     - **Transactional**—Select this profile for applications such as SAP, PeopleSoft where the response time required is more than the generic client-server applications.
     - **Collaboration**—Select this option for highly interactive applications that require user feedback such as Instant Messaging applications.
     - **Best effort**—This profile is used for the majority of the data traffic unless the data requires preferential treatment.
7. **Upstream B/W**—(Optional) Define the upstream bandwidth in Mbits or Kbits.
8. **Downstream B/W**—(Optional) Define the downstream bandwidth in Mbits or Kbits.
9. Click **Save**.

Click **Show QoS profiles** to view the DSCP marking for individual QoS profiles in the **QoS Profiles** table.

Configuring Policy-Based Routing (PBR) Policy

The PBR policies allow full-tunnel traffic to the data center or a cloud security service provider for further traffic inspection.

In Basic mode, the PBR policies can be configured at the group level for Branch Gateways only.

Configuring PBR Policies for a Branch Gateway group

To configure a PBR policy, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.

   The gateway group basic mode configuration page is displayed.
4. In the **Policies** > **PBR** page, turn on the toggle switch to select either **Internet through DC** or **Cloud Security** depending on the role.
   - Select **Internet through DC**, if you want to allow access to the internet via the data center.
   - Select **Cloud Security**, if you want to inspect the traffic by routing it to the third-party cloud security provider.
5. To configure the **Internet through DC** policy, click the edit icon next to it.

6. In the **Internet through DC** table, select the **Primary Hub** from the drop-down list. To know how to set DC preference, see Configuring Overlay Network Using SD-WAN Orchestrator.
7. Select the **Applications** and the **App categories** for which you want to provide an exception.
8. Click **Save**.
9. To configure **Cloud Security** policy, click the edit icon next to it.
10. In the **Cloud Security** table, select the third-party **Cloud Security Partners**.
11. Select the **Applications** and **App categories** for which you want to provide an exception.
12. Click **Save**.

NOTE

For manual integrations, use the advanced configuration workflow.

Configuring Security Policies

Configure firewall policies for website content filtering. In Basic mode, the firewall policies can be configured at the group level for Branch Gateways only.

Configuring Security Policies for a Branch Gateway group

To configure the security policies, complete the following steps:

1. In the **Network Operations** app, set the filter to Branch Gateway group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices**, and then click **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click **Config**.
   The configuration page is displayed for the selected group.
4. Ensure you are in the **Basic Mode**.
5. Click **Policies** > **Security**
   The list of roles and policies appears.
6. To add a role, click the **+** icon in the **Roles** table.
7. To add a policy to a role, click the **+** icon in the **Policies** table.
8. To add an access rule to a policy, click the **+** icon in the **Rules** table and configure the following parameters:
   - **Source** —Select one of the following options from the drop-down list to define the source of the traffic:
     - **Any**—Applies a rule to incoming traffic from any source.
     - **User**—Applies a rule to the traffic originating from a specific user.
     - **Host**—Applies a rule to traffic originating from a specific host IP address. Enter the host **IP** address.
     - **Network**—Applies a rule to the traffic that originates from a specific network. Enter the **IP** address and the subnet **Mask** of the source network.
     - **Network Alias**—Applies a rule to the traffic routed to a specific alias of a host or network. Select the **Source alias** from the drop-down list.
     - **Role**—Applies a rule to traffic originating from a specific user role. Select a **User role** from the drop-down list.

- **Destination**—Select one of the following options from the drop-down list to define a destination for the traffic policy rule:
  - **Any**—Applies a rule to the outgoing traffic to any destination.
  - **Host**—Applies a rule to the traffic routed to a specific host IP address. Enter the host IP address.
  - **Network**—Applies a rule to the traffic routed to a specific network. Enter the IP address and the subnet mask of the source network.
  - **Network Alias**—Applies a rule to the traffic routed to a specific alias of a host or network. Select the **Source alias** from the drop-down list.
- **Service/App**—Select one of the following network services from the drop-down list :
  - **Any**—Applies a rule to all network services.
  - **TCP**—Applies a rule to the incoming and outgoing traffic from the TCP ports. If you have selected the TCP service, specify a list of TCP ports. Select **Min/Max Port** radio-button to specify the start and end port or select the **Source/Dest Port** radio-button to specify the source and destination ports.
  - **UDP**—Applies a rule to the incoming and outgoing traffic from the UDP ports. If you have selected the UDP service, specify a list of UDP ports. Select **Min/Max Port** radio-button to specify the start and end port or select the **Source/Dest Port** radio-button to specify the source and destination ports.
  - **Service**—Applies a rule to the incoming and outgoing traffic from a set of predefined services and protocols; for example, HTTPS and HTTP. Select the **Service alias** from the drop-down list.
  - **Protocol**—Applies a rule to the traffic that uses a specific routing protocol. Enter the protocols in the **Protocol** field.
  - **Application**—Applies rule to the applications. Enter the application names in the **Application** field.
  - **Application category**—Applies rule to the application categories. Enter the Application Categories in the **App category** field.
  - **Web Category/Reputation**—Applies rule to the web category. Enter the web categories in the **Web Category** field and select the **Web reputation** from the drop-down list.
- **Action**—Select one of the following options from the drop-down list:
  - **Deny**—Denies traffic from or to a specific network or network service.
  - **Permit**—Allows traffic from or to a network or network service.
  - **Log**—Creates a log when a policy is applied based on the rules configured.
  - **Mirror**—Mirrors session packets to datapath or remote destination.

9. Click **Save**.

Chapter 17
Overview of Aruba IDPS

The Intrusion Detection and Prevention System (IDPS) monitors, detects, and prevents threats in the inbound and outbound traffic. The Intrusion Detection System (IDS) monitors the network for any malicious activity and generates threat events. The Intrusion Prevention System (IPS) has all the capabilities of IDS along with the ability to prevent intrusions by dropping malicious data packets. As an administrator, you can enable either IDS or IPS.

Aruba IDPS provides an extra layer of protection that actively analyzes the network and takes actions on the traffic flows based on preconfigured rules. These actions include sending threat events and dropping data packets. Aruba IDPS has the capability to analyze data packets that enter the network and act quickly to prevent threats in real time. All identified threats are logged for correlation analysis.

Why Aruba IDPS?

In today's network environments, which are much larger and more complex than in the past, applications and connections are extremely vulnerable. In order to address these challenges, Aruba introduces IDPS that adds an extra layer of security that focuses on users, applications and network connections, and can be integrated with your existing SD-WAN solution. Aruba IDPS proactively prevents and protects the network from intrusions. This is a policy-driven intrusion prevention technology that operates efficiently without manual intervention. IDPS protects the network from real-time attacks without degrading network performance. An advanced security dashboard provides Security Analysts with everything they need to manage an end-to-end zero trust, edge-to-cloud environment providing network-wide visibility, multi-dimensional threat metrics, threat intelligence data, correlation, and incident management.

When IDPS is enabled, certain scenarios in layer 3 high availability (L3HA) are not ideal. Therefore, please review before you choose L3HA with IDPS enabled.

Key Features and Benefits

The following are some of the key features and benefits of Aruba IDPS:

- Full Packet Inspection—Aruba IDPS offers a signature and pattern-based inspection that inspects every data packet for intrusion.
- North-South and East-West inspection—Monitors both LAN and WAN networks.
- Multi-dimensional Threat Metrics—Allows you to identify and view threats from different dimensions such as different protocols, threat types, and so on.
- Allow listing—A list of network-wide and device-level threats, which need not be checked.
- Threat Intelligence—There are various Threat Intelligence categories that can be used in Security Information and Event Management (SIEM). These include Command and control, Ransomware, Phishing, Malware, Spyware, Cryptomining, and so on.
- Correlation and Incident Management—Monitors usage patterns, tracks events, and analyzes event logs and data for any relationship to prevent attacks.

- Simplified Configuration—A user-friendly and intuitive user interface that allows you to configure IDPS for your SD-WAN network with ease. Aruba offers three types of threat profiles: Lenient, Moderate, and Strict.
- Licensing—The Foundation and Advanced SD-WAN licenses are packaged with a Security license that provides IDPS feature.

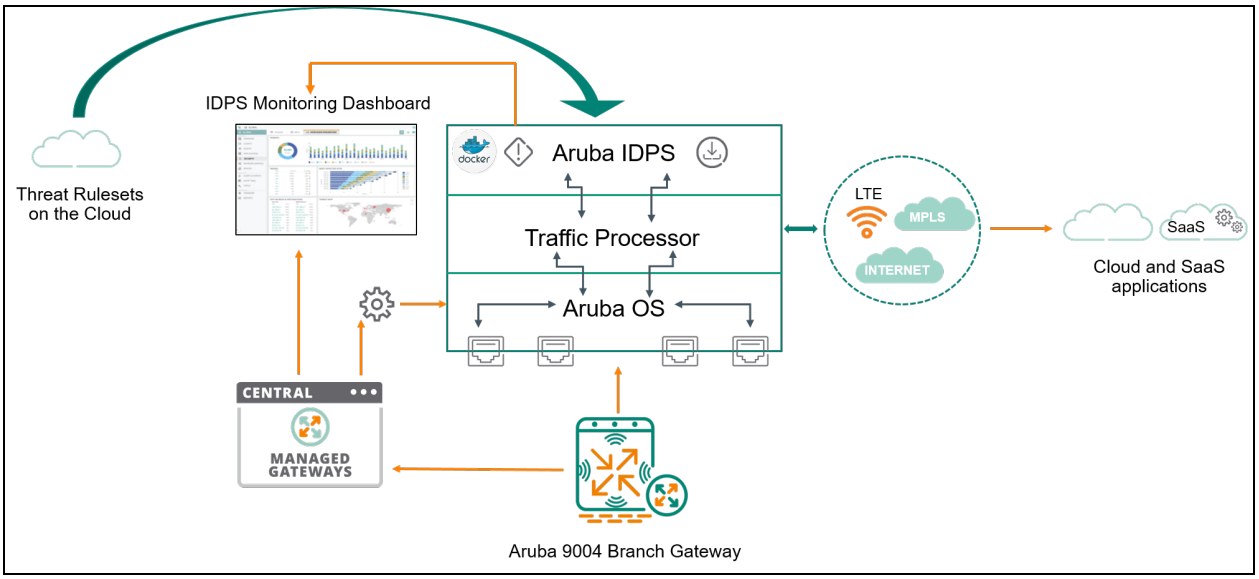
How does Aruba IDPS Work?

Aruba leverages an open source IDPS engine which is integrated as a Virtual Network Function (VNF) with the SD-Branch Gateway. This engine detects and prevents intrusion based on rules set by the user.

The following process describes the Aruba IDPS workflow to detect and prevent intrusions:

- **Download Threat Rulesets**—Aruba IDPS downloads threat rulesets from the cloud repository.
- **Enable Aruba IDPS**—Enable IDPS and configure an IDPS policy in Aruba Central.
- **Stream Realtime Events**—The events are streamed real-time based on preset event category.
- **Enrich Events**—Aruba IDPS enriches events with host, application, and location details.
- **Send Alerts and Drop Packets**—Sends alerts and notifications if IDS is selected and blocks traffic if IPS is selected as the mode of inspection.
- **Monitor Threats**—Monitor and move threats to the Allow List in the IDPS dashboard in Aruba Central.
- **Share Threat Data**—The threat data recorded in Aruba Central is shared with the SIEM server, if configured.

Figure 257 *Aruba IDPS Architecture Diagram*



Preparing to add the Aruba IDPS Supported Gateways

If you are an existing customer who wants to enable and use Aruba IDPS, and do not have Aruba IDPS supported gateways, then you need Aruba IDPS supported gateways and a gateway or SD-Branch security license. For more information on on-boarding and provisioning gateways, see the *Aruba Central Help Center*.

If you are an existing customer who has Aruba IDPS supported gateways deployed, then you need a gateway or SD-Branch security license to use Aruba IDPS

Supported Aruba Gateways for Aruba IDPS

The following table lists the Branch Gateway models that support Aruba IDPS:

Table 283: *Supported Aruba Gateways*

Platform	Deployment Type	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 9004-LTE	Branch Gateway	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0
Aruba 9012	Branch Gateway	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0
	VPNC	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0
Aruba 9004	Branch Gateway	ArubaOS 8.5.0.0-2.1.0.0	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0

The IDPS supported gateway reboots in the following scenarios:

- When you apply the security license to Aruba IDPS supported gateways on the network, the gateways reboot to enable the traffic inspection engine.
- When a System IP is assigned to the gateway.
- When the image on Activate and that on the device are different.
- When you upgrade the software to the recommended version.

When the gateways reboot, there will be a considerable down time in the network. It is recommended that you apply the security license to the existing Aruba IDPS supported gateways during non-working hours.

Best Practices

The following are some of the best practices that you must implement to configure Aruba IDPS and get the IDPS supported gateways up and running:

- Ensure that you set up the recommended SD-WAN image at the group level.
- Assign the gateway or SD-Branch security subscription before you start to configure the IDPS supported gateway.
- Ensure that the device image is compliant with the image in Activate.
- Follow the given sequence of steps to configure Aruba IDPS on a IDPS supported gateway:
    1. Update the SD-WAN software image to ArubaOS 8.5.0.0 - 2.1.0.0.
    2. Apply a valid security subscription.
    3. Enable traffic inspection.

Configuring Aruba IDPS

You must configure Aruba IDPS to enable traffic inspection, threat detection, and threat prevention on the Aruba Branch Gateways. Aruba Central provides an intuitive user interface that allows you to configure IDS or IPS with ease.

- **IDS**—IDS monitors the network for any malicious activity and generates an alert. IDS does not take any action on the identified threats. Configuring IDS will help detect the threats and capture the details of the threats detected.
- **IPS**—IPS monitors the network for malicious activity, generates alerts, and takes action based on a predefined rule. Configuring IPS will help detect the threats, create alerts, and drop the packets for the threats identified.

Threats are detected based on a predefined set of rules grouped based on Common Vulnerability Scoring System (CVSS) .

This chapter contains the following sections:

Configuring Aruba IDPS at Global, Group, and Device Level

- If you select **Global** from the filter, you can configure a Security Incident and Event Management (SIEM) server provided by a third party such as Splunk. To configure Aruba IDPS, you have to select either a group or a gateway that supports Aruba IDPS configuration.
- If you select a **group** from the filter and configure Aruba IDPS, the configuration applies to all Aruba IDPS compatible gateways that are active in the group. The IDPS dashboard and threats list displays data for all Aruba IDPS compatible gateways that are active in the group.
- If you select a **device** from the filter and configure Aruba IDPS, the configuration applies only to the selected gateway, which is active in Aruba Central. The IDPS dashboard and threats list displays data for only the selected Aruba IDPS supported gateways, which are active in Aruba Central.

Enabling Traffic Inspection on Aruba Gateways

You must configure traffic inspection to enable Aruba IDPS.

Before you begin

Ensure that the following requirements are met before you configure Aruba IDPS:

1. You have an active gateway subscription with Security license.
2. You must have on-boarded and connected the Aruba IDPS supported Branch Gateways to Aruba Central successfully.

To enable traffic inspections complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
     The dashboard context for a group is displayed.

b. Click **Gateways**.
c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.

- To configure a Branch Gateway, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
  The dashboard context for the gateway is displayed.

The Branch Gateway or the Branch Gateway in the group that you want to configure must be Aruba IDPS supported.

2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
3. Click the **Config** icon to open the Gateway IDS/IPS configuration page.
4. In the **General** tab, select the **Enable traffic inspection** check box.

After traffic inspection is enabled, the Branch Gateways start to detect malicious events in the inbound and outbound data. IDS is selected as the default mode and IDS Strict is selected as the default policy. You can use the following procedures to configure IDS and IPS based on the requirement. Otherwise, the traffic inspection engine is set up to work on the default configuration.

Updating Ruleset for Aruba IDPS

To use the latest signatures, you must update the rulesets. After enabling traffic inspection, if the rulesets are not the latest, you can update them to the latest. A default ruleset is selected and a list of ruleset versions is available from which you can select a different ruleset version if required. The three recent versions are displayed in the list. The ruleset version is updated automatically every 24 hours.

The following steps provide the procedure to update the ruleset version.

To configure IDS complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
     The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
   - To configure a Branch Gateway, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.

The Branch Gateway or the Branch Gateway in the group that you want to configure must support Aruba IDPS.

2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.

3. Click the **Config** icon to open the Gateway IDS/IPS configuration page.
4. To update the **Ruleset** to a different version, select the version from the **Update To** drop-down list. A confirmation window is displayed.
5. Click **Update.**
6. To automatically update the ruleset at regular intervals, select the **Automatically update the ruleset** check box, and then, select **Week** or **Day** from the drop-down list. If you have selected week, select the day of the week, and time from the drop-down list.

By default, rulesets are updated automatically every 24 hours.

7. Click **Save**.

In the **General** tab, under **Ruleset**, the selected version of the ruleset is displayed. An alert icon ⚠ is displayed if the ruleset version is outdated and is not part of the drop-down list, or when the ruleset version of the device does not match with the ruleset version of the group that it belongs to.

Configuring IDS on Aruba Gateways

Configuring IDS enables traffic inspection engine to check the inbound and outbound data packets for threats and create alerts for the identified threats.

Before you begin

- Ensure that you have enabled traffic inspection to configure IDS.
- The Branch Gateway or the Branch Gateway in the group that you want to configure must support Aruba IDPS.

To configure IDS complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
   - To configure a Branch Gateway, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
3. Click the **Config** icon to open the Gateway IDS/IPS configuration page.
4. In the **General** tab, under **Inspection**, by default, **IDS** is selected as the mode of inspection.
5. Configure **Fail Strategy**:
   a. Select **Bypass** if you want the traffic flow to continue even when the Intrusion Prevention engine crashes and fails to inspect the traffic. A slight disruption in the traffic occurs when

ArubaOS detects an engine failure and takes action based on the fail strategy configuration.

b. Select **Block**, if you do not want the traffic to flow until the Intrusion Prevention engine inspects the data packets. If you select this option, your traffic flow is blocked until the Intrusion Prevention engine starts inspecting the traffic.

6. Click the **Policies** tab. The Policies table displays the following details:
   - **Name**—Displays the names of the following policies:
     - **IDS Lenient**—Contains rules that are from the current year and the previous three years for vulnerabilities with a CVSS score of 4 and above.
     - **IDS Moderate**—Contains rules that are from the current year and the previous two years for vulnerabilities with a CVSS score of 6 and above.
     - **IDS Strict**—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 8 and above.
   - **State**—A toggle switch that allows you to enable policy.

By default, **IDS Strict** is enabled. If you want to change the default policy, select the policy that you want to enforce and click **Enable** in the confirmation window. It takes 2 to 3 minutes for the change to take effect. Note that you can enforce only one policy at a time.
For more information on CVSS score, see https://www.first.org/cvss/.

   - **Mode**—Displays the mode of inspection.

For the current release, IDPS policies are not defined based on user role. Therefore, this field is not configurable.

   - **Security Strategy**—Defines whether the policy is Lenient, Moderate, or Strict.
   - **Action**—The action to be taken on traffic flow: Generate alerts.

Configuring IPS on Aruba Gateways

Configuring IPS enables traffic inspection engine to check the inbound and outbound data for threats, create alerts, drop packets for the threats identified.

Before you begin

- Ensure that you have enabled traffic inspection to configure IPS.
- The Branch Gateway or the Branch Gateway in the group that you want to configure must support Aruba IDPS.

To configure IPS complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
     The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.

- To configure a Branch Gateway, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
  The dashboard context for the gateway is displayed.

2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
3. Click the **Config** icon to open the **Gateway IDS/IPS** configuration page.
4. In the **General** tab, under **Inspection**, select **IPS** as the mode of inspection.
5. Configure **Fail Strategy**:
   - Select **Bypass** if you want the traffic flow to continue even when the Intrusion Prevention engine crashes and fails to inspect the traffic. A slight disruption in the traffic occurs when ArubaOS detects an engine failure and takes action based on the fail strategy configuration.
   - Select **Block** if you do not want the traffic to flow until the Intrusion Prevention engine inspects the data packets. If you select this option, your traffic flow is blocked until the Intrusion Prevention engine starts inspecting the traffic.
6. Click the **Policies** tab. The Policies table displays the following details:
   - **Name**—Displays the names of the following policies:
     - **IPS Lenient**—Contains rules that are from the current year and the previous three years for vulnerabilities with a CVSS score of 4 and above.
     - **IPS Moderate**—Contains rules that are from the current year and the previous two years for vulnerabilities with a CVSS score of 6 and above.
     - **IPS Strict**—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 8 and above.
   - **State**—A toggle switch that allows you to enable the policy.

By default **IPS Strict** is enabled. If you want to change the default policy, select the policy that you want to enforce and click **Enable** in the confirmation window. It takes 2 to 5 minutes for the change to take effect. Note that you can enforce only one policy at a time.
For more information on CVSS score, see https://www.first.org/cvss/.

   - **Mode**—Displays the mode of inspection.
   - **Security Strategy**—Defines whether the policy is Lenient, Moderate, or Strict.
   - **Action**—The action to be taken on traffic flow: Drop packets.

Managing Rules in Aruba IDPS Policies

To enforce and apply Allow List rules for a policy, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To configure a Branch Gateway group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
     The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.

- To configure a Branch Gateway, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
  A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
  The dashboard context for the gateway is displayed.

NOTE

The Branch Gateway or the Branch Gateway in the group that you want to configure must support Aruba IDPS.

2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
3. Click the **Config** icon to open the **Gateway IDS/IPS** configuration page.
4. Click the **Policies** tab.
5. Click a policy to view the rules that are handled by the policy. The following details are displayed:
   - **Name**—The name of the policy.
   - **State**—The policy state, **Enabled** or **Disabled**.
   - **Definition**—Defines how the policy handles threats that are identified.

   By default, the rules based on which the policy is enforced are displayed in the **Rules** table. To view the list of allowed rules, click **Allow Listed**.
6. The following details are displayed in the **Rules** table:
   - **Signature**—The threat signature.
   - **SID**—The signature ID.
   - **Category**—The threat category such as malware, phishing.
   - **Protocol**—The network protocol for the rule.
   - **Action**—The action taken to handle the threat.
   - **Direction**—The direction in which traffic flows**.** The traffic that flows towards the branch from the WAN and the traffic that flows from the branch towards the WAN.
7. To move a single rule to **Allow List**, select the row and click at the end of the row. To move multiple rules to **Allow List**, select the rows and click **Move to Allow List**.

NOTE

In the **Rules** table, use the filter icon in the **Signature** column to filter the signatures that you want to move to Allow List.

8. In the **Move to Allow List** confirmation window, click **Move**.
9. To remove a rule from **Allow List**, select the row and click at the end of the row. To remove multiple rules from **Allow List**, select the rows and click **Remove from Allow List**.
10. In the **Remove from Allow List** confirmation window, click **Remove**.

Troubleshooting Aruba IDPS

You can enable the Aruba IDPS engine to capture malicious data packets to analyze the root cause and troubleshoot.

Before you begin

It is assumed that the following requirements are met before you proceed:

1. You have an active gateway subscription with Security license.
2. You must have on-boarded and connected the Branch Gateways to Aruba Central successfully.

To troubleshoot Aruba IDPS complete the following steps:

1. In the **Network Operations** app, complete one of the following steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.

The Branch Gateway or the Branch Gateway in the group that you want to configure must support Aruba IDPS.

2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
3. Click the **Config** icon to open the Gateway IDS/IPS configuration page.
4. In the **General** tab, select the **Enable traffic inspection** check box.
5. Click **Save**.

After traffic inspection is enabled:

- A **Refresh extended packet capture** dialog pops up with a refresh button to extend large packet capture for another 10 minutes. By default, the traffic inspection configuration is disabled after being active for 10 minutes. If you wish to extend the configuration, click the **Refresh extended packet capture** refresh button.
- The Aruba 9004 Branch Gateway starts sending threat data to Aruba Central. By default, only 256 bytes of data are sent; however, if you enable traffic inspection, up to 4096 bytes of data in the packet are sent to Aruba Central.

Configuring SIEM

Aruba IDPS provides the option to send the threat event data to a third-party Security Incident and Event Management (SIEM) server such as Splunk, which allows you to perform advanced analysis and generate reports. SIEM provides a holistic picture of the security posture of your organization by aggregating and correlating data from disparate sources in the network.

NOTE

SIEM configuration is available only in the **All Devices** context. If configured, threat data from all 9004 Branch Gateways connected to Aruba Central are sent to the SIEM server.

Before you begin

Ensure that the following requirements are met before you configure SIEM server:

1. You have an active subscription with a third-party SIEM provider such as Splunk.
2. You have the server URL, an index, and authentication token handy to enter the details while configuring SIEM

NOTE

To know how to configure Splunk and get the required details to configure SIEM, see the section *Set up and use HTTP Event Collector* in Splunk Cloud Documentation.

Enabling an SIEM Server

To enable an SIEM server for IDPS, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for all devices is displayed.
2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
3. Click the **Config** icon to open the **Gateway IDS/IPS** configuration page.
4. Click the **SIEM** tab.
5. Select the **Enable reporting of threats to SIEM systems** check box.
6. Click **Save**.

NOTE

Note that you must add an SIEM server to report threats.

Adding an SIEM Server

To add an SIEM for IDPS, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for all devices is displayed.
2. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
3. Click the **Config** icon to open the **Gateway IDS/IPS** configuration page.
4. Click the **SIEM** tab.
5. Click **+** in the Servers table.
6. In the **Add SIEM Server** window, enter the following details:
   - **Name**—The name for the server.
   - **URL**—The SIEM server URL.
   - **Index**—The index from the third-party SIEM provider to contain the threat data.
   - **Token**—The authentication token from the third-party SIEM provider to connect to the server.
7. Click **Test Connection** to verify if the connection to the SIEM server is working.
8. Click **Add**.

NOTE

For the threat data to be reported to this server, ensure that you have enabled reporting to SIEM server.

Editing an SIEM Server

To edit an existing SIEM server, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for all devices is displayed.
2. Under **Manage**, click **Security > Gateway IDS/IPS**.
3. Click the **Config** icon to open the **Gateway IDS/IPS** configuration page.
4. Click the **SIEM** tab.
5. In the servers table, hover over the row that you want to edit.
6. Click the edit icon.
7. Make the required changes and click **Save**.

Deleting an SIEM Server

To delete an existing SIEM server, complete the following steps:

1. In the **Network Operations** apps, set the filter to **Global**.
   The dashboard context for all devices is displayed.
2. Under **Manage**, click **Security > Gateway IDS/IPS**.
3. Click the **Config** icon to open the **Gateway IDS/IPS** configuration page.
4. Click the **SIEM** tab.
5. In the servers table, hover over the row that you want to delete.
6. Click the delete icon.
7. Click **Delete** in the confirmation window.

Configuring Aruba IDPS Alerts

It is important to understand how alerts are aggregated and triggered, the conditions for closing an alert, determining severity, and so on, to troubleshoot issues based on these alerts. This topic explains how alerts are aggregated and the different scenarios when these alerts are triggered.

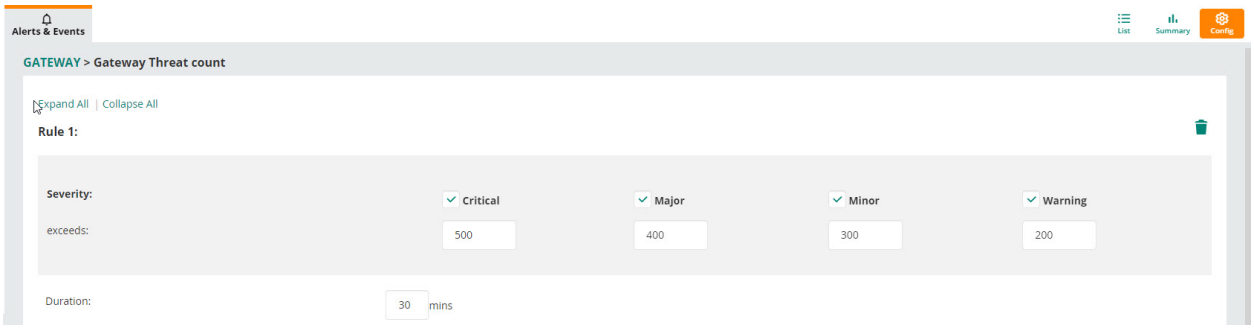
Alert Aggregation

Gateway Threat Count

Aggregation determines how alerts are collected based on the duration, customer, or the device. For example, the Gateway Threat Count alert is aggregated at the gateway level for the duration set in the alert configuration page.

The following is a screen shot of a sample configuration:

Figure 258 *An Example for Gateway Threat Count Alert Configuration*



If you have configured the alert at 5:00 PM for a duration of 30 minutes, the dataset used to run this service is until the configured 5:00 PM, that is 4:30 to 5:00 PM. The dataset used to run this service will be from last 30 minutes form the present time. Considering the present time is 5:05 PM, the dataset used will be from 4:35 PM to 5:05 PM.

The aggregation of alerts happens at the Gateway level. An alert is triggered for every Gateway based on the total number of IDPS events for each gateway.

For example, if you have five gateways with IDPS enabled in your Aruba Central account, and the total number of IDPS events is 250 for two gateways, then, as per the configuration in Figure 258, two alerts are triggered with Alert Severity as **Warning**. The alert is triggered because the events count 250 has exceeded the severity threshold for **Warning**. If the number of events for the other three gateways is 530, then three alerts are triggered with alert severity as **Critical**.

If the number of events for the other three gateway crosses 250, a **Warning** alert will be raised. If the IDPS event count crosses 500 for any of the three gateways, the alert severity of the raised alert changes from **Warning** to **Critical**.

Gateway Threat count per signature

For this alert, the aggregation happens for every customer. If you have configured five IDPS gateways in your Aruba Central account and each of them have 50 IDPS events count for one signature, then only one alert is triggered. The alert severity is **Warning** because the total number of IDPS events sums up to 250 (which exceeds the events count configured for **Warning** in the example). Therefore, this alert does not take into account the individual gateways, but the alerts are aggregated based on the events pertaining to each signature.

Alerts Acknowledgment

- **Automatic acknowledgment**

  Alerts are acknowledged automatically when the event count drops below the lowest severity threshold configured for the alert. For example, if the lowest severity value is 200 for **Warning**, then the alert is acknowledged automatically when the event count falls below 200 in the last 30 minutes.

- **Manual acknowledgment**

  Users with admin access can acknowledge alerts irrespective of the severity configuration. As manually acknowledging an alert does not reset the count data, the alert service continues to aggregate events. When the number of new events meets the configured threshold, an alert is triggered again. The alert service will use the previous data along with new data x1(if any) for aggregation, and when the aggregated count meets the configured threshold, an alert will be raised again.

Alert Severity and Transition

Alert severity falls under one of the following categories:

- Critical
- Major
- Minor
- Warning

The alert severity changes based on the severity threshold set up for each category and the events count in the last span of time interval.

The severity configured for the alerts is different from the **Threat Lists** and **Threat Details** pages in the **Security** > **Gateway IDS/IPS** tab. The Severity value displayed in the **Gateway IDS/IPS** tab is specific to the threat signature.

Troubleshooting Branch Gateway for Aruba IDPS

If you come across any of the following scenarios, you can collect logs to debug the gateway from Aruba Central:

- When the **Traffic Inspection Engine Status** is **Crashed** in the Gateways > Overview > IDPS.
- When the **Traffic Inspection Engine Status** is not **Running** despite enabling traffic inspection.
- When the gateway is not updating to a ruleset selected in the **Gateway IDS/IPS** > **General** page.
- While debugging other errors such as incorrect packet drops and so on.

1. In the **Network Operations** app, complete either of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **System** > **Logging**.
4. Expand the **Logging Levels** drop-down and click **+** in the **Logging levels** table.
5. Select **System** in the **Category** drop-down list.
6. Do not select any sub category.

7. Select one of the following in the **Process** drop-down list and repeat steps 4 to 8 to add logging levels.
   - **idps_mgr**
   - **vnf_mgr**
   - **flbwrap**
8. Select **Informational** in the **Logging Level** drop-down list.

After troubleshooting Aruba IDPS, ensure to delete the three **Logging Levels** that you added. To delete an entry, select the row and click the delete icon.

Troubleshooting Packet Drops

There might be instances when an IDPS engine incorrectly identifies legitimate traffic as malicious activity and drops packets. The following sections provide procedures to troubleshoot scenarios when legitimate data packets are dropped.

Packets Dropped for Legitimate Traffic and Generated Alerts

This section provides the procedure to troubleshoot when the Aruba IDPS traffic inspection engine drops data packets for legitimate traffic and generates alerts. For example, you try to access your email account in a web browser and you notice that the page does not load as expected and an alert is generated for the threat event type. This could be because some data packets are dropped by the traffic inspection engine.

To troubleshoot this scenario, complete the following steps:

1. Aruba IDPS allows you to move a threat signature to the **Allow List** in the following ways to allow the blocked traffic to flow:
   - To move a threat signature to **Allow List** from the **Threats List** page, complete the following steps:
     a. In the **Network Operations** app, complete one of the following steps:
        - To configure a Branch Gateway group, complete the following steps:
          i. Set the filter to a group containing at least one Branch Gateway that supports Aruba IDPS.
          The dashboard context for a group is displayed.
          ii. Click **Gateways**.
          iii. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
        - To configure a Branch Gateway, complete the following steps:
          i. Set the filter to **Global** or a group containing at least one Branch Gateway that supports Aruba IDPS.
          ii. Under **Manage**, click **Devices** > **Gateways**.
          A list of gateways is displayed in the List view.
          iii. Click a gateway under **Device Name**.
          The dashboard context for the gateway is displayed.

     b. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
     c. Click the list icon to view the **Threats List** table.

d. Select a threat and click **Move threat to Allow List** icon. The **Move to Allow List** window is displayed.
e. Click **Move** in the **Move to Allow List** window to move the threat to **Allow List**.

- To move a threat signature to **Allow List** from the **Policy** page, complete the following steps:
  a. In the **Network Operations** app, complete one of the following steps:
     - To configure a Branch Gateway group, complete the following steps:
       i. Set the filter to a group containing at least one Branch Gateway that supports Aruba IDPS.
       The dashboard context for a group is displayed.
       ii. Click **Gateways**.
       iii. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
     - To configure a Branch Gateway, complete the following steps:
       i. Set the filter to **Global** or a group containing at least one Branch Gateway that supports Aruba IDPS.
       ii. Under **Manage**, click **Devices** > **Gateways**.
       A list of gateways is displayed in the List view.
       iii. Click a gateway under **Device Name**.
       The dashboard context for the gateway is displayed.
  b. Under **Manage**, click **Security** > **Gateway IDS/IPS**.
  c. Click the **Config** icon to view the **Gateway IDS/IPS** configuration page.
  d. Click the **Policies** tab, and select a policy to view the policy details.
  e. In the **Rules** table, select a row and click the **Move to Allow List** icon.

NOTE

To move multiple rules to Allow List, select the rows and click **Move to Allow List.**

In the **Rules** table, use the filter icon in the **Signature** column to filter the signatures that you want to move to **Allow List**.

  f. Click **Move** in the **Move to Allow List** window.

NOTE

The **Allow Listed** rules might take up to 10 minutes to take effect after the traffic flow stops.

2. After moving the threat signatures to **Allow List**, contact Aruba Technical Support for further assistance.

Packets Dropped for Legitimate Traffic without Generating Alerts

This section provides the procedure to troubleshoot when the Aruba IDPS traffic inspection engine drops data packets for legitimate traffic and does not generate alerts.

To troubleshoot this scenario, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway that supports Aruba IDPS.
   The dashboard context for a group is displayed.

2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Overview**. The Gateway Details page is displayed.
5. From the **Actions** drop-down list, click **Open Remote Console**. It opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.
6. Execute the following commands to enable blocked flow log and pcap log:

```
(A9004) *#idps debug blocked-flow
```

```
(A9004) *#idps debug pcap-log
```

The debugging commands reloads the Aruba IDPS engine which results in a momentary network disruption. Therefore, it is recommended to plan this activity in advance during planned maintenance.

7. Execute the `show idps debug status` command to ensure that the required Aruba IDPS debug options are enabled. Wait until the **Blocked-Flow** status changes to **Active**. Reproduce the issue to capture the corresponding logs.
8. Execute the following commands to disable blocked flow log and pcap log:

```
(A9004) *#no idps debug blocked-flow
```

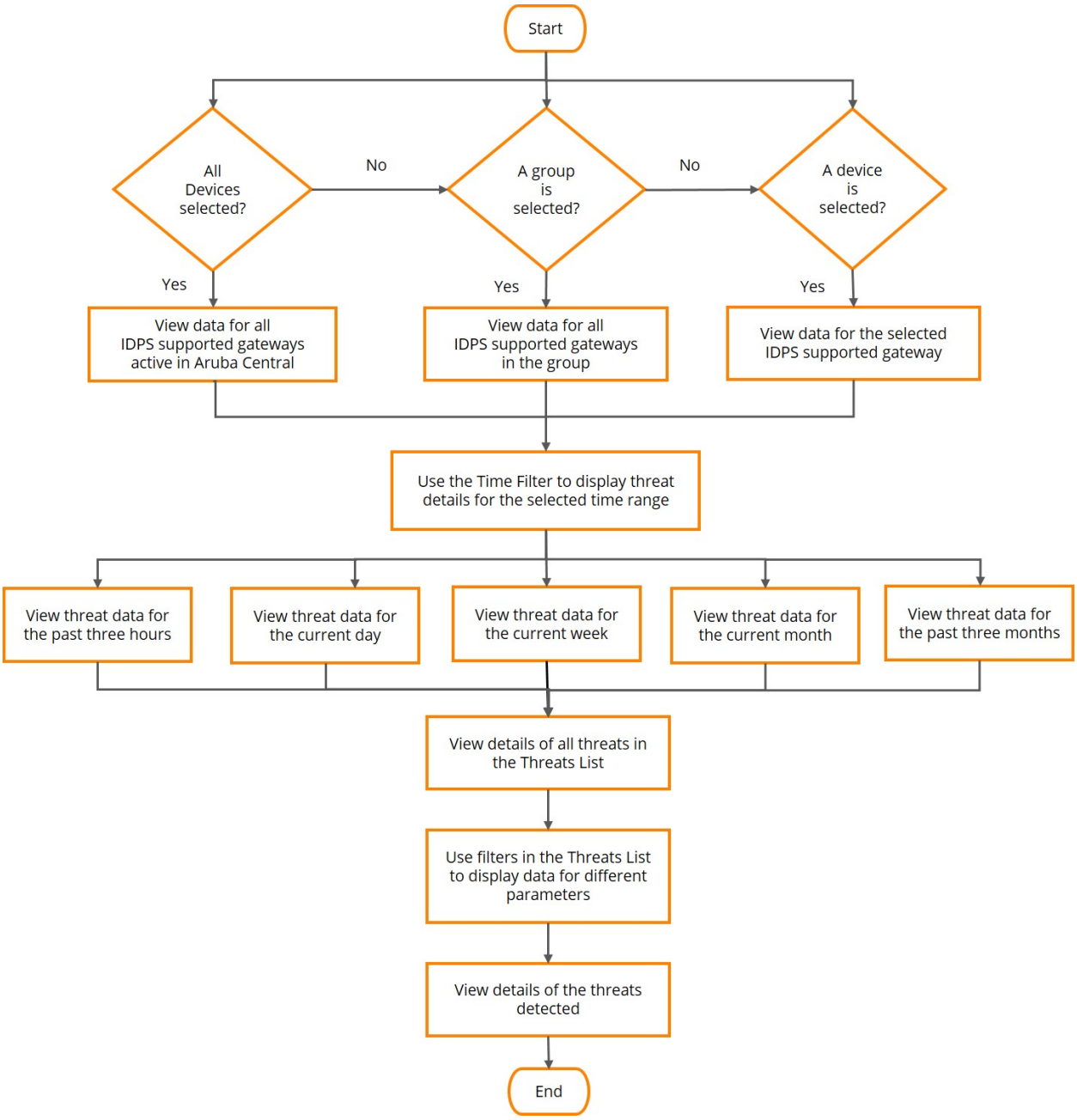
```
(A9004) *#no idps debug pcap-log
```

9. Execute the `show idps debug status` command to ensure that the Aruba IDPS debug options are disabled.
10. Execute the `tar logs idps-logs` command to collect the Aruba IDPS traffic inspection engine logs.
11. Copy the **idps-logs.tar.7z** file from the gateway and share it with Aruba Technical Support.

Monitoring Aruba IDPS

The **IDPS** dashboard provides all metrics about the threats information associated with the IDPS supported gateways connected to Aruba Central. The **IDPS** dashboard displays the threats detected by the traffic inspection engine in charts for different parameters.

The following flowchart shows how the threat data can be filtered and viewed.



Data Filters

The different data filters allow you to monitor and customize the threat data displayed on the charts.

Filter

The filter allows you to select a group or a IDPS supported gateway for performing specific configuration and monitoring tasks. If you do not select a group or a device, then the charts display data for all the IDPS supported gateways provisioned and managed through Aruba Central.

When you select a group from the filter, the IDPS dashboard displays threat data specific to the IDPS supported gateways within the group. When you select an individual IDPS supported gateway from the filter, the IDPS dashboard displays data specific to the hosts associated with the gateway.

Time Filter

The time filter allows you to set a time range to display threat details in the charts and threats list. You can set the filter to any of the following time ranges:

- **3 Hours**—The charts display the threat details for the past three hours.
- **1 Day**—The chart displays the threat details for the current day.
- **1 Week**—The chart displays the threat details for the current week.
- **1 Month**—The chart displays the threat details for the current month.
- **3 Months**—The chart displays the threat details for the past three months.

Threats List Filters

The filters in the Threats List table allows you to filter data in the columns. The and icons allow you to sort the columns in the ascending and descending order.

Threats List

The Threats List provides details of the threats detected by the traffic inspection engine.

Viewing the Threats List Page

To view the **Threats List** table, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites** that has IDPS supported gateways. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, select **Security > Gateway IDS/IPS**.
3. Click the **List** icon to view the **Threats List** table.

The **Threats List** table provides the following information:

- **Occurred On**—The timestamp of the threat detected.
- **Gateway**—Name of the gateway in which the threat was detected.
- **Type**—The type of protocol in which the threat is identified.
- **Source**—The IP address of the sending host.
- **Destination**—The IP address of the receiving host.
- **Severity**—The severity of the threat.
- **Action**—The action taken on the detected threat.
- **Description**—The signature description of the threat detected.

NOTE

Click the icon and select the columns that you want to display in the table. To reset the columns, click the icon and select **Reset to default**.
In the **Threats List** table, use the filter and the sort icons to filter and sort the threats data respectively.
To set the charts to show data for specific duration, use the options in the time range filter. By default, the data is displayed for a duration of 3 hours. To view the graphs for different durations, click the time filter icon and select a time range of your choice.
You can view the data for a group of 9004 gateways or an individual gateway device using the filter. To view data collectively for all 9004 gateways, select **All Devices** from the filter

Viewing the Threat Details

To view the details of a threat, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites** that has IDPS supported gateways. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, select **Security > Gateway IDS/IPS**.
3. Click the **List** icon to view the **Threats List** table.
4. Select a threat and click the **View Packet info** icon to view the details of the threat.

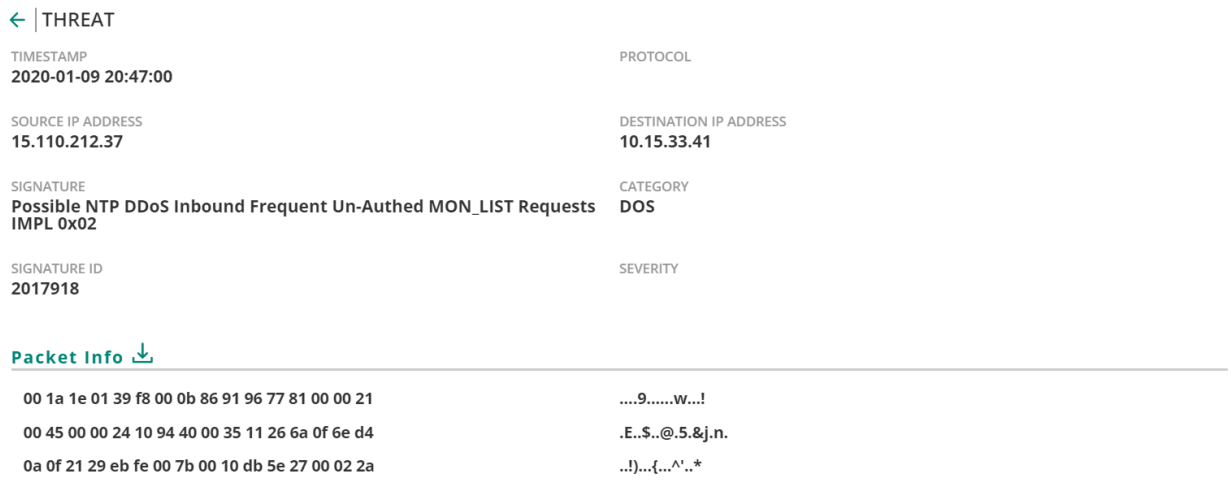
The **Threat** details page provides the following information:

- **Timestamp**—The timestamp of the threat detected.
- **Protocol**—The type of protocol in which the threat is identified.
- **Source IP address**—The IP address of the sending host.
- **Destination IP address**—The IP address of the receiving host.
- **Signature**—The signature description of the detected threat.
- **Category**—The alert type under which the threat is categorized.
- **Signature ID**—The signature ID associated with the signature.
- **Severity**—The severity of the threat.

NOTE

Click the icon to download the packet info to your local setup for troubleshooting.

Figure 259 *Threat Details*



Moving a Threat to the Allow List

A user can move a rule from the enforced ruleset list to the Allow List to allow the rule which identified the threat. You can also move threats to the allowed list in the policies. For more information, see Managing Rules in Aruba IDPS Policies

To move a threat to the **Allowed List**, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites** that has IDPS supported gateways. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, select **Security > Gateway IDS/IPS**.
3. Click the **List** icon to view the **Threats List** table.
4. Select a threat and click the **Move threat to Allow List** icon. The **Move to Allow List** window is displayed.
5. Click **Move** in the **Move to Allow List** pop-up window to move the threat to Allow List.

Gateway IDS/IPS Dashboard

The Gateway IDS/IPS dashboard displays the threat details associated with the gateways with IDPS license and the hosts connected to the gateways. The Gateway IDS/IPS dashboard displays the threats detected by the traffic inspection engine in different charts and tables.

Viewing Threat Details in the Gateway IDS/IPS Dashboard

To view the Gateway IDS/IPS dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites** that has IDPS supported gateways. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, select **Security > Gateway IDS/IPS**.
3. Click the **Summary** icon for a graphical view of the threats identified.

To set the charts to show data for specific duration, use the options in the time range filter. By default, the data is displayed for a duration of 3 hours. To view the graphs for different durations, click the time filter icon and select a time range of your choice.

The **Gateway IDS/IPS** dashboard displays the following charts and tables.

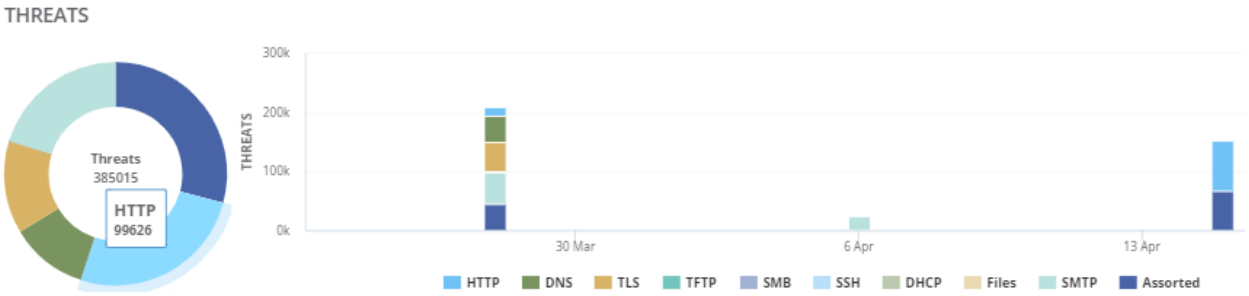
Threats Charts

The **Threats** charts display the number of threats detected by the traffic inspection engine for a selected duration, grouped by the type of protocol. This can be useful to identify the highest number of intrusions in the network traffic.

- **Threats pie chart**—The center of the chart displays the grand total number of threats detected for a selected duration. When you hover over the different regions on the chart, each region displays the total number of threats specific to the type of protocol for which the threat was detected. Click a region on the chart to view the threats for the particular type of protocol for the selected duration in the **Threats List**.
- **Threats bar chart**—The stacked vertical bars display the number of threats detected in a protocol for a selected duration. When you hover over a stacked vertical bar, it displays the timestamp and the number of threats for each type of protocol. Click a region on the stacked vertical bar to view threats for the particular type of protocol for the selected duration in the **Threats List**.
  - A legend is displayed for each type of protocol below the Threats bar chart. When you click a legend, the stacked vertical bar chart hides or shows the data for the selected type of protocol. By default, the stacked vertical bar displays the number of threats detected for all the protocols for a selected duration. For example, when you click **HTTP**, the stacked vertical bar chart hides or shows the number of threats detected for the **HTTP** protocol.

- The time filter allows you to set a time range to display threat details in the charts. You can set the filter to any of the following time ranges:
  - **3 Hours**—The bar chart is plotted on an hourly basis to display the threat details for the past three hours.
  - **1 Day**—The bar chart is plotted on an hourly basis to display the threat details for the current day.
  - **1 Week**—The bar chart is plotted on a daily basis to display the threat details for the current week.
  - **1 Month**—The bar chart is plotted on a daily basis to display the threat details for the current month.
  - **3 Months**—The bar chart is plotted on a weekly basis to display the threat details for the past three months.

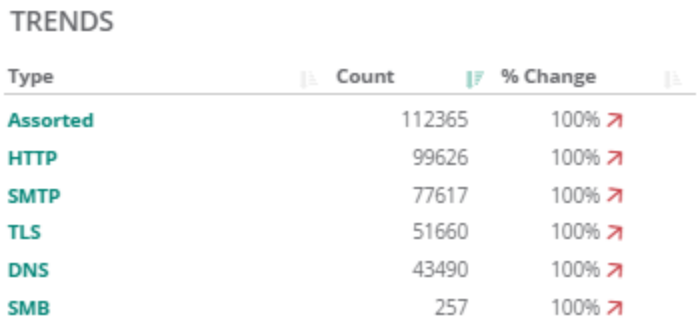
Figure 260 *Threats Pie and Bar Chart*



Trends Table

The **Trends** table displays the threat type, number of threats, and the percentage of change in the number of threats of each type in comparison to the previous duration. This is useful to indicate a sudden change in the number of threats of a certain type from the previous duration to help identify a threat pattern. Click a threat type to view threats for the particular type in the **Threats List**.

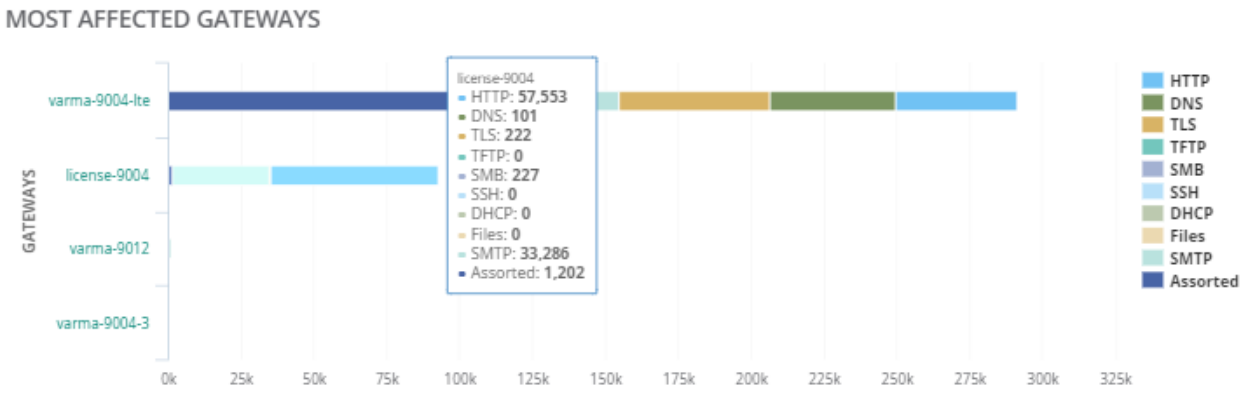
Figure 261 *Trends Table*



Most Affected Gateways or Hosts Chart

When you select **All Devices** in the filter, the chart displays the top 10 gateways with the number of threats detected in a stacked horizontal bar chart. When you hover over a horizontal stacked bar, it displays the number of threats for each type of protocol. Click a stacked horizontal bar to view threats for the particular type of protocol in the **Threats List** table. Click the legend for the threat type to show or hide the data for the threat type on the chart.

Figure 262 *Most Affected Gateways Chart*

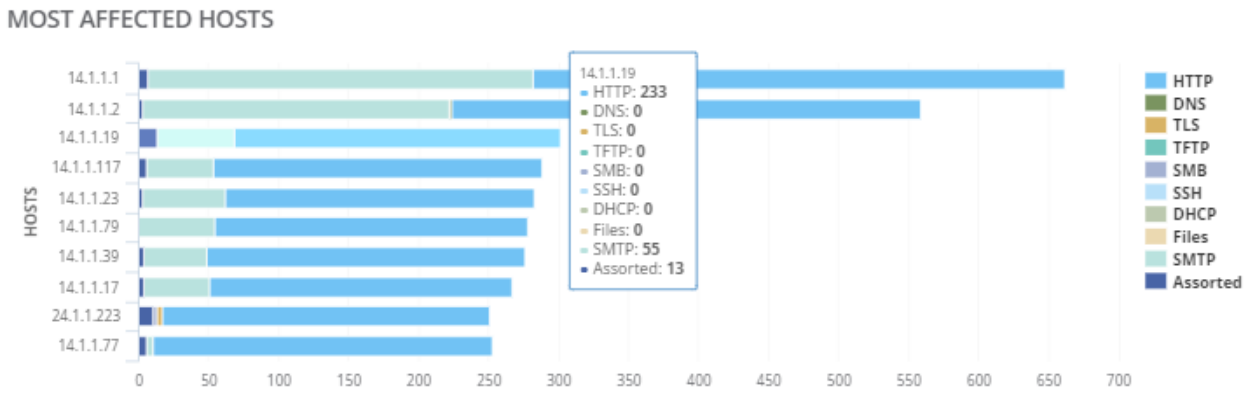


NOTE

When you select a group or an IDPS supported gateway in the filter, the **Most Affected Gateways** chart is replaced by the **Most Affected Hosts** chart.

When you select a group in the filter, the chart displays the number of threats detected for the top 10 hosts connected to all IDPS supported gateways within a group. When you select an IDPS supported gateway in the filter, the chart displays the number of threats detected for the top 10 hosts associated with the gateway.

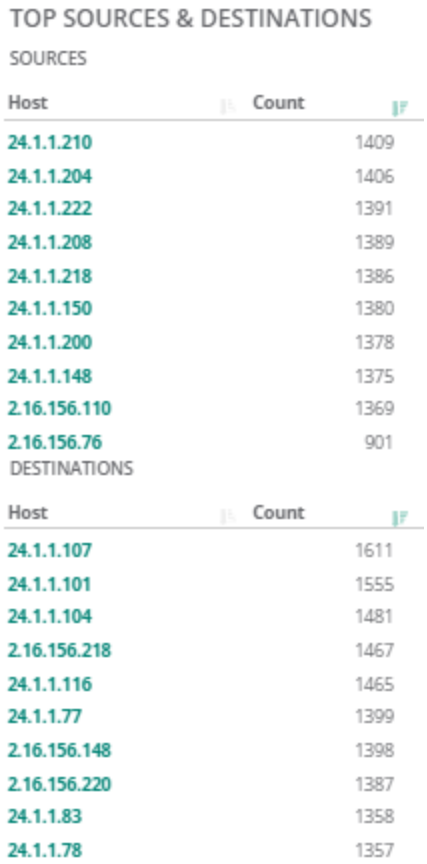
Figure 263 *Most Affected Hosts Chart*



Top Sources & Destinations Table

The **Top Sources & Destinations** table displays the top ten IP addresses of the source and destination hosts with the number of threats identified. Click an IP address under **Sources** to view threats in the **Threats List** table for the selected source IP address. Click an IP address under **Destinations** to view threats in the **Threats List** table for the selected destination IP address.

Figure 264 *Top Sources & Destinations Table*


TOP SOURCES & DESTINATIONS

SOURCES

Host	Count
24.1.1.210	1409
24.1.1.204	1406
24.1.1.222	1391
24.1.1.208	1389
24.1.1.218	1386
24.1.1.150	1380
24.1.1.200	1378
24.1.1.148	1375
2.16.156.110	1369
2.16.156.76	901

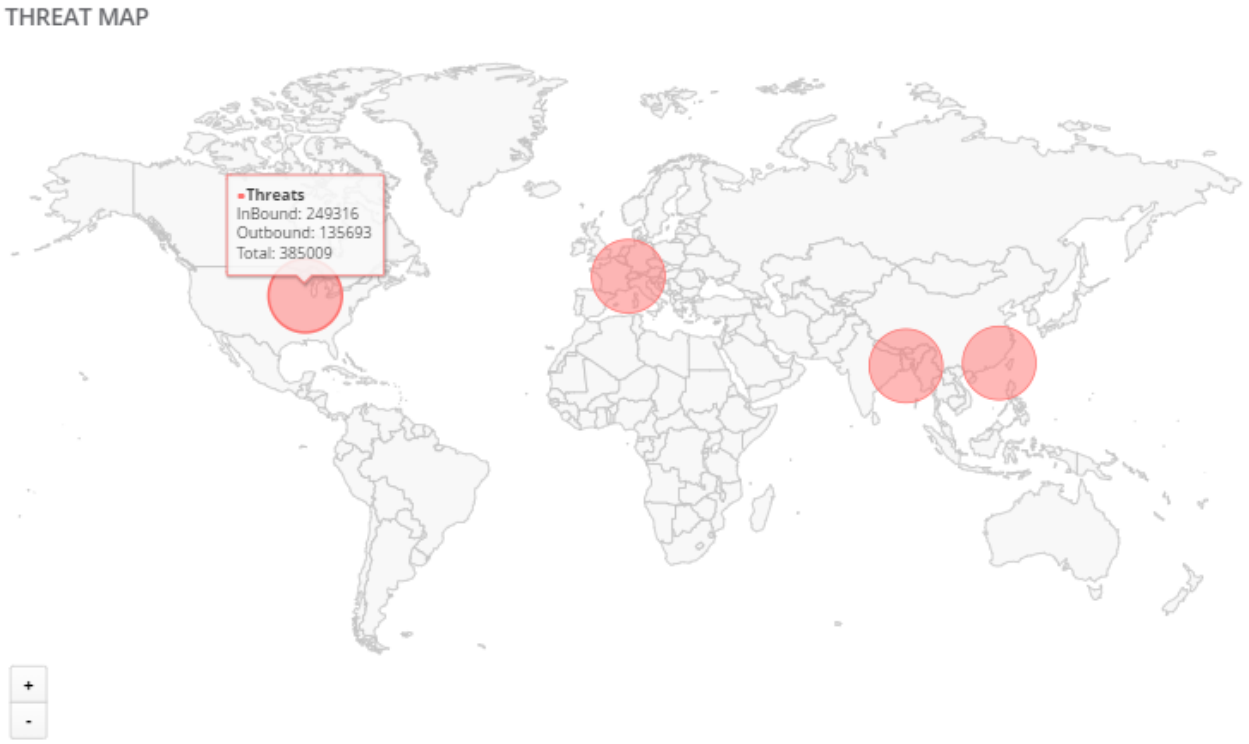
DESTINATIONS

Host	Count
24.1.1.107	1611
24.1.1.101	1555
24.1.1.104	1481
2.16.156.218	1467
24.1.1.116	1465
24.1.1.77	1399
2.16.156.148	1398
2.16.156.220	1387
24.1.1.83	1358
24.1.1.78	1357

Threat Map

The **Threat Map** displays the locations of the hosts, in which threats are detected. Hover over a location to view the number of inbound, outbound, and the total number of threats detected. Inbound displays the number of threats in the incoming traffic at a specific location. Outbound displays the number of threats in the outgoing traffic at a specific location. You can zoom in, zoom out, and move the map to view the threat details for a specific location. Click a location to view threats in the **Threats List** table.

Figure 265 *Threat Map*



Threat Categories

This section lists the various threat categories and their descriptions in a table. This information helps you to understand and troubleshoot issues while monitoring and analyzing threats in your **Gateway IDS/IPS** dashboard.

Table 284: *Threat Categories*

Category	Description
Activex	Rules that detect attacks and vulnerabilities related to ActiveX.
Adware-PUP	Rules that are not explicitly malware, but might indicate software that is used for Ad tracking or other types of spyware related activity.
Attack Response	Responses that could indicate an intrusion. These rules are designed to detect the results of a successful attack. For example, error messages that indicate an intrusion.
Botcc (Bot Command and Control)	Rules autogenerated from several sources of known and confirmed active Botnet and other Command and Control hosts. The primary data source is shadowserver.org.
Botcc Portgrouped	Botcc rules that are grouped by destination port. Rules grouped by ports offer higher fidelity.
Chat	Rules to detect traffic related to numerous chat clients, Internet Relay Chat (IRC), and possible check-in activity.
CIArmy	IP rules generated by Collective Intelligence to block traffic.

Category	Description
Coinmining	Rules to detect activities related to coinmining such as coinmining for Bitcoin. Rules in this category mostly detect malware that perform coinmining.
Compromised	Rules to identify threats from a list of known compromised hosts that are confirmed and updated daily. This is a compilation of several private, but highly reliable data sources.
Current Events	Rules for active and short lived campaigns. This category covers exploit kits and malware that will be aged and removed quickly due to the short lived nature of the threat. These are rules that we don't intend to keep in the ruleset for long, or that need to be tested before they are considered for inclusion. For example, these rules contain simple signatures for Storm binary URL of the day signatures to detect CLSIDs of newly found vulnerable apps.
Decoder events	Rules to log normalization events related to decoding.
Deleted	Rules removed from the ruleset.
DNS	Rules to detect attacks and vulnerabilities related to DNS. This category includes abuse of the service for things such as tunneling.
DOS	Rules to detect Denial of Service (DOS) attempts, intended to detect inbound DOS activities, and outbound indications.
Drop	Rules to block spamhaus DROP (Don't Route or Peer) listed networks. This list is updated daily. For more information, see http://www.spamhaus.org.
Dshield	IP-based rules for Dshield Identified attackers. This list is updated on a daily basis. For more information, see http://www.dshield.org.
Exploit	Rules to detect direct exploits that are not covered in specific service category. For example, Windows exploit and Veritas are categorized as Exploit. While intrusions such as SQL injection are categorized as Exploits, they have their own category.
Exploit-Kit	Exploit Kit rules are used specifically to detect activity related to Exploit Kits, their infrastructure, and delivery.
FTP	Rules for attacks, exploits, and vulnerabilities related to FTP. This category includes basic non-malicious FTP activities such as login for logging purposes.
Games	Rules for identifying gaming traffic and attacks against those games.
HTTP Events	Rules to log HTTP protocol specific events.
Hunting	Rules that may match legitimate traffic or require intensive matching, but is useful for threat hunting because they provide indicators which are useful when matched with other rules.
ICMP	Rules for attacks and vulnerabilities related to ICMP. This category includes rules that detect basic activities of the protocol for logging purposes.
ICMP Info	Rules to log ICMP protocol specific events.
IMAP	Rules to identify attacks and vulnerabilities related to IMAP protocol. This category includes rules to detect basic activities of the protocol for logging purposes.
Inappropriate	Rules to identify pornography related activities.

Category	Description
JA3	Rules that support the mechanism to fingerprint malicious SSL certificates based on parameters that are in the SSL handshake negotiation by both clients JA3 and Servers JA3S. These signatures have a higher propensity for False Positives but are great for Threat Hunting or Malware Detonation Environments.
Malware	Rules for malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating, and anything that can be detected on the wire.
Mobile Malware	Rules specific to mobile platforms. This includes rules for malware and spyware related activities.
Netbios	Rules to identify attacks, exploits, and vulnerabilities related to Netbios. This category includes rules that detect basic activities of the protocol for logging purposes.
P2P	Rules to identify peer to-peer traffic and attacks. These are not labeled as malicious, but might not be appropriate for all networks and environments.
Phishing	Rules that detect Credential Phishing activity including landing pages exhibiting credential phishing as well as successful submission of credentials into credential phishing sites.
Policy	Rules for applications like DropBox and Google Apps. This category covers off port protocols, basic DLP such as credit card numbers and social security numbers. Rules to block applications that are not allowed based on organizational policy.
POP3	Rules to identify, attacks, and vulnerabilities related to the POP3 protocol. This category includes rules to detect basic activities of the protocol for logging purposes.
RPC	Rules to detect attacks, vulnerabilities, and protocol related to RPC. This category includes rules to detect basic activities of the protocol for logging purposes.
SCADA	Rules for SCADA attacks, exploits, and vulnerabilities, and protocol detection.
SCADA_special	Rules for SCADA preprocessor based on Snort Digital Bond.
SCAN	Rules to detect reconnaissance and probing.
Shellcode	Rules for Remote Shellcode detection. Remote shellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. Remote shellcodes normally use standard TCP/IP socket connections to allow the attacker access to the shell on the target machine. Such shellcodes can be categorized based on how the connection is set up. If the shellcode can establish the connection, it is called a "reverse shell" or a connect-back shellcode because the shellcode connects back to the attacker's machine.
SMTP	Rules for attacks, exploits, and vulnerabilities related to SMTP. This category includes rules to detect basic activities of the protocol for logging purposes.
SMTP events	Rules that log SMTP operations.
SNMP	Attacks, exploits, and vulnerabilities related to SNMP. This category includes rules to detect basic activities of the protocol for logging purposes.
SQL	Attacks, exploits, and vulnerabilities related to SQL. This category includes rules to detect basic activities of the protocol for logging purposes.

Category	Description
Stream events	Rules to identify intrusions through TCP stream engine events.
TELNET	Rules that detect attacks and vulnerabilities related to the TELNET service. This category includes rules to detect basic activities of the protocol for logging purposes.
TFTP	Rules that detect attacks and vulnerabilities related to the TFTP service. This category includes rules to detect basic activities of the protocol for logging purposes.
TLS events	Rules for identifying LS events and anomalies.
TOR	IP-based rules to identify traffic to and from Tor exit nodes.
Trojan	Malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating, and anything that can be detected on the wire.
User Agents	User agent identification and detection.
VOIP	Rules that detect attacks and vulnerabilities related to VOIP environment. For example, intrusion using protocols such as SIP and RTP.
Web Client	Web-client-side attacks and vulnerabilities.
Web Server	Rules that detect attacks and vulnerabilities against web servers.
Web Specific Apps	Rules for specific web applications.
WORM	Traffic indicative of network-based worm activity.

Chapter 18
Integration with AWS Public Cloud through Cloud Connect Service

The SD-Branch integration with a cloud infrastructure hosted on AWS through Cloud Connect service allows you to set up a secure connection between the Aruba Branch Gateways and AWS Transit Gateway Network Manager. This integration simplifies deploying large-scale, secure and optimized branch connectivity across the global AWS network.

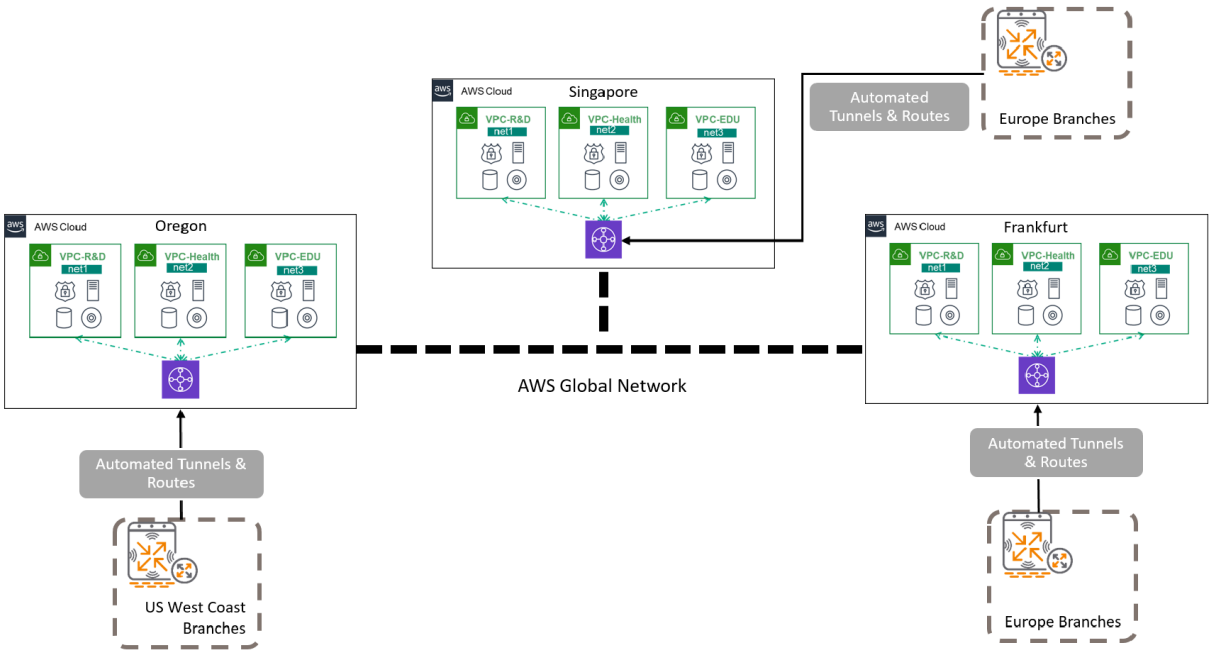
Using the Cloud Connect service, the Aruba Branch Gateways establish a secure connectivity with AWS Transit Gateways acting as headends. Cloud Connect service uses SD-Branch Orchestrator as the transport medium to send configurations to Branch Gateways. Branch Gateways connect to AWS Transit Gateways through the automatically orchestrated IPsec tunnels and automated route exchange to optimize routing between branch offices and AWS Transit Gateways in any region.

Once the tunnels are up, eBGP sessions are established to exchange prefixes between the AWS Transit Gateways and Aruba SD-Branch, and allow dynamic exchange of routes. The reverse-pinning technology is used to ensure that the traffic is sent back through the same tunnel from which the traffic originated.

For more information about the supported scenarios, see *Aruba SD-WAN Integration with AWS Public Cloud Tech Note*.

The following figure illustrates the SD-Branch integration with the AWS VPC:

Figure 266 *Cloud Connect and SD-Branch Integration with AWS Public Cloud through Cloud Connect*



To integrate SD-Branch with AWS public cloud through Cloud Connect service, complete the following steps:

1. Generate API token in AWS Console
2. Configure Aruba Branch Gateway in Aruba Central
3. Onboard AWS accounts into Aruba Central through Cloud Connect service

4. Orchestrate tunnel to the AWS VPC through Cloud Connect
5. Verify tunnel status

Additional References

For more information about adding AWS account in central, AWS specific configurations related to VPCs and TGWs, refer to the *Aruba SD-WAN Integration with AWS Public Cloud Tech Note*.

Generating API Token in AWS Console

To generate API token, complete the following steps:

1. Login to the AWS Console.
2. Navigate to **Services** > **IAM** > **Roles**.
3. Click **Create Role**.
4. Click **Add Another AWS Account** and provide the **Account ID** and **External ID** noted while onboarding the AWS account in Aruba Central. For more information, see Onboarding AWS Account in Aruba Central.
5. Click **Next: Permissions**.
6. In the Attach permissions policies window, enable the checkboxes against **AmazonEC2FullAccess** and **AWSNetworkManagerFullAccess**.
7. Click **Next: Tags**.
8. Click **Next**.
9. Provide a **Role Name** for the AWS role.
10. Click **Create Role**.
11. Note the **Role ARN** from the **Summary** page.
12. Add network manager policy **AWSNetworkManagerFullAccess** to the IAM role.

Configuring Aruba Branch Gateway in Aruba Central

Before you onboard an AWS account in Aruba Central, ensure that the following prerequisites are met:

1. Configure uplinks for the ArubaBranch Gateway or VPNC. For more information, see Configuring Uplinks. In every device of the connected group, for each uplink, two IPsec tunnels are formed to have high availability.

The site name should not include the underscore (_) special character.

The uplink name should not include the special characters hyphen (-) and underscore (_).

1. Configure uplinks for the Aruba Branch Gateway or VPNC. For more information, see Configuring Uplinks. In every device of the connected group, for each uplink, two IPsec tunnels are formed to have high availability.
2. Enable tunnel orchestration to establish tunnels between Aruba Branch Gateways and AWS Transit Gateway Network Manager service. For more information, see SD-WAN Overlay Tunnel and Route Orchestration .

3. Enable BGP and configure a valid Autonomous System (AS) number at device level. BGP can be enabled at group level but ensure that the AS number is unique per site. For more information, see Enabling BGP.

For more information about supported and not supported AS numbers, see AWS Documentation.

4. Enable BGP multipath at device level or group level. It is recommended to enable BGP multipath globally. For more information, see Configuring Multipath Selection.
5. To advertise branch subnets with AWS, redistribute connected, static, or OSPF routes to BGP.

Cloud connect service creates route-maps `auto_cloud_connect_in` and `auto_cloud_connect_out`. These route-maps are editable and have a default permit rule with sequence number 20.

It is recommended to edit these route-maps to filter the routes exchanged with the AWS Transit Gateway.

Onboarding AWS Account in Aruba Central

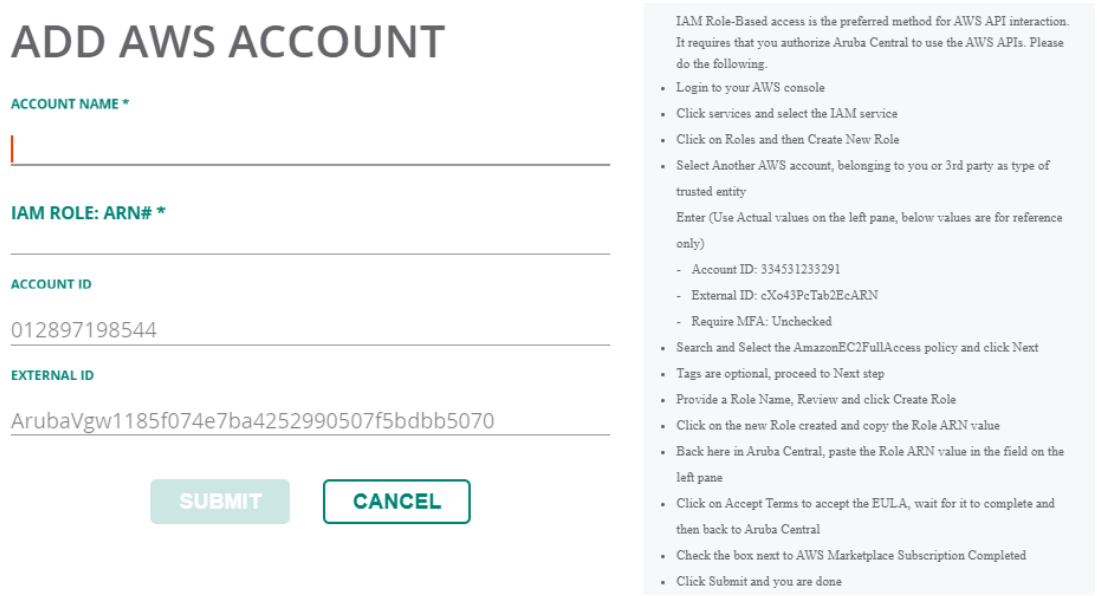
To onboard an AWS account, complete the following steps:

1. Log in to Aruba Central.
2. In the **Network Operations** app, set the filter to **Global**.
3. Go to **Manage** > **Network Services** > **Cloud Connect**, click the settings icon. The configuration page is displayed.
4. To add an account, click **Settings**. Under **Accounts**, select **AWS** from the available options and click **Add Account**.
5. In the **Add AWS Account** pop-up window, enter the following details:
   - **Account Name**—Account name of the AWS admin account. This is the account name created by the user to access the AWS admin account.

The Account name is limited to a maximum of 32 alphanumeric characters.

   - **IAM ROLE: ARN#**—Role ARN of the role created in AWS Console.
   - **Account ID**—Account ID of Aruba Central registered in AWS.
   - **External ID**—External ID of the Aruba Central user account who uses the AWS API token.
   - **AWS Marketplace Subscription Completed**—Enable this option after subscribing to AWS Marketplace Subscription in AWS Marketplace.

Figure 267 *Adding an AWS Account*



6. Click **Submit**.

Orchestrating Tunnel to the AWS VPC through Cloud Connect Service

When the new AWS account is submitted in the **Add AWS Account** window, the orchestration application is triggered to connect to the new AWS account.

To view the orchestration status of the AWS account, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Cloud Connect**, click the settings icon.

   The configuration page is displayed.
3. Select the cloud provider **AWS**, the newly added AWS account is listed.
4. Verify the status of the AWS account. Initially, the status of the AWS account is **INIT**. After a few seconds it changes to **Access Verified**.
5. Click **Deployment** tab. The Cloud Connect service discovers the Transit Gateways (TGWs) for the account and displays them under the Deployment tab.
6. Select a Group from the available options under **Filter groups** and map it to one of the displayed TGWs.
7. Enable the check box under **Connection** column. Select other groups and enable the **Connection** check box to connect multiple Groups to Cloud Hub. Optionally, enable **Accelerated VPN** to connect to the closest AWS edge location.
8. Click **Preview**.

   The page displays all the Groups selected for connecting to Cloud Hub.
9. Click **Submit**.

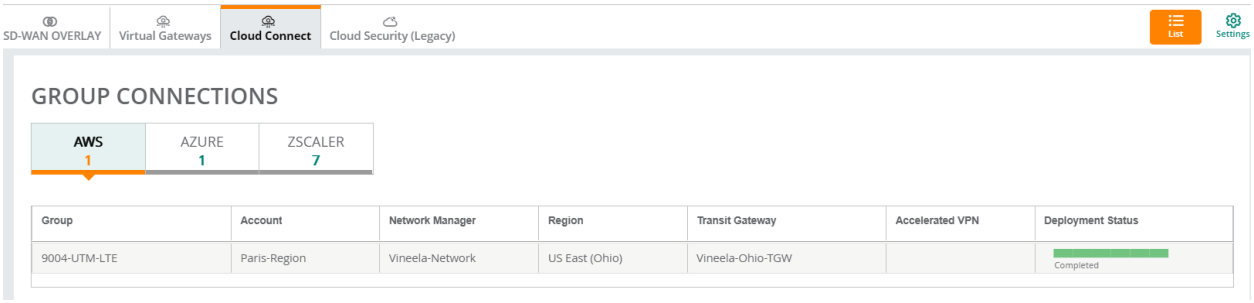
   The **Deployment Status** displays one of the following statuses:
   - **Not started**—Groups are waiting to get connected to Cloud Hub.
   - **Completed**—Groups successfully connected to Cloud Hub.

- **Partially completed**—Cloud connect service is in the process of connecting all the devices belonging to a group from the cloud endpoint.
- **Failed**—If a group or multiple groups fail to connect to Cloud Hub, the failed groups are retried for connecting to Cloud Hub every three minutes.

A summary of the deployment is displayed in the **List** view of the **Group Connections** page with the following columns

- **Group**—Displays the name of the group connected to the Cloud Hub.
- **Account**—Displays the account name of the AWS admin account.
- **Network Manager**—Displays the name of the AWS Transit Gateway Network Manager.
- **Region**—Displays the region of the AWS VPC.
- **Transit Gateway**—Displays the name of the AWS Transit Gateway.
- **Accelerated VPN**—Allows you to enable accelerated VPN for the group. Accelerated VPN uses AWS Global Accelerator to route traffic from your on-premises network to an AWS edge location that is closest to Aruba Branch Gateway. For more information, see AWS Documentation.
- **Deployment Status**—Displays the deployment status of the group.

Figure 268 *Group Connections Summary*



Verifying the Instantiation Status

To verify the instantiation status, complete the following steps:

1. Verify the tunnel status
2. Verify the two default VLANs created to establish BGP neighborship
3. Verify the BGP neighbors and route map configurations
4. Verify the established BGP sessions with AWS Transit Gateways

Verifying Tunnel Status

To verify the status of the tunnels, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.

4. Under **Manage**, click **WAN** > **Tunnels**.

   The Tunnels summary and Tunnels table displays the information about all the tunnels associated with the gateway. For more information, see Gateway > WAN > Tunnels.
5. Click the **Mode** drop-down in the **Tunnels** table.
6. Select **Orch-IKE** to view the tunnel created from Aruba Branch Gateway to AWS Transit Gateway. For more information, see Gateway > WAN > Tunnels.

   You can also view the tunnel status and uplink health in the **Monitoring & Reports** > **Topology** page. For more information, see Monitoring Sites in the Topology Tab.

Ensure that the gateway is part of a site to appear in the Topology page.

Verifying the Default VLANs

To verify the status of the two default VLANs created, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Device**. The gateway device configuration page is displayed.

   If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Interface**> **VLANs**. The two default VLANs automatically pushed by the Cloud Connect service is displayed under the **VLANs** table.

The VLAN IDs ranging from 4000 to 4080 is reserved for Cloud Connect service.

Verifying the BGP Neighbors and Route Map Configurations

To verify the BGP neighbors and route map configurations, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Device**. The gateway device configuration page is displayed.

   If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Routing** > **BGP**> **Neighbors**.

   The **Neighbors** table displays the two BGP neighbor configurations pushed by the Cloud Connect service along with the default route maps **auto_cloud_connect_in** and **auto_cloud_connect_out** attached to the neighbors.

6. Click Route Map to view the **Route maps** table that lists the default route map configurations **auto_cloud_connect_in** and **auto_cloud_connect_out**.

Verifying the Established BGP Sessions with AWS Transit Gateways

To verify the established BGP sessions with AWS Transit Gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **BGP**.

   The two BGP neighbors connected with the AWS Transit Gateways are listed under the **BGP Details** table.

The BGP neighbor addresses range from 169.254.0.0 to 169.254.0.24.

Chapter 19
Integration with Microsoft Azure Public Cloud through Cloud Connect Service

The SD-Branch integration with Azure public cloud through Cloud Connect service allows you to set up a secure connection between the Aruba Branch Gateways and Azure Virtual WANs or Virtual hubs (Vhubs). This integration simplifies deploying large-scale, secure and optimized branch connectivity across the global Microsoft network.

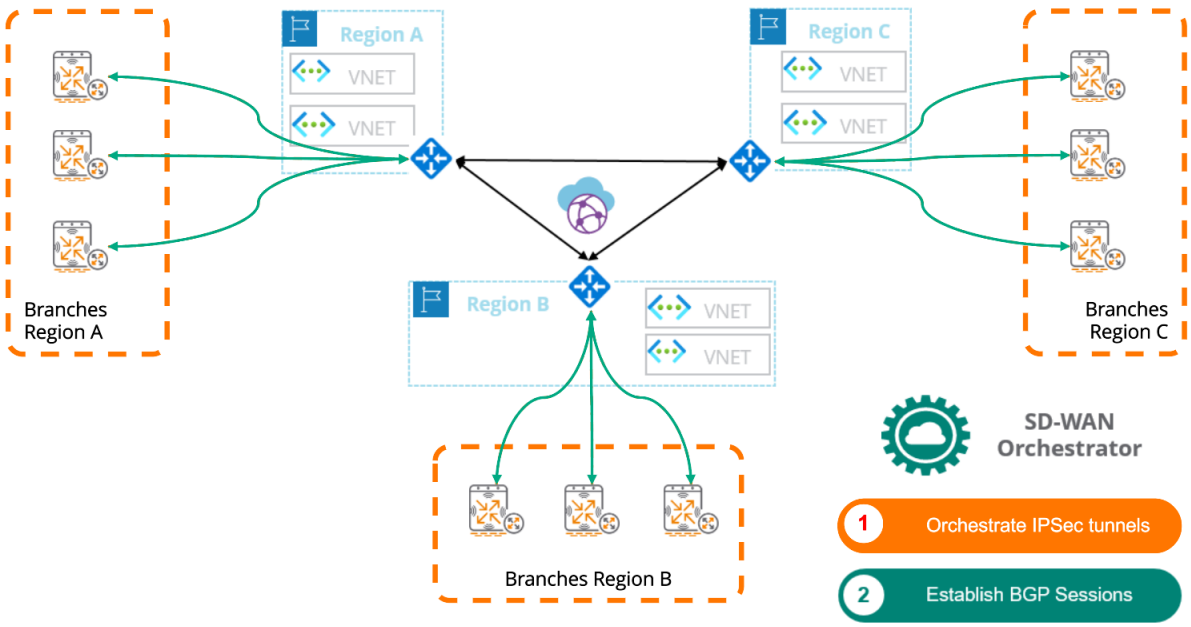
Using the Cloud Connect service, the Aruba Branch Gateways establish a secure connectivity with regional Azure VNETs through the Azure Virtual WAN. The Cloud Connect service uses SD-Branch Orchestrator as the transport medium to send configurations to Branch Gateways. Branch Gateways connect to Azure Virtual WANs and Vhubs through the automatically orchestrated IPsec tunnels and route exchange.

Once the tunnels are up, eBGP sessions are established to exchange prefixes between the Azure Virtual WAN and Aruba SD-Branch, and allow dynamic exchange of routes. The reverse-pinning technology is used to ensure that the traffic is sent back through the same tunnel from which the traffic originated.

For more information about the supported scenarios, see *Aruba SD-WAN Integration with Microsoft Azure Public Cloud Tech Note*.

The following figure illustrates the SD-Branch integration with the Azure public cloud network:

Figure 269 *Cloud Connect and SD-Branch Integration with Azure Public Cloud through Cloud Connect*



To integrate SD-Branch with Azure public cloud through Cloud Connect service, complete the following steps:

1. Configure Azure application in Azure Admin Portal
2. Configure Azure application for API access in Azure Admin Portal
3. Configure Aruba Branch Gateway in Aruba Central
4. Onboard Cloud provider accounts into Aruba Central through Cloud Connect service

5. Orchestrate tunnel to the Azure virtual WAN through Cloud Connect service
6. Verify tunnel status

Additional References

For more information about Microsoft Azure Virtual WAN, see https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about.

For detailed instructions about adding Azure account in Aruba Central, and Azure specific configurations related to vWan and vhubs, see *Aruba SD-WAN Integration with Microsoft Azure Public Cloud Tech Note*.

Configuring Azure Application in Azure Admin Portal

To configure a new Azure application, complete the following steps:

1. Log in to the Azure admin portal.
2. Go to the search bar and type **App registrations**.
3. Click **New registration**.
4. Create the new application with a **Name** and **Supported account types**.
5. Click **Register**.
6. Note the **Tenant ID** and **Application ID** of the registered application. The **Tenant ID** and **Application ID** are required to add the Azure application in Aruba Central.
7. Navigate to **Manage** > **Certificates & secrets** to create a new application secret.
8. Click **New Client secret**.
9. Create the application secret with a description of the secret and duration.
10. Click **Add**.
11. Note the value of the client secret. The client secret value and the Application ID is required for orchestration in Aruba Central.

Configuring Azure Application for API Access in Azure Admin Portal

To configure Azure application for API access, complete the following steps:

1. Log in to the Azure admin portal.
2. Navigate to **Manage** > **API permissions** to add permissions.
3. Click **Add a permission**.
4. Click **Microsoft APIs** and select **Azure Service Management**.
5. Enable the **user_impersonation** check box permission. This permission allows Aruba Central to access the Azure API.
6. Click **Add permissions**.
7. Navigate to **Home** > **Subscriptions**.
8. Go to your subscription and select **Access Control (IAM)**.
9. Click **Add**.
10. Click **Add role assignment**. The Add role assignment pane opens.
11. Select **Role** as **Contributor** role from the drop-down list.

12. Select the created Azure application from the **Select** drop-down list.
13. Click **Save** to assign the role.
14. Go to the **Role assignments** tab to view the recently added role.

Configuring Aruba Branch Gateway in Aruba Central

Before you onboard an Azure account in Aruba Central, ensure that the following prerequisites are met:

1. Configure uplinks for the ArubaBranch Gateway or VPNC. For more information, see Configuring Uplinks

NOTE

Microsoft Azure only supports one active tunnel from a branch.

The site name should not include the special characters hyphen (-) and underscore (_).

The uplink name should not include the special characters dot (.), hyphen (-), and underscore (_).

2. If there are multiple uplinks in the device, the uplink selection is based on the following selection criteria:
   - INET link type— If there are multiple uplinks, then the uplink with higher weight is selected. If the uplinks have the same weight, then the uplink with higher speed is selected. If uplinks have the same speed, an uplink with higher VLAN ID is selected.
   - LTE link type—This link type is used when INET link type is not present.
3. Enable tunnel orchestration to establish tunnels between Aruba Branch Gateways and Azure vWAN. For more information, see SD-WAN Overlay Tunnel and Route Orchestration .
4. Enable BGP and configure a valid Autonomous System (AS) number at device level. BGP can be enabled at group level but ensure that the AS number is unique per site. For more information, see Enabling BGP.

NOTE

For more information about supported and not supported AS numbers, see Microsoft Azure Documentation.

5. Enable BGP multipath at the device level or group level. For more information, see Configuring Multipath Selection.
6. To advertise branch subnets with with Azure, redistribute connected, static, or OSPF routes to BGP.

NOTE

- Branch-HA deployments are not supported and a tunnel is formed only through the physical uplink.
- Cloud connect service creates route-maps `auto_cloud_connect_in` and `auto_cloud_connect_out`. These route-maps are editable and have a default permit rule with sequence number 20. It is recommended to edit these route-maps to filter the routes exchanged with Azure vWAN service.

Onboarding Azure Account in Aruba Central

To onboard an Azure account, complete the following steps:

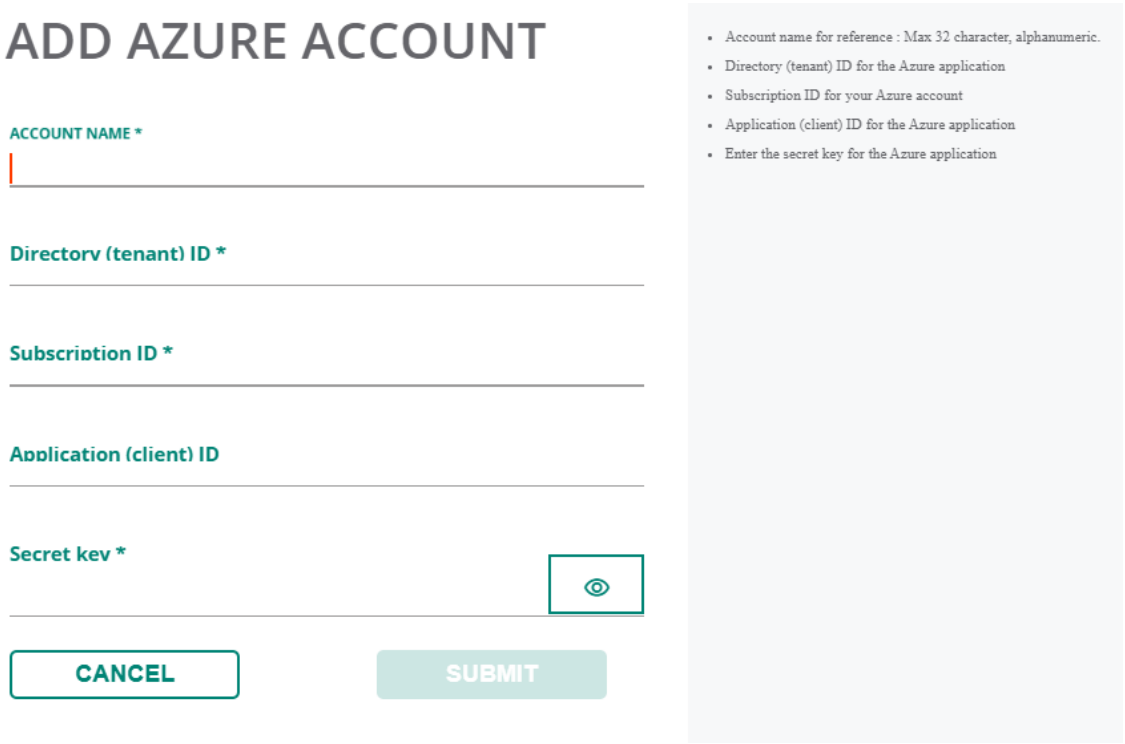
1. Log in to Aruba Central.
2. In the **Network Operations** app, set the filter to **Global**.
3. Go to **Manage** > **Network Services** > **Cloud Connect**, click the settings icon. The configuration page is displayed.
4. To add an account, click **Settings**. Under **Accounts**, select **Azure** from the available options and click **Add Account**.
5. In the **Add Azure Account** pop-up window, enter the following details:
   - **Account Name**—Account name of the Azure admin account. This is the account name created by the user to access the Azure admin account.

NOTE

The Account name is limited to a maximum of 32 alphanumeric characters.

   - **Directory (tenant) ID**—Tenant ID of the Azure application created in Azure Admin Portal.
   - **Subscription ID**—Subscription ID for the Azure admin account.
   - **Application (client) ID**—Application ID of the Azure application created in Azure Admin Portal.
   - **Secret key**—Secret key of the Azure application created in Azure Admin Portal.

Figure 270 *Adding an Azure Account*



6. Click **Submit**.

Orchestrating Tunnels to Azure Virtual WAN and Vhub through Cloud Connect Service

When the new Azure account is submitted in the **Add Azure Account** window, the orchestration application is triggered to connect to the new Azure account.

To view the orchestration status of the Azure account, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Cloud Connect**, click the settings icon.

   The configuration page is displayed.
3. Select the cloud provide **Azure**, the newly added Azure account is listed.
4. Verify the status of the Azure account. Initially, the status of the Azure account is **INIT**. After a few seconds it changes to **Access Verified**.
5. Click the **Deployment** tab. The Cloud Connect service discovers the Virtual WAN hubs for the account and displays them under the Deployment tab.
6. Select a Group from the available options under **Filter groups** and map it to one of the Virtual WAN hubs.
7. Enable the check box under **Connection** column. Select other groups and enable the **Connection** check box to connect multiple Groups to Cloud Hub.
8. Click **Preview**.

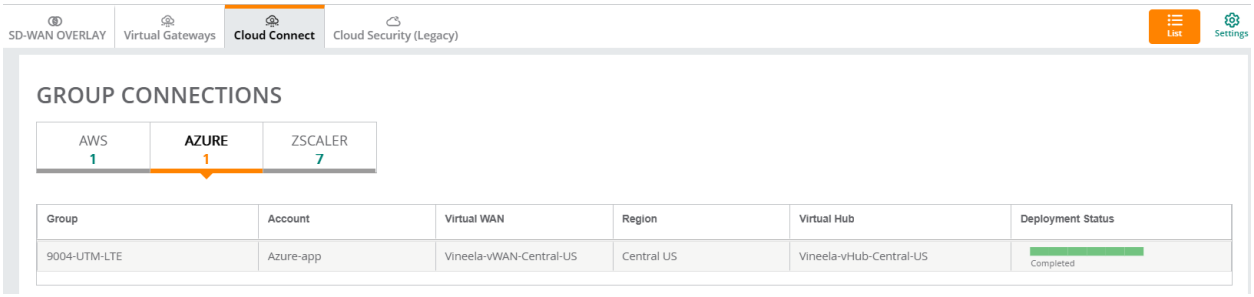
   The page displays all the Groups selected for connecting to Cloud Hub.
9. Click **Submit**.

   The **Deployment Status** displays one of the following statuses:
   a. **Not started**—Groups are waiting to get connected to Cloud Hub.
   b. **Completed**—Groups successfully connected to Cloud Hub.
   c. **Partially completed**—Cloud connect service is in the process of connecting all the devices belonging to a group from the cloud endpoint.
   d. **Failed**—If a group or multiple groups fail to connect to Cloud Hub, the failed groups are retried for connecting to Cloud Hub every three minutes.

A summary of the deployment is displayed in the **List** view of the **Group Connections** page with the following columns:

- **Group**—Displays the name of the group connected to the Cloud Hub.
- **Account**—Displays the account name of the Azure admin account.
- **Virtual WAN**—Displays the name of the Azure Virtual WAN.
- **Region**—Displays the region of the Azure VNET.
- **Virtual Hub**—Displays the name of the Azure Vhub. For more information, see Azure Documentation.
- **Deployment Status**—Displays the deployment status of the group.

Figure 271 *Group Connections Summary*



Verifying the Instantiation Status

To verify the instantiation status, complete the following steps:

1. Verify the tunnel status
2. Verify the BGP neighbors and route map configurations
3. Verify the established BGP sessions with Azure vWAN

Verifying Tunnel Status

To verify the status of the tunnels, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Tunnels**.

   The Tunnels summary and Tunnels table displays the information about all the tunnels associated with the gateway. For more information, see Gateway > WAN > Tunnels.
5. Click the **Mode** drop-down in the **Tunnels** table.
6. Select **Orch-IKE** to view the tunnel created from ArubaBranch Gateway to AWS Transit Gateway. For more information, see Gateway > WAN > Tunnels.

   You can also view the tunnel status and uplink health in the **Monitoring & Reports** > **Topology** page. For more information, see Monitoring Sites in the Topology Tab.

Ensure that the gateway is part of a site to appear in the Topology page.

Verifying the BGP Neighbors and Route Map Configurations

To verify the BGP neighbors and route map configurations, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Device**. The gateway device configuration page is displayed.

   If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Routing** > **BGP**> **Neighbors**.

   The **Neighbors** table displays the BGP neighbor configurations pushed by the Cloud Connect service along with the default route maps **auto_cloud_connect_in** and **auto_cloud_connect_out** attached to the neighbors.
6. Click **Route Map** to view the **Route maps** table that lists the default route map configurations **auto_cloud_connect_in** and **auto_cloud_connect_out**.

Verifying the Established BGP Sessions with Azure vWAN

To verify the established BGP sessions with Azure vWAN, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **BGP**.

   The two BGP neighbors connected with the Azure vWAN are listed under the **BGP Details** table.

The BGP neighbor addresses range from 169.254.0.0 to 169.254.0.24.

Chapter 20
Integration with Zscaler through Cloud Connect Service

The SD-Branch integration with Zscaler through Cloud Connect service allows you to set up a secure connection between the Aruba Branch Gateways and one or several cloud-hosted enforcement points called Zscaler Internet Access (ZIA) Public Service Edges.

The Cloud Connect service uses SD-Branch Orchestrator as the transport medium to send configurations to Branch Gateways. Branch Gateways connect to ZIA Public Service Edges through the automatically orchestrated IPsec tunnels—Orch-IKE tunnels, which use the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite with Zscaler. This provides the ability to traverse NAT boundaries and leverage IKEv2 for authentication, while at the same time limiting the overhead. After the tunnels are established between the Branch Gateways and ZIA Public Service Edges, Zscaler uses reverse-pinning technology to ensure that the traffic is sent back through the same tunnel from which the traffic originated.

When using framework to orchestrate Cloud Security connections, it is preferable to establish a maximum of 50 connections within a span of one hour. If any tunnel is deleted, Cloud Connect has the auto healing mechanism to re-establish that tunnel through orchestration.

The Cloud Connect service continuously looks for new ZIA Public Service Edges. If there are new ZIA Public Service Edges available, it pushes the maps of these ZIA Public Service Edges to the Branch Gateways and ensures that they are always connected to a Public Service Edge at any give time.

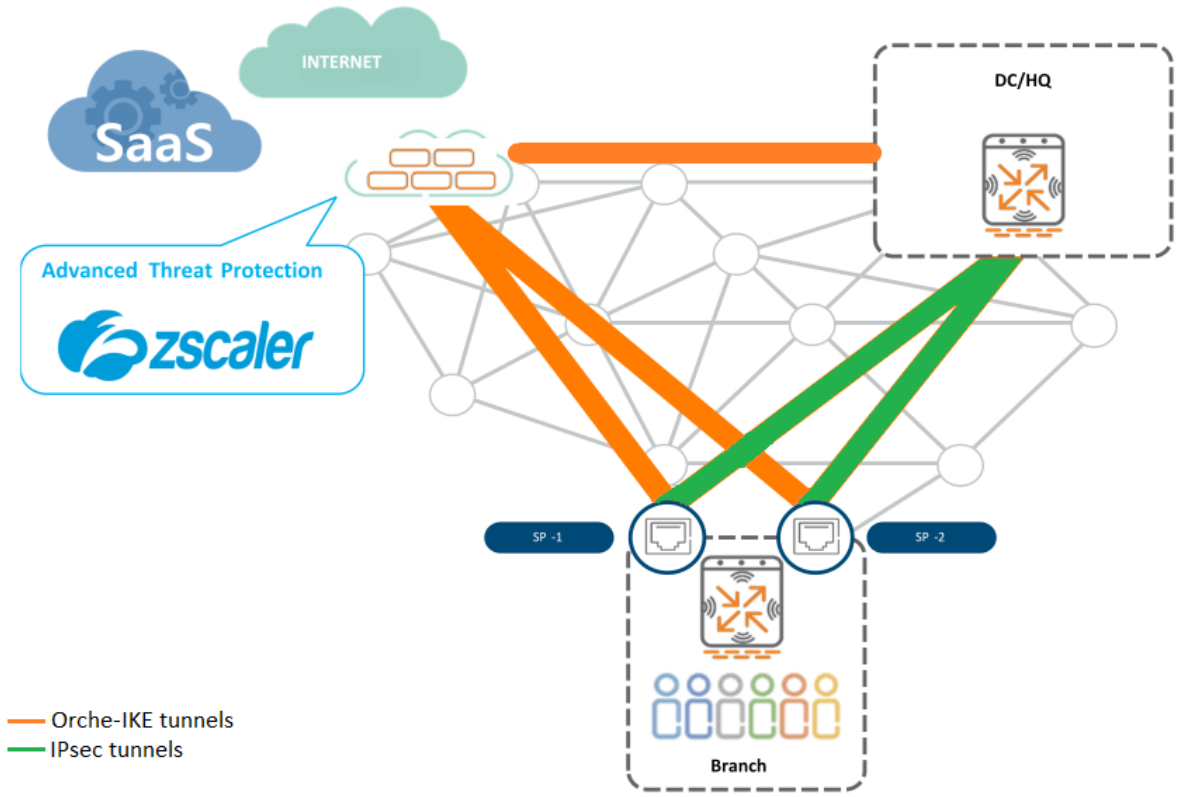
The integration of SD-Branch and ZIA is supported with following scenarios:

- Single Branch Gateway to ZIA—If multiple uplinks are used, the Branch Gateway establishes one tunnel per uplink for the primary and secondary nodes.
- Dual Gateway to ZIA—If branch High Availability (HA) is used, the gateways establish tunnels to ZIA through virtual and physical uplinks.
- Headend Gateway (VPNC or Virtual Gateway) to ZIA— VPNCs establish tunnels to two ZIA nodes. In this case, only one tunnel per ZIA node is established, as the VPNC does not support the load-balancing logic.

For more information about the supported scenarios, see *Aruba SD-Branch and Zscaler Internet Access Integration Tech Note*.

The following figure illustrates the SD-Branch integration with the Zscaler cloud network:

Figure 272 *Cloud Connect and SD-Branch Integration with Zscaler through Cloud Connect*



To integrate SD-Branch with Zscaler through Cloud Connect service, complete the following steps:

1. Configure ZIA for API access in Zscaler Admin Portal
2. Onboard Cloud provider accounts into Aruba Central through Cloud Connect service
3. Orchestrate tunnel to the nearest ZIA Public Service Edge through Cloud Connect service
4. Configure Zscaler nexthop list
5. Add nexthop list to PBR policy
6. Verify tunnel status

Additional References

For more information on Zscaler and Aruba SD-Branch integration with ZIA:

- Visit https://www.zscaler.com/
- Refer to the *Aruba SD-Branch and Zscaler Internet Access Integration Guide*

Configuring ZIA for API Access in Zscaler Admin Portal

In the automated workflow, it is not required to configure locations or VPN credentials in the Zscaler admin portal. Instead, SD-WAN Orchestrator uses the partner access to communicate through the API.

To add a partner API key for Aruba SD-Branch, complete the following steps:

1. Log in to the Zscaler admin portal.
2. Click **Administration** > **Partner Integrations** > **SD-WAN** in the Partner Integrations page in the ZIA portal.
3. Click **Add Partner Key** and create a Partner API Key.
4. Create a **Partner Administrator Role** with a name, access control, and SD-WAN API partner access to provide credentials for the API access. This is done from **Administration** > **Role Management**.
5. Create a partner account for the SD-WAN Orchestrator with the following details. This can be done from Administration > Administrator Management > Partner Administration.
   a. Login ID—Login ID of the ZIA API user account.
   b. Email—Email address of the ZIA API user account.
   c. Name—Username of the ZIA API user account.
   d. Partner Role—Name of the Partner Administrator Role.
   e. Password—Password of the ZIA API user account.

Onboarding a Cloud Provider Account in Aruba Central

Before onboarding a cloud provider account through Cloud Connect service, ensure that any existing account created through the Cloud Security (Legacy) service is deleted.

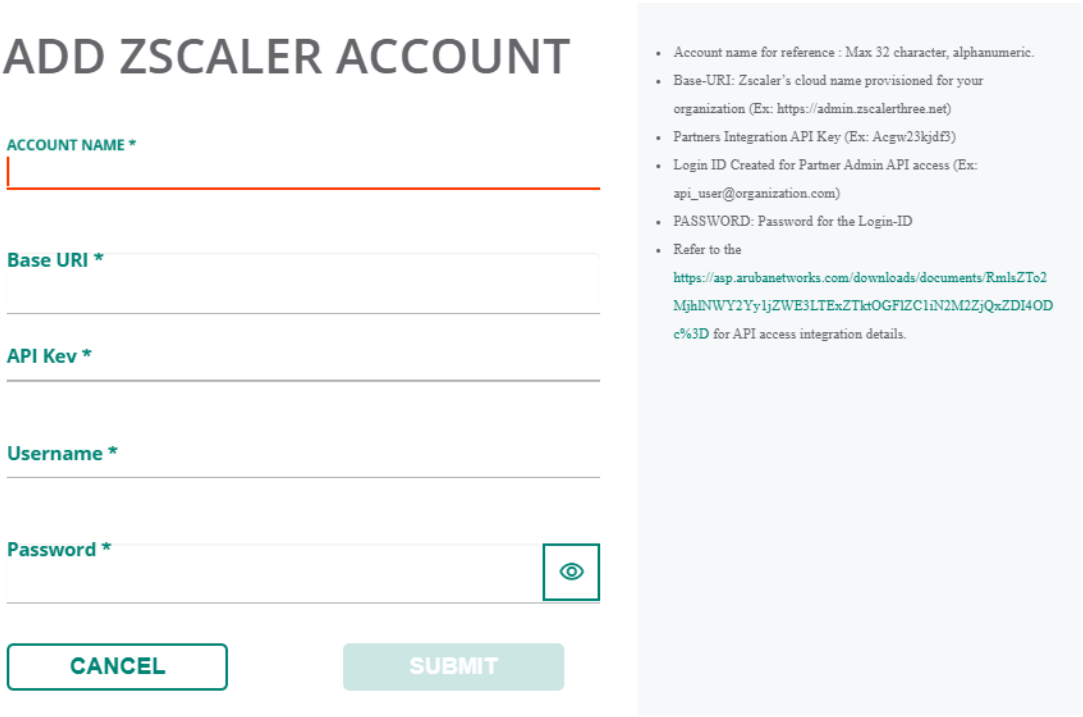
To onboard a Zscaler account, complete the following steps:

1. Log in to Aruba Central.
2. In the **Network Operations** app, set the filter to **Global**.
3. Go to **Manage** > **Network Services** > **Cloud Connect**, click the settings icon. The configuration page is displayed.
4. To add an account, click **Settings**. Under **Accounts**, select **Zscaler** from the available options and click **Add Account**.
5. In the **Add Zscaler Account** pop-up window, enter the following details:
   - **Account Name**—Account name of the ZIA admin account. This is the account name created by the user to access the ZIA admin account.

The Account name is limited to a maximum of 32 alphanumeric characters.

   - **Base URI**—Base URI of the Zscaler API. This is the Zscaler cloud name that was provisioned for your organization.
   - **API Key**—Integration API key to access ZEN.
   - **Username**—Username of the ZIA admin account. This is the username created by the user to access the ZIA credentials for Partner admin API access.
   - **Password**—Password of the admin account. This is the password created by the user to access the ZIA credentials.

Figure 273 *Adding a Zscaler Account*



6. Click **Submit**.

Orchestrating Tunnels to the Nearest ZIA Public Service Edge

Connect a Group to Cloud Hub using the Cloud Connect service to automatically orchestrate an Orch-IKE tunnel to the nearest ZIA Public Service Edge.

To connect a Group to Cloud Hub, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Cloud Connect**, click the settings icon.

   The configuration page is displayed.
3. Click **Deployment** tab.
4. Select a Group from the available options under **Filter groups**.
5. Enable the check box under **Connection** column. Select other groups and enable the **Connection** check box to connect multiple Groups to Cloud Hub.
6. Click **Preview**.

   The page displays all the Groups selected for connecting to Cloud Hub.
7. Click **Submit**.

The **Deployment Status** displays one of the following statuses:

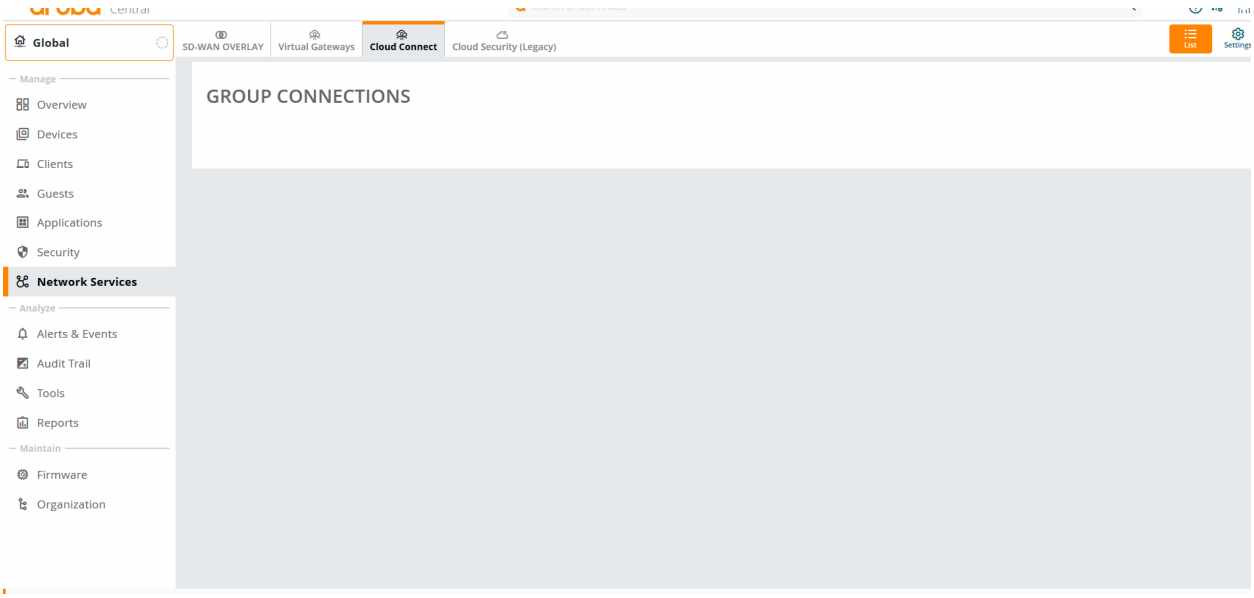
- **Not started**—Groups are waiting to get connected to Cloud Hub.
- **Completed**—Groups successfully connected to Cloud Hub.
- **Partially completed**—Cloud connect service is in the process of connecting all the devices belonging to a group from the cloud endpoint.

- **Failed**—If a group or multiple groups fail to connect to Cloud Hub, the failed groups are retried for connecting to Cloud Hub every three minutes.

NOTE

You may notice a delay up to five minutes to see the actual deployment status.

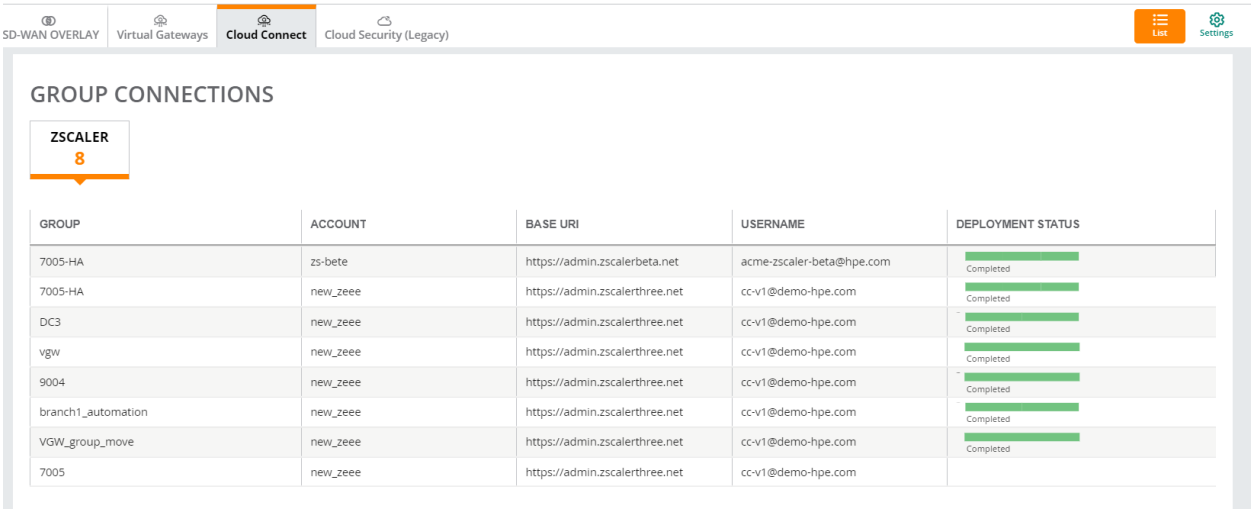
Figure 274 *Connecting a Group to Cloud Hub*



A summary of the deployment is displayed in the **List** view of the **Orchestrated Cloud Provider** page with the following columns:

- **Group**—Displays the name of the group connected to the Cloud Hub.
- **Account**—Displays the account name of the ZIA admin account.
- **Base URI**—Displays the Base URI of the Zscaler API.
- **Username**—Displays the username of the ZIA admin account.
- **Deployment Status**—Displays the deployment status of the group.

Figure 275 *Group Connections Summary*



Important Points to Note

- The topology scan is performed every one hour to probe the cloud topologies. To expedite the topology scan to two minutes:
  - Navigate to **Manage** > **Network Services** > **Cloud Connect** > **Deployment tab** and click the manual refresh icon located at the right corner of the page.
- Resync is a periodic job that triggers every one hour to complete any pending or failed connect and disconnect actions. It can be expedited to five minutes through:
  - External events such as CAAS changes, device addition, device deletion, device movement, Public IP change, and site changes.
  - Internal events such as failure to deploy, undeploy, or download.

Configuring Zscaler Nexthop List

Configure Zscaler nexthop list with Zscaler active and standby IPsec tunnels on different uplinks. For more information on configuring a nexthop list, see Configuring Next Hop Lists for PBR.

Adding Nexthop List to PBR Policy

Add the nexthop list to a PBR policy and ensure that the policy is applied to a user role or VLAN. For more information on adding a nexthop list to a global PBR policy, see Configuring Policies for PBR.

Verifying Tunnel Status

To verify the status of the tunnels, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. Ensure that the filter selection contains at least one gateway.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Tunnels**.

   The Tunnels summary and Tunnels table displays the information about all the tunnels associated with the gateway. For more information, see Gateway > WAN > Tunnels.
5. Click the **Mode** drop-down in the **Tunnels** table.
6. Select **Orch-IKE** to view the Zscaler tunnels. For more information, see Gateway > WAN > Tunnels.

   You can also view the tunnel status and uplink health in the **Monitoring & Reports** > **Topology** page. For more information, see Monitoring Sites in the Topology Tab.

Ensure that the gateway is part of a site to appear in the Topology page.

You can view the BGP status and route distribution status in the BGP monitoring dashboard. For more information, see Verifying the BGP Configuration.

To secure traffic and enforce policies, businesses often use MPLS links or encrypted VPN links to tunnel traffic between the branch and data center. However, backhauling branch traffic to the data center before it reaches an endpoint can result in latency and increased bandwidth consumption.

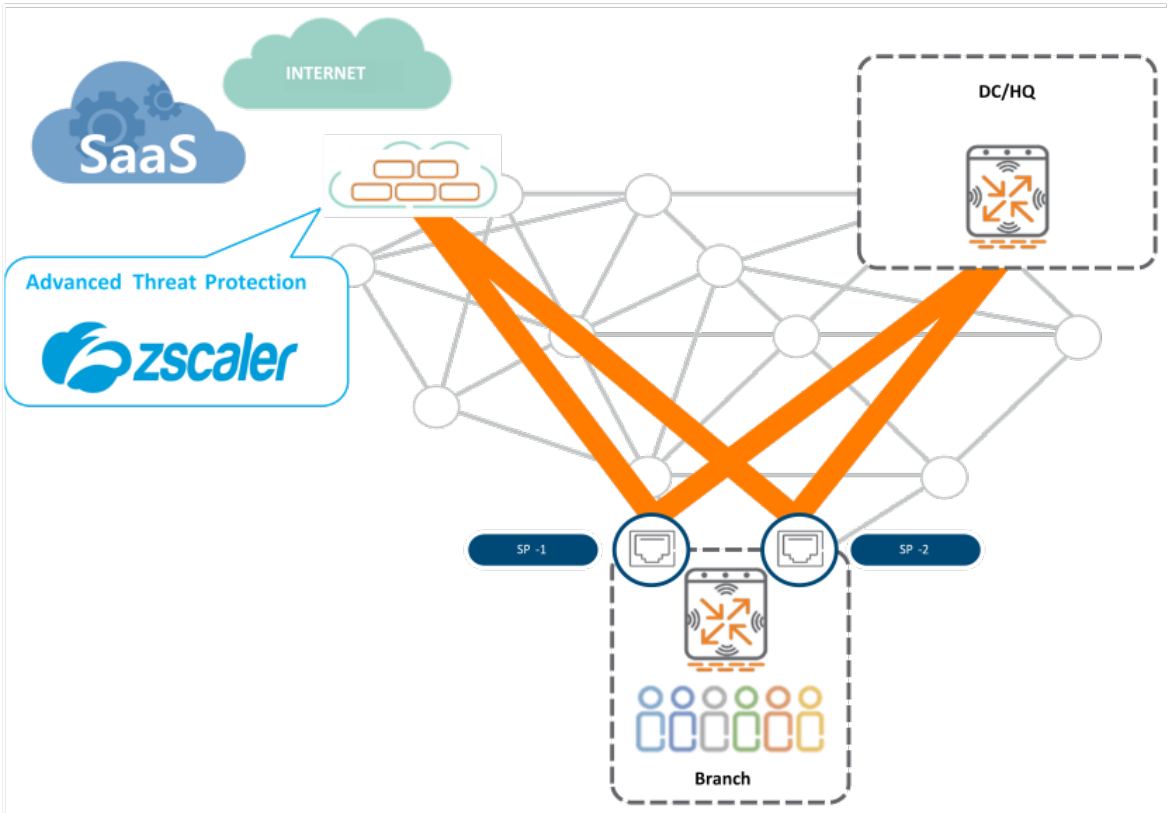
For faster delivery and efficient use of bandwidth, you can break your branch traffic locally and redirect the traffic directly to the Internet. However, if you want to allow branch devices to directly connect to the Internet, you must ensure that your branch network is secured from threats. The most common approach to secure the branch Internet traffic is to enable branch devices to route all Internet traffic through a cloud security platform, such as the Zscaler cloud security service.

The Zscaler Cloud Security Platform provides fast and secure connections between users and applications, regardless of device, location, or network. Branch Gateways in the SD Branch can inter-operate with Zscaler cloud network to provide a secure branch network connectivity with threat detection capabilities.

The integration between the Aruba Branch Gateways and Zscaler Internet Access (ZIA) allows you to set up a secure connection between the branch networks and one or several cloud-hosted enforcement points called Zscaler Enforcement Nodes (ZENs).

The following figure illustrates the SD-Branch integration with the Zscaler cloud network:

Figure 276 *Zscaler and SD-Branch Integration*



Branch Gateways connect to ZENs through IPsec tunnel with null encryption. This provides the ability to traverse NAT boundaries and leverage IKEv2 for authentication, while at the same time limiting the overhead.

After the tunnels are established between the Branch Gateways and ZEN nodes, Zscaler uses reverse-pinning technology to ensure that the traffic is sent back through the same tunnel from which the traffic originated.

Integrating SD-Branch with ZIA

The SD-Branch and Zscaler integration requires configuration at both Zscaler admin interface and Aruba Central.

Ensure that you complete these prerequisite steps, before configuring Branch Gateways for ZIA integration:

1. Locate the FQDN of the ZIA instance to be used. For more information, see the *Locating the Hostnames and IP Addresses of Your ZENs* at ZIA Help portal.
2. Verify that the Branch Gateways can resolve the FQDN of the selected nodes.
3. Access the ZIA admin portal and set up the customer information, VPN credentials, and location (site information).
4. Set up the API key to use for the Zscaler REST APIs.

Setting up Tunnels to ZIA

The Aruba SD-Branch supports the following types of configuration methods for setting up IPsec tunnels to ZIA:

- **Orchestrated Tunnel Establishment**—In this method, ZENs are automatically discovered and assigned for tunnel establishment. This configuration can be applied globally or at the group level. Aruba recommends that you use the global configuration or large SD-Branch deployments.
- **Manual Tunnel Establishment**—In this method, you must manually configure ZEN nodes on each Branch Gateway group.

Orchestrated Tunnel Establishment

The orchestrated tunnel establishment or automatic tunnel service is a limited availability feature. To avail this feature, contact your Aruba Sales specialist.

In this method, SD-Branch Orchestrator automates large distributed deployments to integrate Aruba SD-Branch and ZIA.

To enable SD-Branch Orchestrator to automate large distributed deployments, perform the following steps:

1. Configure ZIA for API Access in Zscaler admin portal.
2. Configure Aruba SD-Branch for Orchestrated Tunnels in Aruba Central.

Configuring ZIA for API access

In the automated workflow, it is not required to configure locations or VPN credentials in the Zscaler admin portal. Instead, SD-Branch Orchestrator uses the partner access to communicate through the API.

To add a partner API key for Aruba SD-Branch, complete the following steps:

1. Log in to the Zscaler admin portal.
2. Click **Administration** > **Partner Integrations** > **SD-WAN** in the Partner Integrations page in the ZIA portal.
3. Click **Add Partner Key** and create a Partner API Key.
4. Create a **Partner Administrator Role** with a name, access control, and SD-Branch API partner access to provide credentials for the API access. This is done from **Administration** > **Role Management**.
5. Create a partner account for the SD-Branch Orchestrator with the following details. This can be done from Administration > Administrator Management.
   a. Login ID—Login ID of the ZIA admin account.
   b. Email—Email address of the ZIA admin account.
   c. Name—Username of the ZIA admin account.
   d. Partner Role—Name of the Partner Administrator Role.
   e. Password—Password of the ZIA admin account.

Configuring Aruba SD-Branch for Orchestrated Tunnels

The automatic tunnel service is a limited availability feature. To avail this feature, contact your Aruba Sales specialist.

To automatically set up IPsec tunnels between the Branch Gateways in Aruba Central and ZIA:

1. 1. To enable automatic configuration of IPSec Tunnels globally on all Branch Gateways, click **Global Settings** and configure the following parameters:
   a. Select the **Automatic** option.
   b. Configure the following parameters:
      - **Base URI**—Base URI of the Zscaler API. This is the Zscaler cloud name that was provisioned for your organization. For example: **admin.zscalerbeta.net**
      - **Username**—Username of the ZIA admin account. This is the username created by the user to access the ZIA credentials.
      - **Password**—Password of the admin account. This is the password created by the user to access the ZIA credentials.
      - **API Key**—API key for accessing the ZENs.

The base URI and API key information are available in the ZScaler Admin Portal.

   a. Click **Save Settings**.
2. To enable automatic IPSec tunnel establishment with ZIA on specific device groups:
   a. Click **Group Orchestration**
   b. Select the device groups.
   c. Click **Enable**.

When automatic tunnel configuration is enabled, the tunnel orchestration service performs the following functions:

- Obtains the public IP address of all Gateways that are currently connected to Aruba Central.
- Based on the public IP address of the Branch Gateways, discovers two ZENs closer for each Branch Gateway.

- Generates and publishes an IKE crypto map on the Branch Gateways.
- Registers Branch Gateways in the Zscaler cloud network using the ZIA admin credentials configured in Aruba Central. When the devices are registered, the tunnel configuration is distributed to the ZENs in the Zscaler cloud.

Manual Tunnel Establishment

In the manual workflow, the integration with ZIA requirs configurations on the Zscaler admin portal and Aruba Central.

Prerequisites

Locate the FQDN of the ZIA instance to be used. For more information, see the *Locating the Hostnames and IP Addresses of Your ZENs* at ZIA Help portal.

Configuring ZIA

Configure the ZIA service to terminate VPN tunnels from Aruba Branch Gateway. These VPN tunnels are the IPSec tunnels using IKEv2 credentials to uniquely identify each Branch Gateway. Each Branch Gateway would therefore have to be assigned with a Location and the corresponding VPN credentials in the Zscaler admin portal.

To create the Location and credentials in Zscaler admin portal:

1. Navigate to **Administration** > **Resources** > **Location Management**.
2. Choose **Add Location** and enter the general information about the location.
3. Select the previously created VPN credentials or create a new set of credentials by clicking the **+** sign.
4. Optionally, enable other features for this location.

Configuring Aruba Branch Gateways to manually establish tunnels to ZIA

Perform the following tasks on the Branch Gateway to enable Zscaler integration:

1. To configure a Gateway group or Gateway complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.

3. Click **VPN** > **Cloud Security**.
4. In the **IPsec Maps** section, click **+** to open the **New IPsecmap** section.
5. Ensure that Zscaler is set as the cloud security provider.
6. Enter an administrative name for the tunnel.
7. Enter a priority number for the IPsec map within a range of 1 to 10,000. A priority value of 1 indicates the highest priority. Ensure that the same priority is set for all active and backup tunnels.
8. Configure a transform set. Transform sets allow you to define a combination of security protocols and algorithms that you can apply to the IPsec traffic flow. To add a transform set:
   a. Click **+** in the **Transforms** section.
   b. Enter a name for the transform.
   c. Specify the encryption methods to use in the transformation set.

The Zscaler cloud provider does not support DES encryption in IKEv2 phase 2 parameters. For more information, see https://help.zscaler.com/zia/about-ipsec-vpns.

   d. Click **Save Settings**.
9. Enter the FQDN of the Zscaler Enforcement Node (ZEN) as **Destination gateway FQDN**.

Ensure that the destination gateway FQDN value contains the string, zscaler in it.

10. Enter the FQDN of the VPN source in **Source FQDN**.
11. Select the VLAN ID to which you want to apply the IPsec map. For Branch Gateways, select uplink VLAN. You can select multiple VLANs to enable load balancing between multiple uplinks.
12. Enter IKE pre-shared secret key that you configured on the ZIA portal.
13. Click **Save Settings**.
14. Repeat the steps to create a backup tunnel.
15. Specify the source FQDN in the **Source FQDN** field.
16. Configure the following parameters to the specified values:
    - Select Any in the Source network type field.
    - Select **Any** in the **Destination network type** field.
    - Select **v2** in the **IKE version** field.
    - Create and add **ESP-NULL** transform set in the **Transforms** table.
    - Select **Dynamic** in the **Remote peer addressing** field.
    - Select **Initiator** in the **Destination gateway** field.
    - Select **FQDN** in the **Peer gateway type** field.
    - Specify the **<ZEN node FQDN>** in the **Destination gateway FQDN** field.
    - Specify the source FQDN in the **Source FQDN** field.
    - Select the **Authentication type** as **PSK**.
    - Enter the PSK secret in the **PSK value** field.

Configuring Zscaler Nexthop List

Configure Zscaler nexthop list with Zscaler active and standby IPsec tunnels on different uplinks. For more information on configuring a nexthop list, see Configuring Next Hop Lists for PBR.

Adding Nexthop List to PBR Policy

Add the nexthop list to a PBR policy and ensure that the policy is applied to a user role or VLAN. For more information on adding a nexthop list to a global PBR policy, see Configuring Policies for PBR.

Verifying Tunnel Status

To verify the status of the tunnels:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the List view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Overview**. The **Gateway Details** page is displayed.
5. Click the **Tunnels** tab to view the Zscaler tunnel details.

For more information, see Gateway > WAN > Tunnels.

You can also view the tunnel status and uplink health in the **Monitoring & Reports** > **Topology** page.

Additional References

For more information on Zscaler and Aruba SD-Branch integration with ZIA:

- Visit https://www.zscaler.com/
- Refer to the *Aruba SD-Branch and Zscaler Internet Access Integration Guide*

Chapter 22
Integration with Prisma Access

A common network architecture today is to tunnel traffic between an organization's HQ and branches over either MPLS or dedicated encrypted VPN links. As more services are moving to a cloud-based architecture, breaking out traffic locally from the branches allows faster delivery and efficient use of bandwidth as opposed to tunneling traffic back to an aggregation point before routing it to its final destination. However, allowing branch devices to directly connect to the Internet may introduce security issues.

The integration between the Aruba Branch Gateways and Prisma Access secures connection between the branch networks and one or several cloud-hosted enforcement points. Prisma Access is a cloud-based infrastructure that provides security to branch networks by allowing organizations to set up regional cloud-based firewalls. The Aruba Branch Gateways can be configured to bring up secure tunnels to the Prisma Access firewall and redirect selected traffic flows through Prisma Access to provide advanced threat protection in an efficient and scalable way.

The integration between ClearPass and Prisma Access also enables sharing the user context with the firewall and facilitates the creation of role-centric security policies.

The combined solution can offer the following benefits:

- Unified security management for campus and branch networks.
- Context-aware security policies driven by ClearPass.
- Intelligent routing of traffic based on user-role and application.

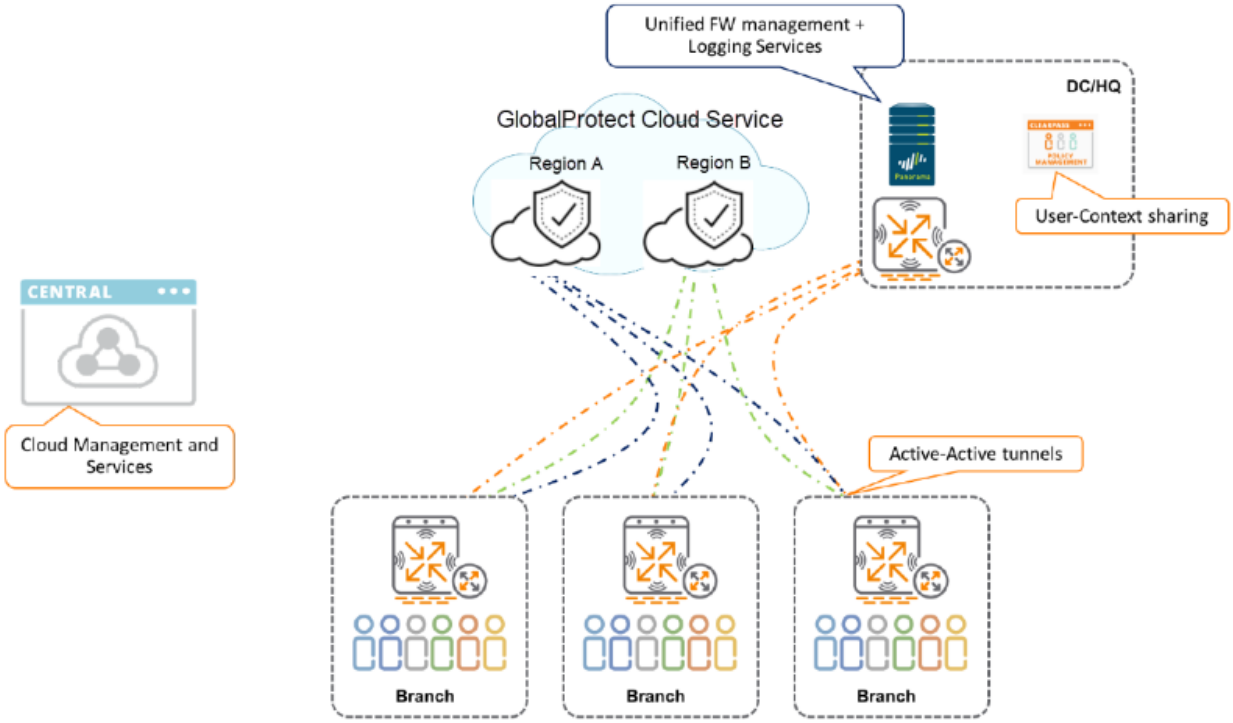
Deployment Scenarios

The SD-Branch and Prisma Access integration supports the following deployment scenarios.

Branch Gateways to Prisma Access

Aruba Branch Gateways can establish tunnels to one or several Prisma Access nodes (in different regions, as shown in the following figure) to secure user traffic going to public cloud services or to the Internet, thus providing high availability. The solution allows for active-active cloud firewalls.

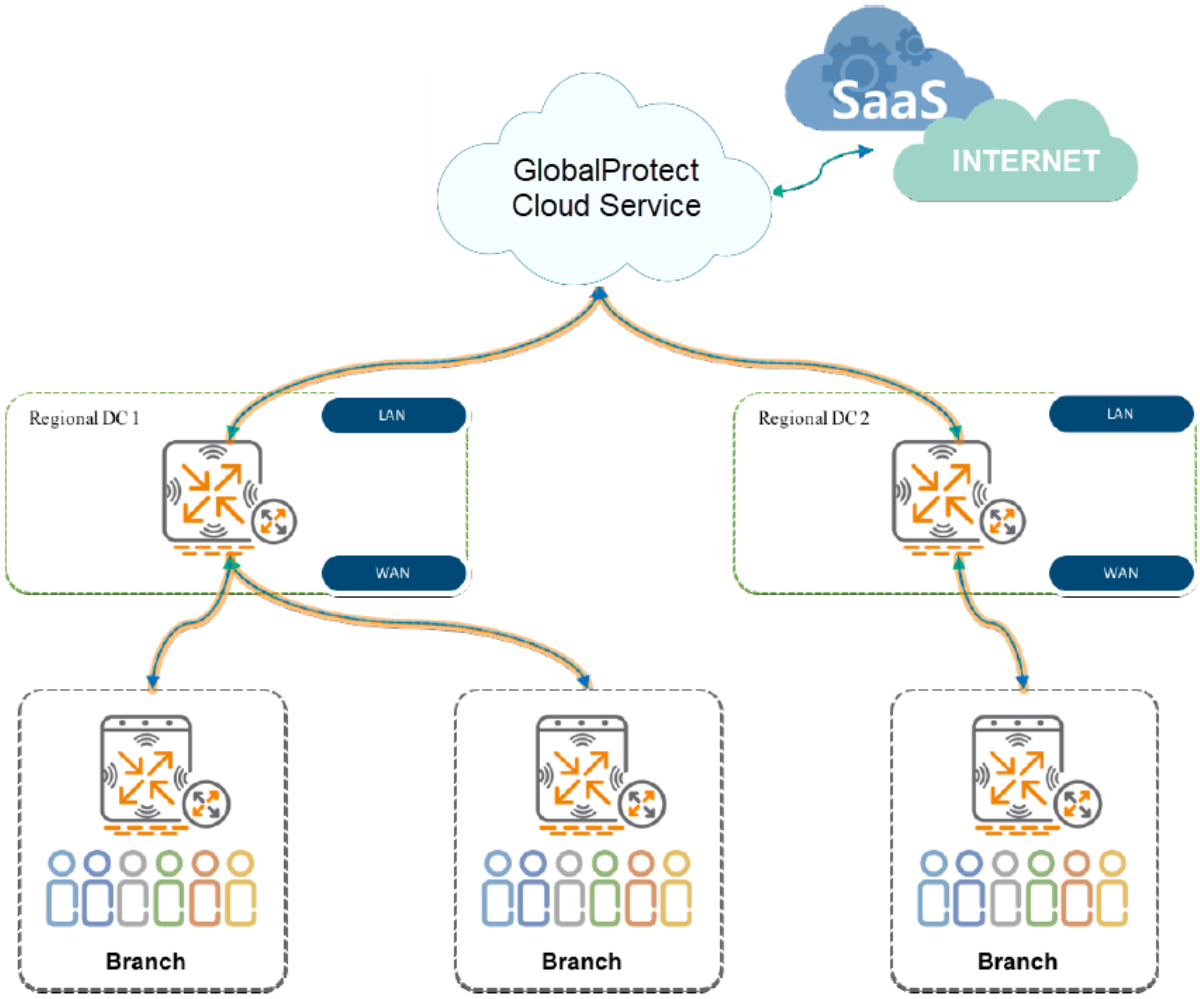
Figure 277 *Branch Gateways to Prisma Access*



Regional Hub to Prisma Access

In certain deployments, the branch traffic is aggregated at a local hub and then routed to the Internet or to other corporate resources. In such scenarios, Aruba VPNCs can set up tunnels to the nearest Prisma Access firewall to allow branch traffic go through the distributed security service as shown in the following figure:

Figure 278 *Regional Hub to Prisma Access*



Supported IKE and IPSec Cryptographic Profiles

The tunnel configuration recommended for this integration are described in the following table:

Table 285: *Tunnel Encryption*

Parameters	Phase 1	Phase 2
Confidentiality	AES-256	AES-256
Integrity	SHA256	SHA1
Authentication	Username/password	N/A
Key Exchange Method	Diffie-Hellman	Diffie-Hellman
Diffie-Hellman Group	14	14
NAT-Transversal	Enabled	N/A
Dead Peer Detection	Enabled	

Parameters	Phase 1	Phase 2
Perfect Forward Secrecy	N/A	Yes
VPN Type	N/A	Policy-based VPN

To know how to enable integration between the Aruba SD-Branch and Prisma Access, see Configuring Prisma Access.

Configuring Prisma Access

To enable integration between the Aruba SD-Branch and Prisma Access, complete the following steps:

- Configuring Prisma Access for Aruba SD-Branch Integration
- Configuring Branch Gateways for Prisma Access Integration

Configuring Prisma Access for Aruba SD-Branch Integration

To configure branch locations, IPsec tunnels, and crypto policies, complete the following steps in the Prisma Access portal:

1. Ensure that you deploy the Panorama VM in your data center.
2. To access the Prisma Access dashboard, install the cloud service plug-in on Panorama.
3. Log in to Prisma Access dashboard and complete the following tasks:
   a. Create IPsec tunnels.
   b. Configure crypto profiles.
   c. Create a branch network in Panorama.
   d. Use route summary to advertise the branch local subnets to Prisma Access.

From the Prisma Accesss dashboard, you can get the IP address of the required cloud service region. This IP address is configured as the peer gateway IP address of the Gateway on .

For more information on planning the cloud service infrastructure and service connection, see Prisma Access documentation.

Configuring Branch Gateways for Prisma Access Integration

Before configuring the Branch Gateways, ensure that the devices can reach the IP address of the selected cloud region on Prisma Access.

Complete the following steps on the Branch Gateway:

1. Configuring IPsec Maps.
2. Configuring Prisma Access Next-hop List .
3. Adding Next-hop List to a Routing Policy .
4. Applying Policies to Roles or VLANs.
5. Verifying Tunnel Status.

Configuring IPsec Maps

To configure an IPsec map for Prisma Access, complete the following tasks:

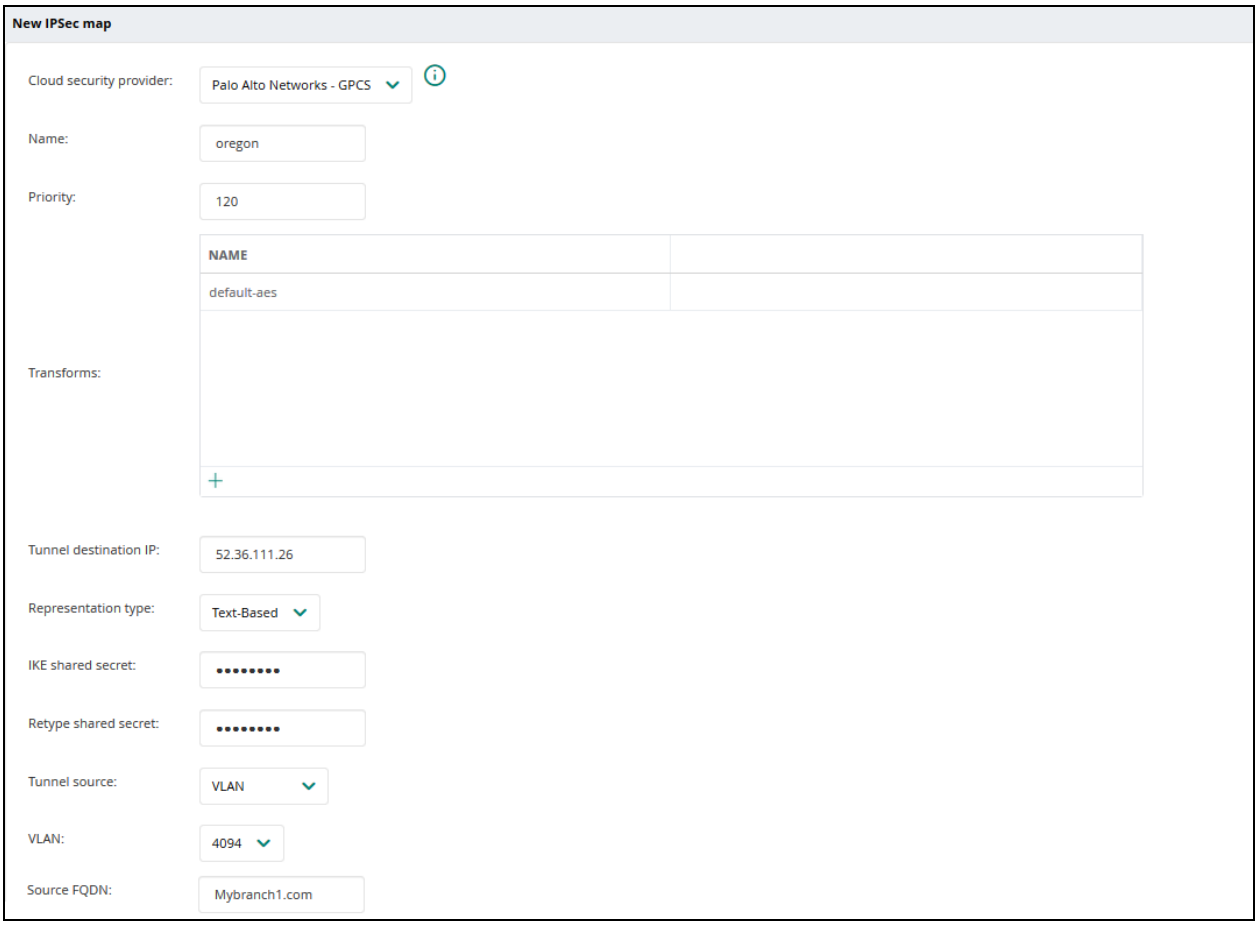
1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **VPN** > **Cloud Security**.
3. In the **IPsec Maps** section, click **+** to open the **New IPsec map** section.
4. Select **Palo Alto Networks - Prisma** as the cloud security provider from the drop-down list.
5. Enter a name for the IPsec map. The allowed character limit is 128.
6. Enter a priority number for the IPsec map within a range of 1 to 10,000. A priority value of 1 indicates the highest priority.
7. Configure a transform set. Transform sets allow you to define a combination of security protocols and algorithms that you can apply to the IPsec traffic flow.
   To add a transform set:
   a. Click **+** under **Transforms**.
   b. Specify the encryption methods to use in the transformation set.
   c. Click **Save Settings**.
8. Enter the IP address of the cloud region elected from the Prisma Access dashboard in the **Tunnel destination IP** field.
9. Select one of the following options in the **Representation** type drop-down list:
   - **Text-Based**
   - **Hex-Based**
10. Enter IKE pre-shared secret key that you configured on the Prisma Access dashboard in the I**KE shared secret** and **Retype shared secret** fields.
11. Select one of the following options for **Tunnel source** as per your configuration requirements.
    - **VLAN**—Select a VLAN from the **VLAN** drop-down list. Select the VLAN to use for bringing up tunnels to Prisma Access (in the case of Branch Gateway) or the source VLAN in the case of VPNCs.

- **Uplink VLAN**—If required, configure a primary and secondary uplink VLAN for the primary and secondary source FQDNs. If multiple uplinks are configured, ensure different priorities are assigned for each uplink when you add a next-hop list.

12. Specify the FQDN of the tunnel source in the **Source FQDN** field. The source FQDN must match the FQDN configured on the Prisma Access. If you want to configure both primary and secondary source FQDNs, ensure that a primary and secondary uplink VLANs are defined.
13. Click **Save Settings**.

The following figure shows an example of cloud security profile configured for Prisma Access:

Figure 279 *IPsec Map for Prisma Access*



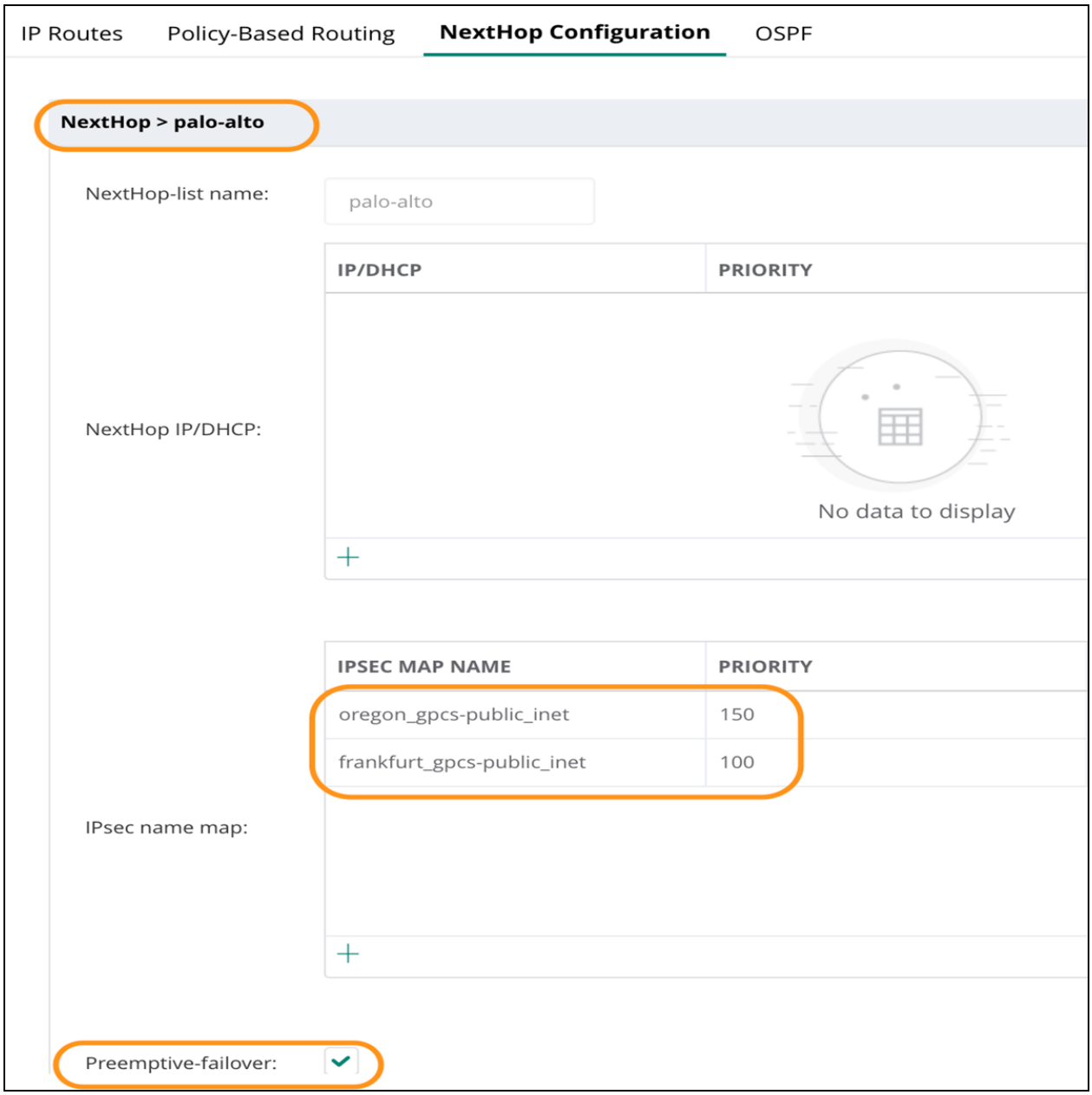
Configuring Prisma Access Next-hop List

Configure a Prisma Access next-hop list with active and standby IPsec tunnels on different uplinks.

When configuring a next-hop list:

- Assign a higher priority for the tunnel that points to the primary node.
- Enable **Preemptive failover**.

Figure 280 *Next-hop List Configuration*



For more information on configuring a next-hop list, see Configuring Next Hop Lists for PBR.

Adding Next-hop List to a Routing Policy

After you configure the next-hop list with the tunnels towards Prisma Access, add the next-hop list to a routing policy.

For more information on creating a routing policy, see Configuring Policies for PBR.

Applying Policies to Roles or VLANs

After creating a routing policy, ensure that you apply this policy to a user role or VLAN. For more information, see Applying Policies to Gateway Interfaces.

Verifying Tunnel Status

To verify the tunnel status:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Overview**.
5. Click **Tunnels**.

For more information, see Gateway > WAN > Tunnels.

You can also view the tunnel status and uplink health in the **Topology** page.

Chapter 23
Integration with Check Point

With more services moving to a cloud-based architecture, one of the most common requirements is to allow SD-branches to route traffic to its intended destination using the Internet. Direct access from branch to the Internet allows faster delivery and efficient use of bandwidth as opposed to tunneling traffic to an aggregation point before routing it to its final destination. However, allowing branch devices to directly connect to the Internet may introduce security issues.

To enhance branch security and provide advanced threat protection, Aruba supports SD-Branch integration with third-party cloud network security services such as Check Point. Check Point Network Security as a Service is a cloud security platform that provides Check Point threat prevention and access control for branch offices. With the Check Point integration, network administrators can connect Aruba Gateway device to Network Security as a Service to leverage Check Point's best-in-class network security services and deploy a secure SD-WAN network.

The SD-Branch integration with Check Point offers the following benefits:

- Unified security management for campus and branch networks
- Context-aware security policies driven by ClearPass
- Intelligent routing of traffic based on user role and application
- Security event logging and monitoring

Supported IKE and IPsec Cryptographic Profiles

The Aruba Branch Gateway and Check Point support several options for setting up VPN tunnels. Aruba and Check Point recommend using IKEv2 for cloud security.

The following encryption settings are recommended for tunnel configuration.

Table 286: *Tunnel Encryption*

Parameters	Phase 1	Phase 2
Confidentiality	AES-256	AES-256
Integrity	SHA1	SHA1
Authentication	Username/password	N/A
Key Exchange Method	Diffie-Hellman	Diffie-Hellman
Diffie-Hellman Group	Group 2	-

Configuration Steps

The SD-Branch integration with Check Point requires configuration the Check Point portal and Aruba Gateways.

Before you begin, perform the following checks:

- The Aruba Gateways are connected to and managed from Aruba Central.
- You have access to the Check Point web portal and administrative credentials to set up tunnels with Aruba Gateways.

To enable Aruba SD-Branch integration with Check Point, complete the following configuration steps:

- Configuring Check Point for SD-Branch Integration
- Configuring Aruba Gateways for Integration with Check Point

Configuring Check Point for SD-Branch Integration

To configure Check Point for SD-Branch integration:

1. Log in to the Check Point Portal.
2. Access Network Security As A Service app.
3. Create a site. The **Create New Site** wizard opens.
4. Enter site details.
5. Select the tunnel type as **IPsec - Pre-Shared Key** and define the external IP address and shared secret key.
6. Set the IP address of the branch site as external IP address and configure subnets for internal networks within a branch site.
7. Confirm site creation.
8. From **the Network Security As A Service** dashboard, select the site you just created and click **View Instructions**.
9. Note the tunnel destination FQDN.

The following figures illustrate the site creation procedure in Check Point portal.

Figure 281 *Site Creation*

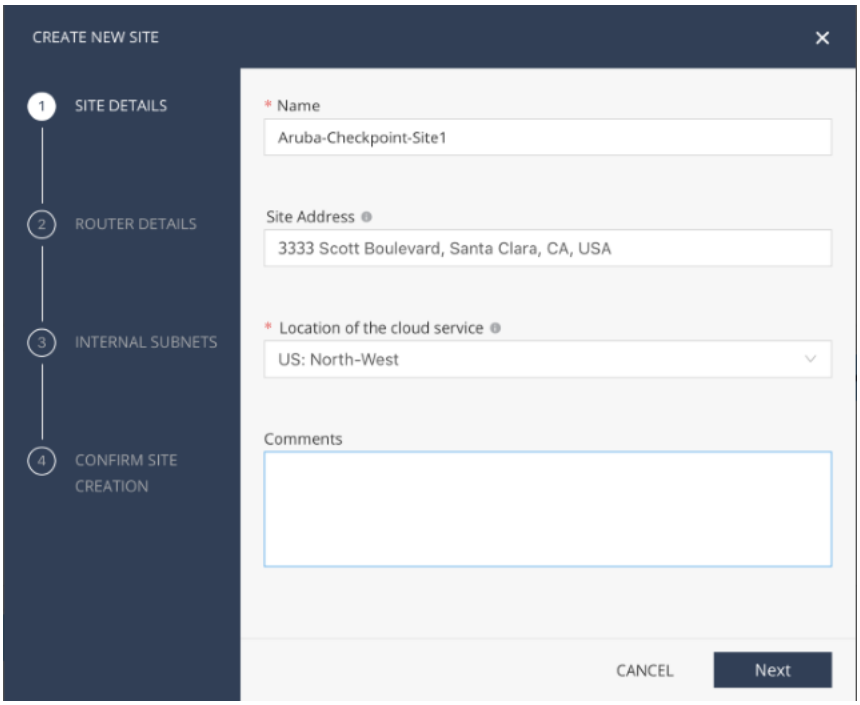


Figure 282 *Tunnel Configuration*

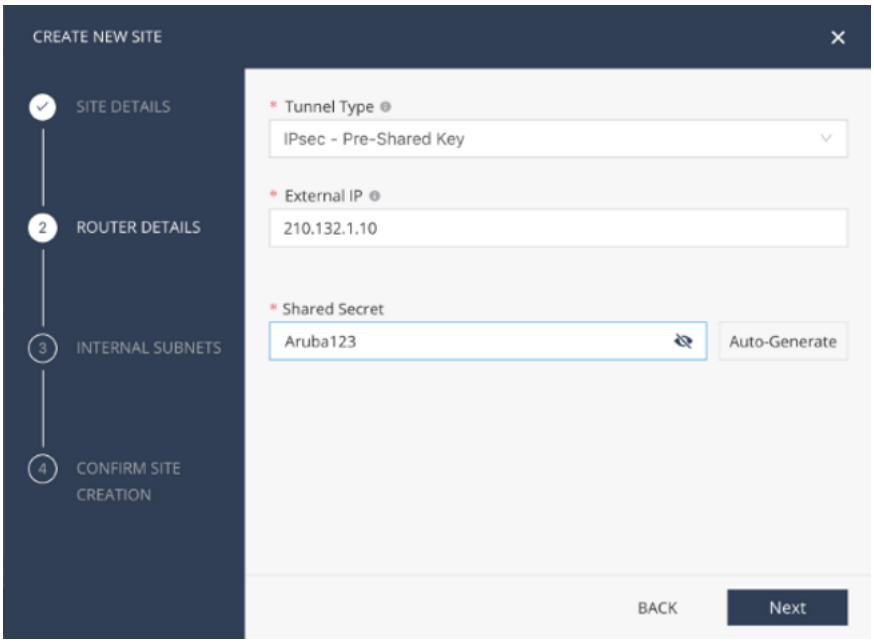


Figure 283 *Subnet Configuration*

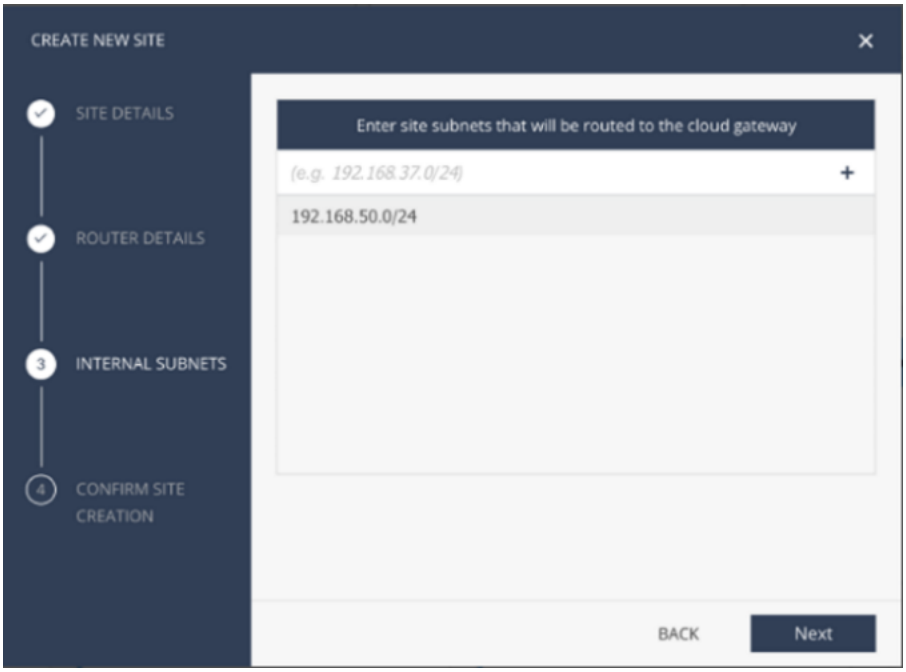
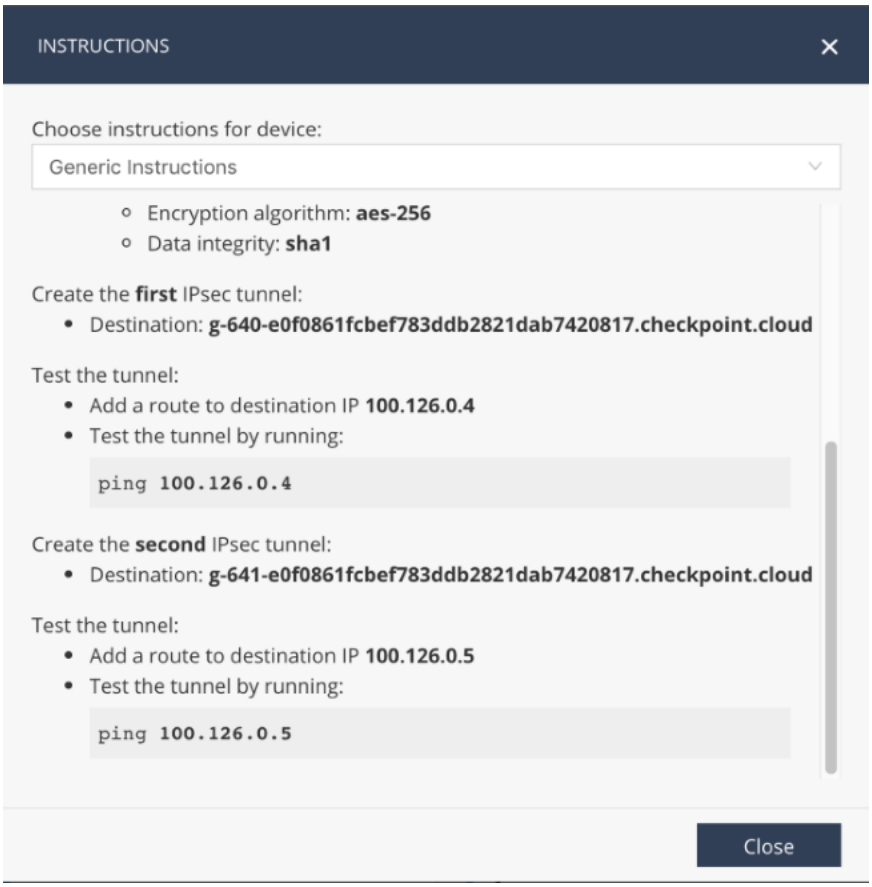


Figure 284 *View Instructions*



Configuring Aruba Gateways for Integration with Check Point

To enable Aruba Gateways to connect to Check Point, complete the following configuration steps:

- Configuring IPsec Tunnels to Check Point
- Adding the Next-hop List to a Routing Policy
- Applying Policies to a Role or VLAN

Configuring IPsec Tunnels to Check Point

To configure an IPsec tunnel to Check Point:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.

- To configure a Branch Gateway or VPNC, complete the following steps:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.
     The gateway device configuration page is displayed.

2. Click **VPN** > **Cloud Security**.
3. In the **IPSec Maps** section, click **+** to open the **New IPSec map** section.
4. Select **Check Point - CloudGaurd Connect** as the cloud security provider from the drop-down list.
5. Enter a name for the IPsec map. The allowed character limit is 128.
6. Enter a priority number for the IPsec map within a range of 1 to 9998. A priority value of 1 indicates the highest priority.
7. Configure the **default-aes** transform. Transform sets allow you to define a combination of security protocols and encryption settings that you can apply to the IPsec traffic flow.

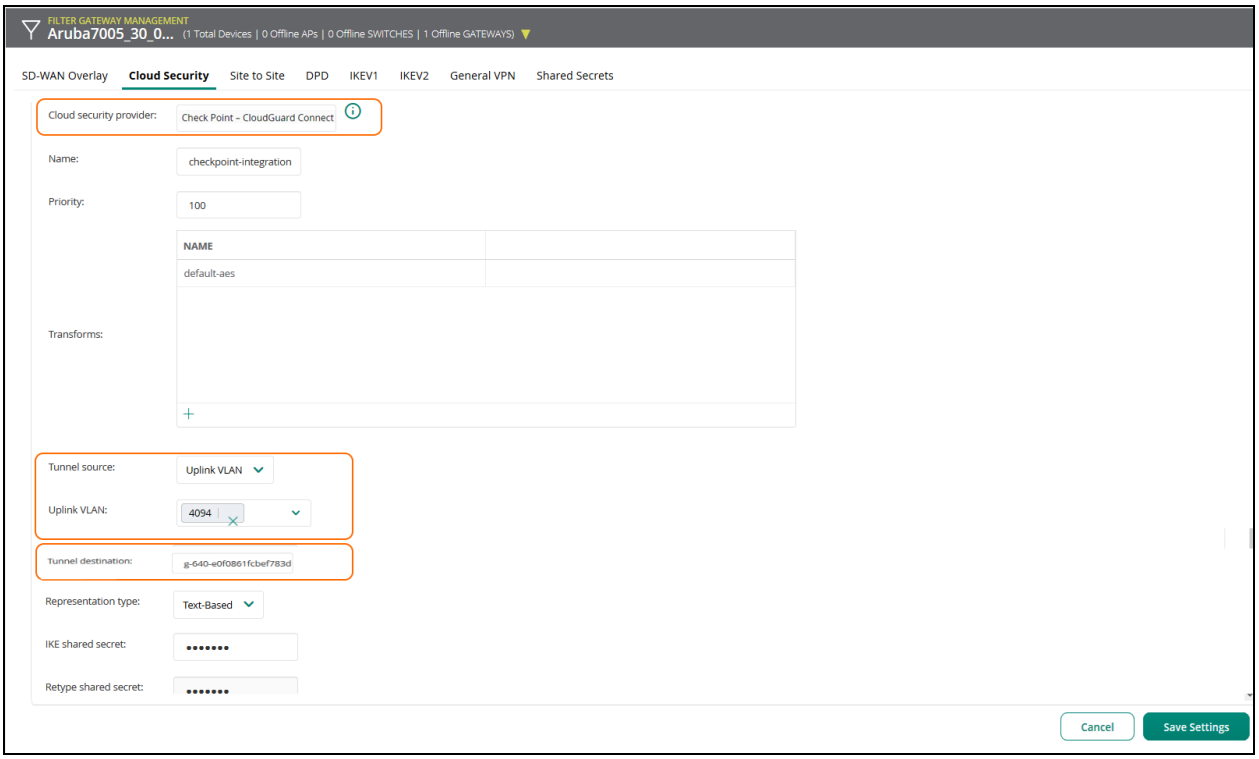
   To add a transform set:
   a. Click **+** under **Transforms**.
   b. From the available transforms set, select **default-aes**. The **default-aes** transform uses AES 256 encryption with SHA1 Hash.
   c. Click **Save Settings**.
8. Select one of the following options in **Tunnel source** based on your requirement. Select the Uplink VLAN to use for bringing up tunnels to Check Point (in the case of Branch Gateway) or the source VLAN in the case of VPNCs.
   - **VLAN**—Select a VLAN from the **VLAN** drop-down list.
   - **Uplink VLAN**—Select an uplink VLAN from the **Uplink VLAN** drop-down list.

Ensure that you assign different priorities for different uplinks in the next-hop list configuration.

9. In the **Tunnel destination** field, specify the FQDN address of the branch site configured in Check Point to which the tunnel will be established.
10. Select one of the following options in the **Representation** type drop-down list:
    - **Text-Based**
    - **Hex-Based**
11. In the **IKE shared secret**, field, enter the IKE pre-shared secret key that you configured on the Check Point portal and retype the secret key to confirm.

The following figure shows the sample configuration values:

Figure 285 *Checkpoint Configuration*



1. Click **Save Settings**.
2. Repeat steps 1 through 13 to add a secondary IPsec tunnel.

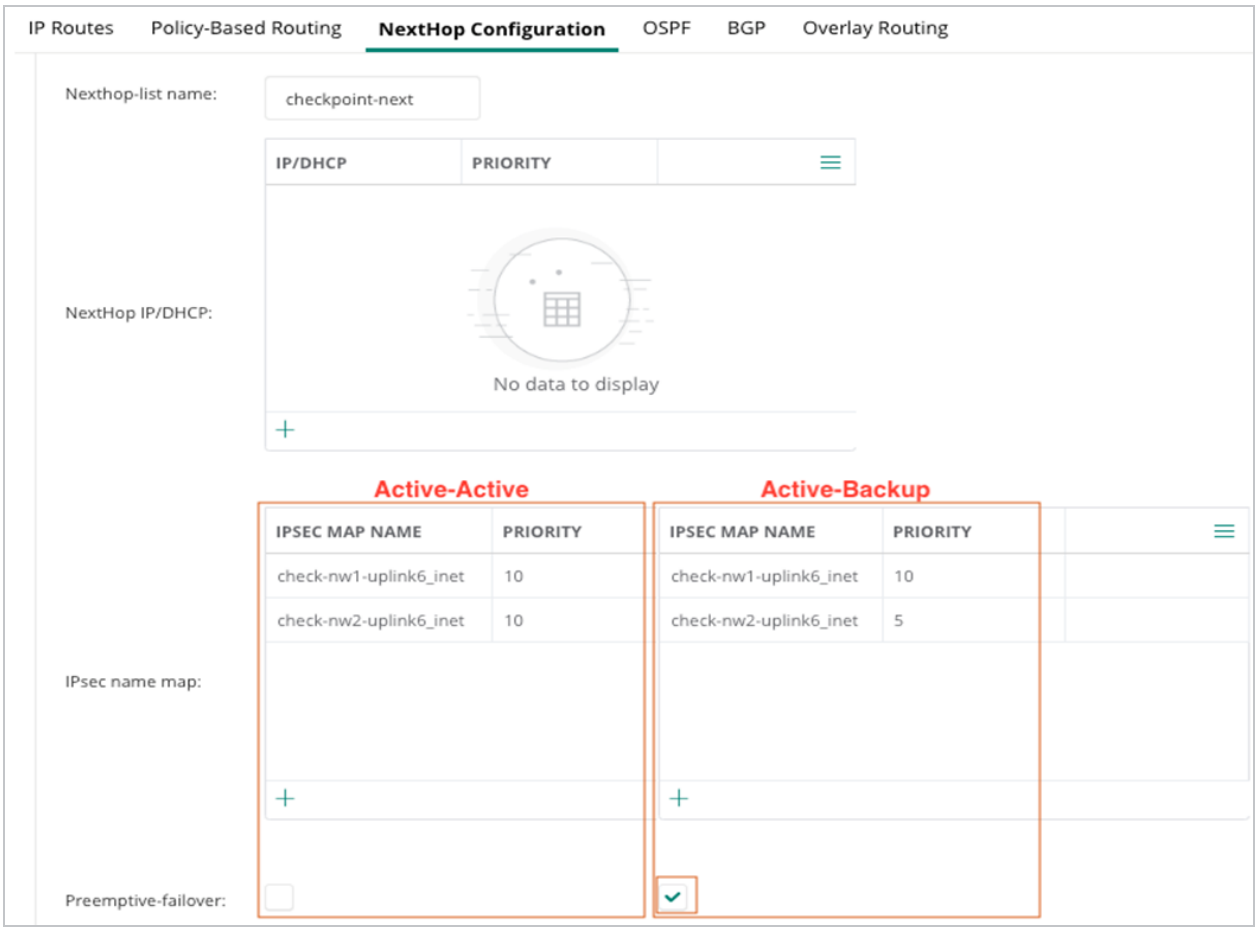
Configuring a Next-hop List

After configuring the tunnels, you can create a next-hop list to group the tunnels inside a routing policy.

Note the following points for next-hop list configuration:

- If you want to use both (primary and secondary) IPsec tunnels in the Active-Active mode, assign the same priority for the tunnels.
- If you want to use the tunnels in the Active-Standby mode, assign a higher priority for the tunnel that points to the primary node and enable **Preemptive failover**.

Figure 286 *Next-hop Configuration*



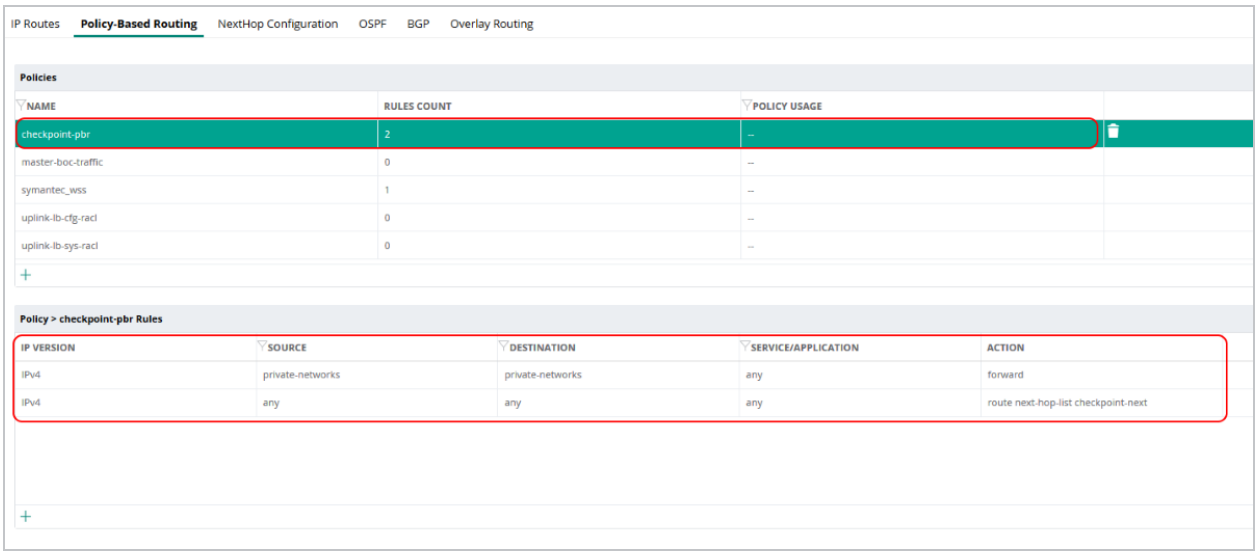
For more information, see Configuring Next Hop Lists for PBR.

Adding the Next-hop List to a Routing Policy

After creating the next-hop list, you must add the next-hop list to a routing policy.

In the example shown in the following figure, the policy is sending all the traffic to private subnets through the regular path and the rest of the traffic through the Check Point nodes.

Figure 287 *Routing Policy for Check Point*



For more information on adding a next-hop list to a global routing policy, see Configuring Policies for PBR.

Applying Policies to a Role or VLAN

After you configure a routing policy, apply it to a role or VLAN.

The following figures illustrate the procedure for configuring a Check Point role and applying routing policies to a role and VLAN:

Figure 288 *Apply Check Point Routing Policy to a Role*

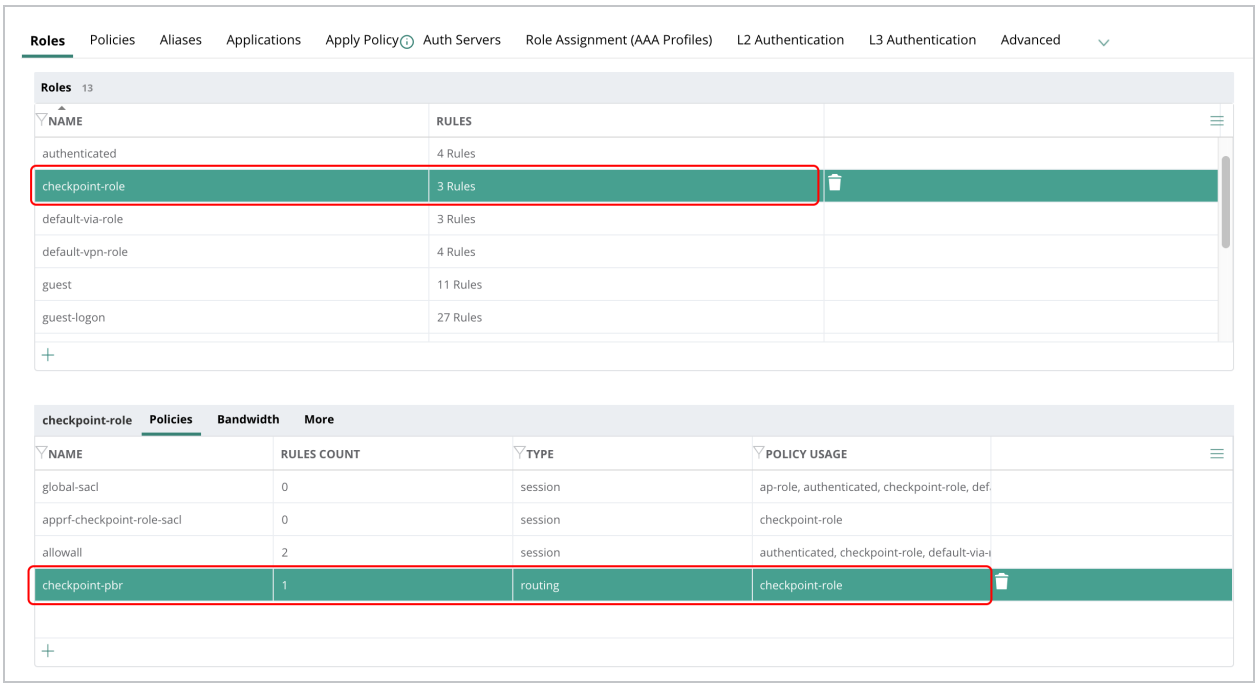
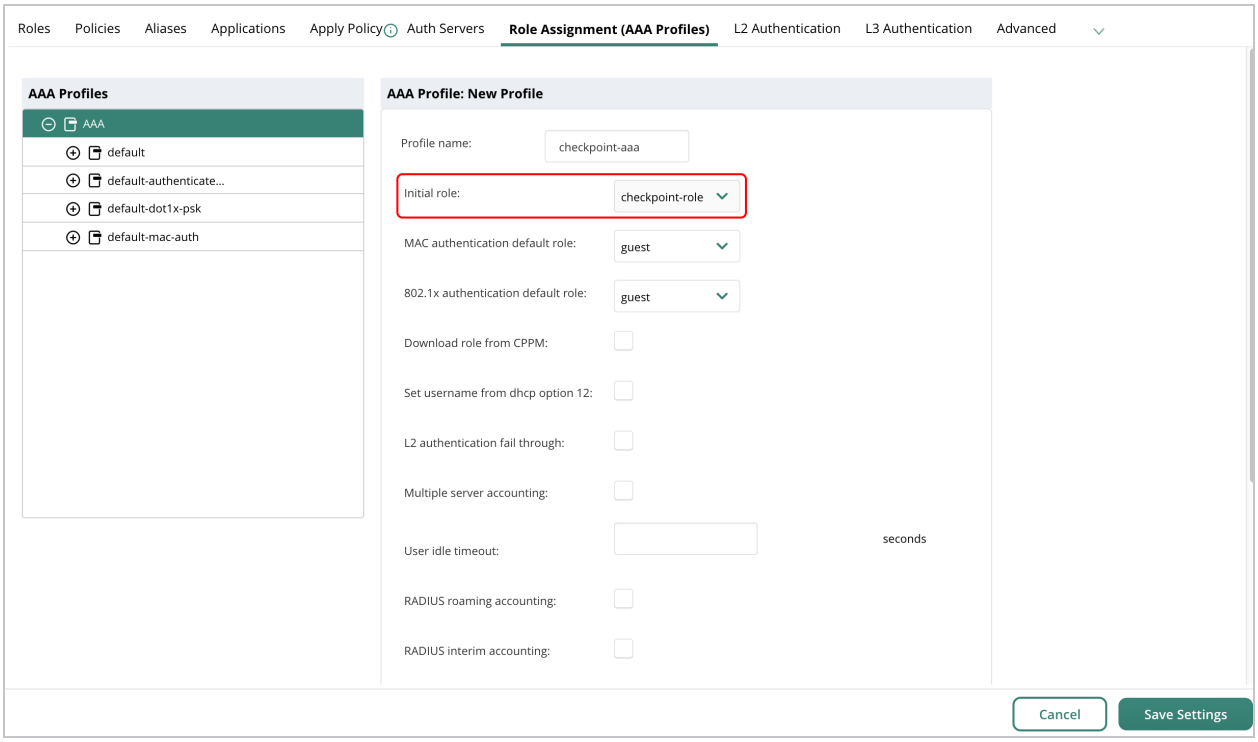
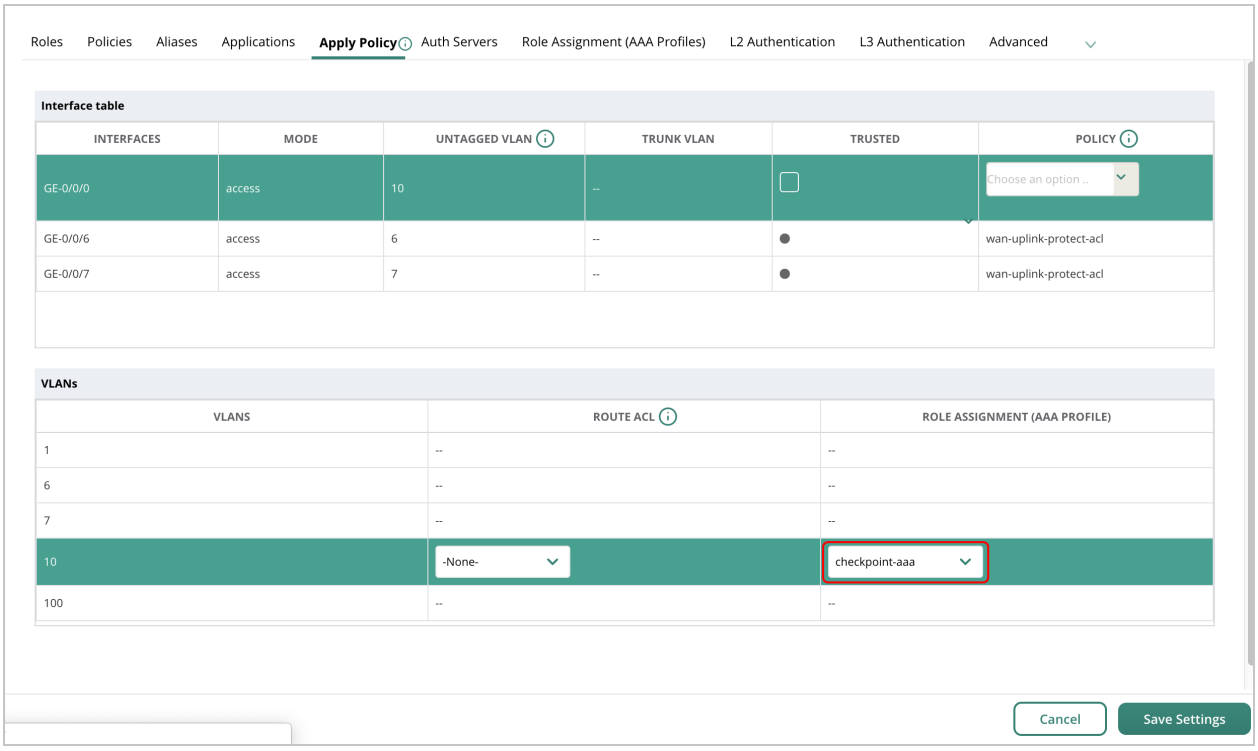


Figure 289 *Apply Routing Policy to VLAN*





For more information, see Applying Policies to Gateway Interfaces.

Verifying Tunnel Status

To verify the tunnel status:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, click **Overview**.
5. Click **Tunnels**.

For more information, see Gateway > WAN > Tunnels.

You can also view the tunnel status and uplink health in the **Monitoring & Reports** > **Topology** page.

Chapter 24
Integration with Symantec WSS

With more services moving to a cloud-based architecture, one of the most common requirements is to allow SD-branches to route traffic to its intended destination using the Internet. Direct access from branch to the Internet allows faster delivery and efficient use of bandwidth as opposed to tunneling traffic to an aggregation point before routing it to its final destination. However, allowing branch devices to directly connect to the Internet may introduce security issues.

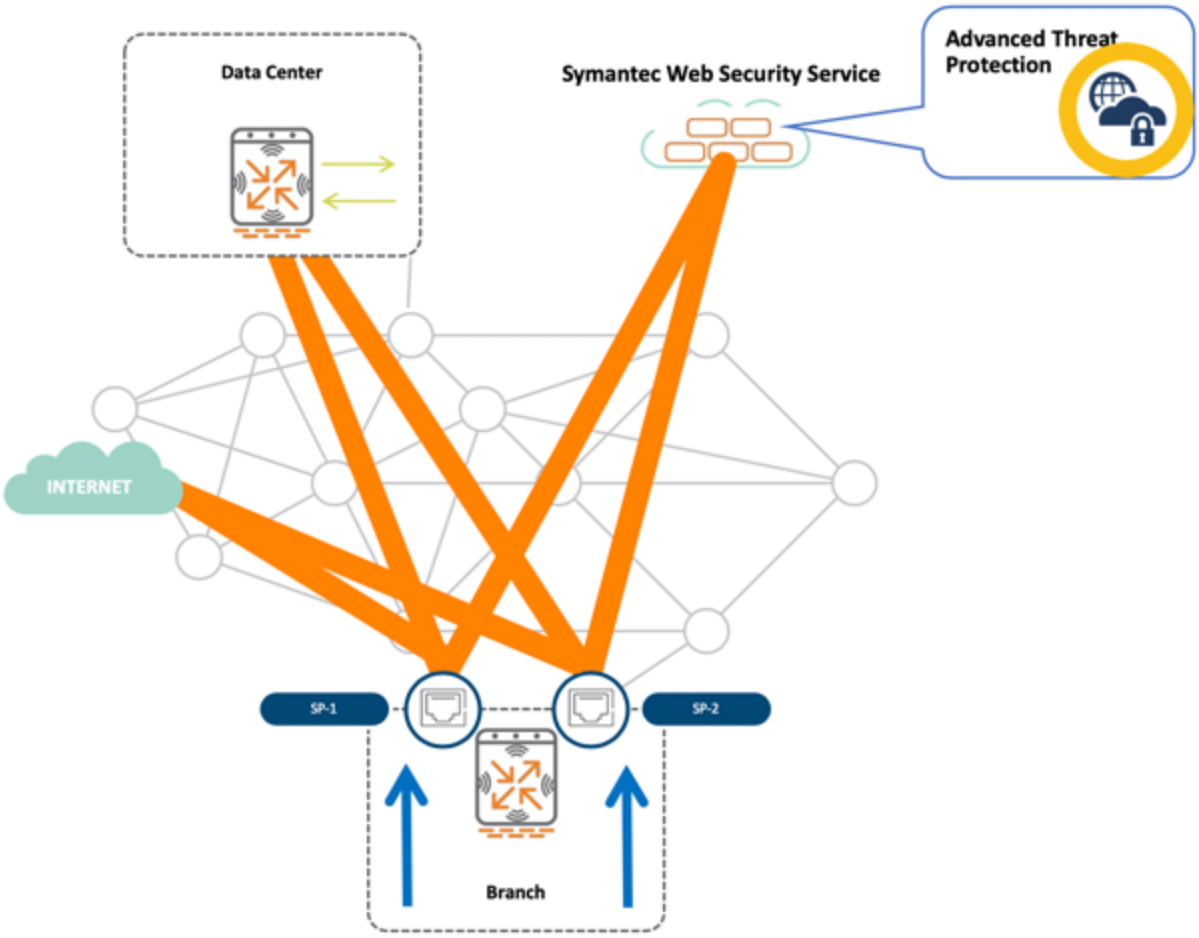
To enhance branch security and provide advanced threat protection, Aruba supports SD-Branch integration with third-party cloud security and firewall services such as Symantec Web Security Service (WSS).

Integration Overview

The integration between the Aruba Branch Gateway and Symantec WSS allows network administrators to set up a secure connection between an SD-Branch and one or several cloud-hosted enforcement points. Branch Gateways can establish secure tunnels to the WSS firewall and redirect selected traffic flows through WSS and leverage advanced threat protection, such SSL decryption, malware inspection, web isolation and enforce Data Loss Prevention (DLP), in an efficient and scalable way.

The following figure illustrates SD-Branch integration with Symantec Web Security Service:

Figure 290 *Figure 2 - SD-Branch integration with Symantec Web Security Service*



The SD-Branch integration with Symantec WSS offers the following benefits:

- Unified security management for campus and branch networks
- Context-aware security policies driven by ClearPass
- Intelligent routing of traffic based on user role and application

  The integration also allows SD-Branch users to leverage the benefits of the advanced threat protection:

  URL Filtering and categorization

  Malware analysis

  Anti-virus

  Web isolation

  Cloud Access Security Broker (CASB)

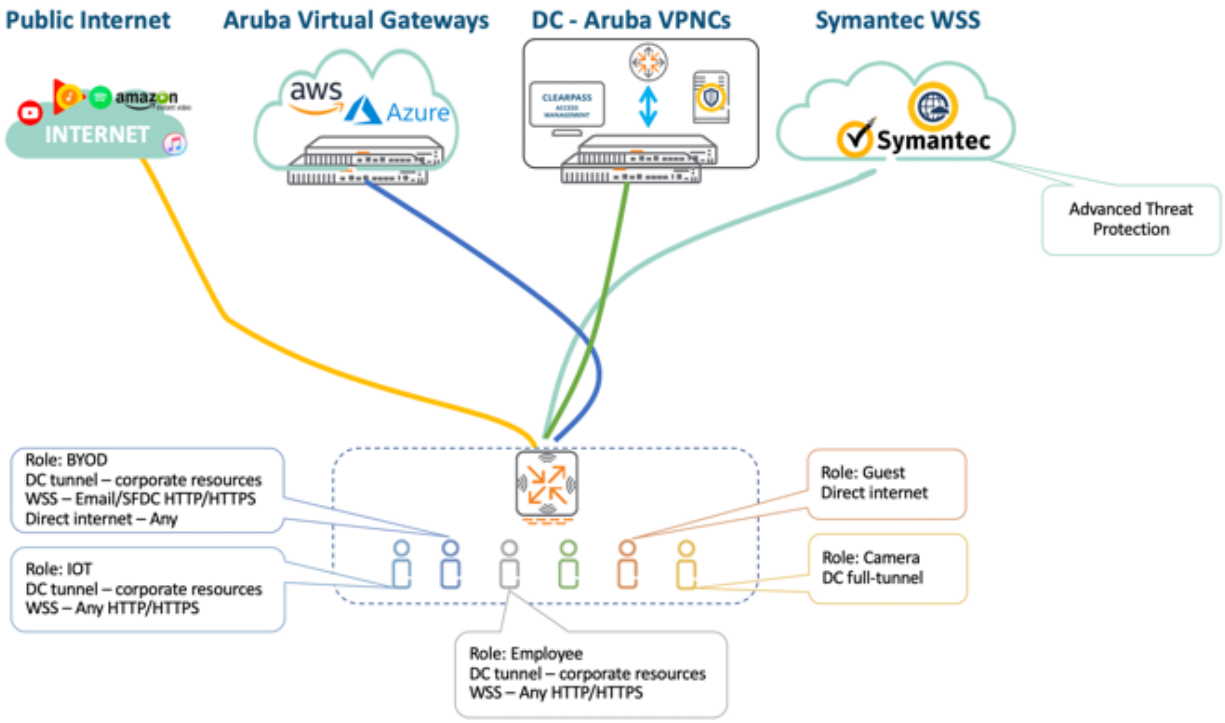
  Data Loss Prevention

Role-Based and Application-Based Routing

Aruba Branch Gateway function as stateful firewalls with support for web content, reputation and geolocation filtering. This means that it can selectively determine which traffic needs to be routed through WSS.

For example, security policies for guest users generally require content and reputation filtering, and other devices like printers or network cameras may not need to reach out to the Internet. At the same time, traffic to trusted cloud services like streaming providers may not require the additional security of an advanced threat protection engine.

Figure 291 *Figure 3 - Role-Based and Application-Based Routing*



The following parameters can be taken into consideration when determining which traffic types are to be sent through WSS:

- VLAN/User Role—PBR policies can be applied to roles or VLANs
- Application/Application Category
- Stateful policies with protocol, source/destination address, source/destination port, and DSCP parameters
- FQDN—ArubaOS supports creating **netservices** based on FQDN, which can be used to build PBR policies

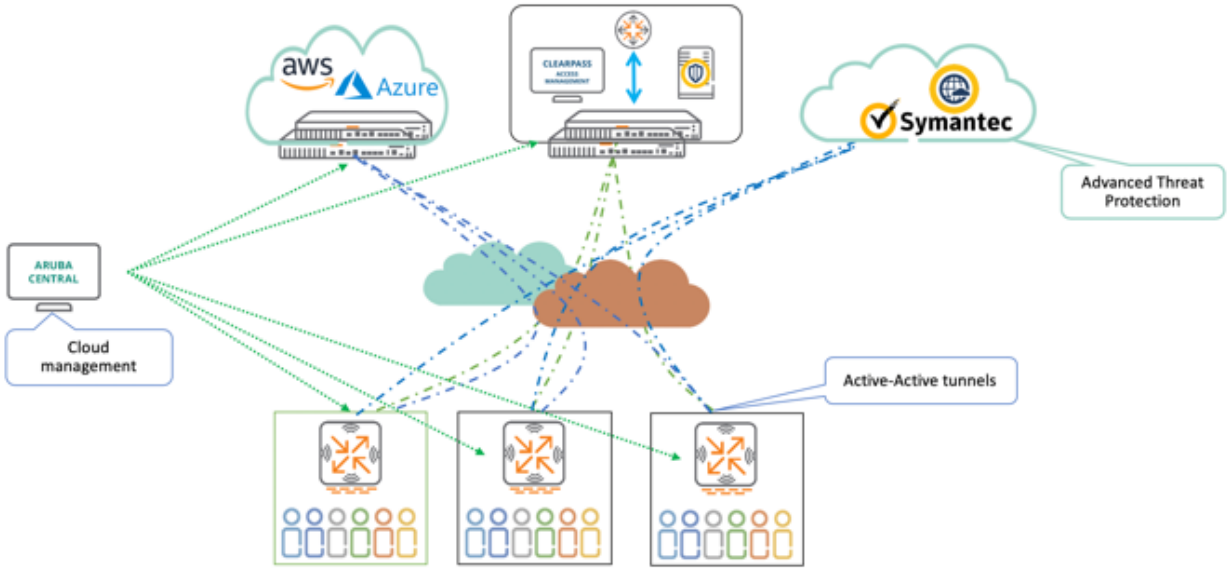
Branch Gateway to WSS

The Aruba SD-Branch WSS integration allows branches to securely connect to various WSS datacenter locations and sending HTTP and HTTPS traffic of users to Symantec for further inspection.

Branch Gateways an establish tunnels to one or several WSS datacenter locations to secure user traffic going to public cloud services or to the Internet.

The solution allows for active-active cloud firewalls as shown in the following figure:

Figure 292 *Figure 4 - Active-Active Firewall Regions*



For a complete list of available DC locations and their IP addresses, see https://support.symantec.com/en_US/article.TECH242979.html.

Supported IKE and IPSec Cryptographic Profiles

The Aruba Branch Gateway and WSS support several options for setting up VPN tunnels.

The tunnel configuration recommended for this integration are described in the following table:

Table 287: *Tunnel Encryption*

Parameters	Phase 1	Phase 2
Confidentiality	AES-256	AES-256
Integrity	SHA256	SHA1
Authentication	Username/password	N/A
Key Exchange Method	Diffie-Hellman	Diffie-Hellman
Diffie-Hellman Group	14	14
NAT-Transversal	Enabled	N/A
Dead Peer Detection	Enabled	
Perfect Forward Secrecy	N/A	Yes
VPN Type	N/A	Policy-based VPN

To know how to enable Aruba SD-Branch integration with WSS, see Configuring Symantec WSS.

Configuring Symantec WSS

To enable Aruba SD-Branch integration with WSS, the following steps are required:

- Configuring Web Security Service for SD-Branch Integration .
- Configuring Aruba Gateways for Integration with WSS.

Configuring Web Security Service for SD-Branch Integration

The Web Security Service is managed and configured through the UI or APIs. The configuration steps described in this section follow the UI-based workflows.

Before you begin, ensure that you are a registered user of the Web Security Service portal with administrative privileges.

The Web Security Service configuration includes the following steps:

- Creating IPSec and IKE Crypto Profiles
- Configuring IPsec Tunnels to WSS
- Adding Branch Sites to WSS Datacenters
- Configuring an Authentication Policy (Optional)

Creating IPSec and IKE Crypto Profiles

Symantec Web Security Service supports the crypto profile that Aruba uses by default. For more information, see https://portal.threatpulse.com/docs/am/reference/ref-ike-proposals.htm.

Adding Branch Sites to WSS Datacenters

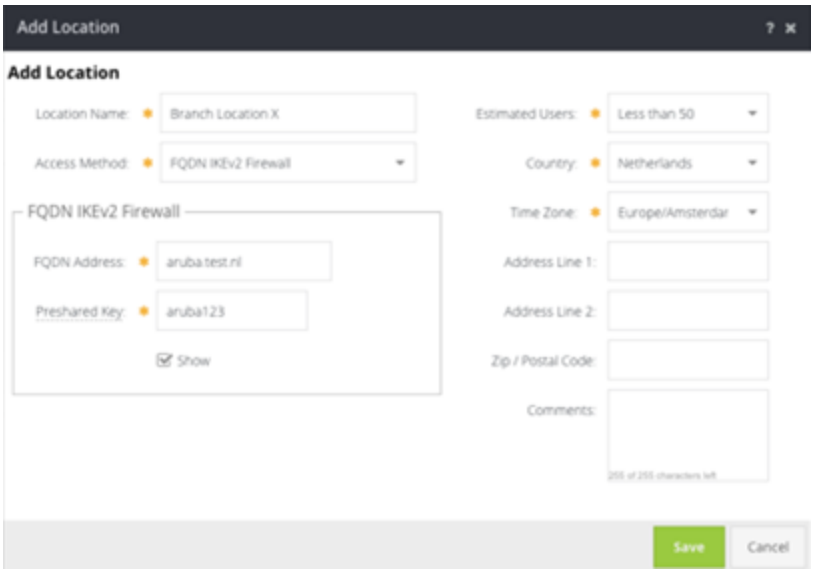
To allow Aruba branches to connect to WSS, you must add branch locations in WSS.

To add a branch site to WSS:

1. Log in to the WSS portal.
2. Go to **Service** > **Network** > **Locations**. The **Locations** page opens and displays a list of sites that are already configured and the VPN connection status indicators for these sites.
3. To add branch location, click **+ Add Location**.
4. In the **FQDN IKEv2 Firewall** section, enter the FQDN address of the branch location and the pre-shared key.
5. Click **Save**.

The following figure illustrates how to add a branch to WSS Datacenter.

Figure 293 *Adding a Branch location to a WSS Datacenter*



Configuring an Authentication Policy (Optional)

When traffic from the branch is sent over to WSS, traffic can be inspected transparently, or SAML authentication can be used to leverage DLP and CASB services. If an authentication policy is configured, WSS identifies the user and device. Administrators can also use a software client on the device to authenticate a user.

If the users have installed Symantec root CA certificate and Branch Gateways forward HTTP and HTTPS traffic, SSL interception will be effective upon adding a branch location in WSS. However, you can configure custom authentication profile to enable role-based policies in WSS. For example, administrators can perform web isolation for all HR management and Finance employees and only perform web category filtering for IOT devices. Authentication can be performed by a software client, the Symantec Endpoint Client with or without SAML authentication.

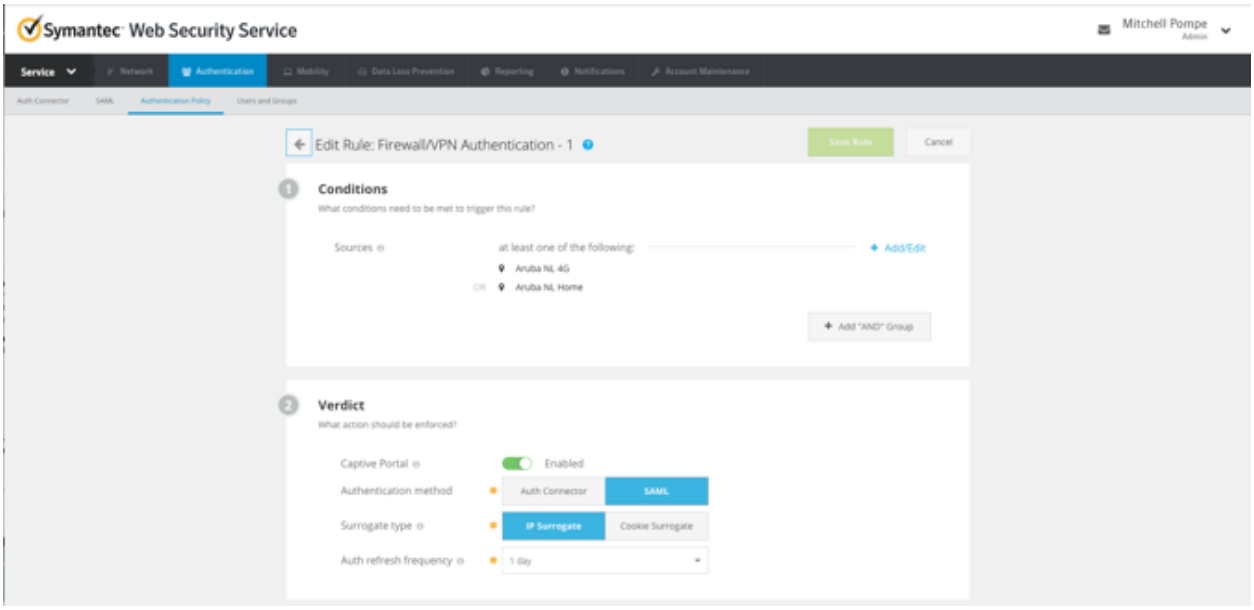
For SAML authentication, the traffic through TCP port 8443 must be routed through WSS as well, besides TCP 80 and TCP 443 ports.

To configure an authentication policy:

1. In the WSS portal, go to **Service** > **Authentication** > **Authentication Policy** > **Location Policy** > **Firewall/VPN Authentication**.
2. Configure an authentication profile.

The following figure shows an example for the authentication method configuration.

Figure 294 *Authentication Policy*



1. Click **Save Rule**.

Configuring Aruba Gateways for Integration with WSS

To enable Aruba Gateways to connect to WSS, the following configuration is required:

- Configuring IPsec Tunnels to WSS
- Configuring a Next-hop List
- Adding the Nexthop List to PBR Policy
- Applying Policies to a Role or VLAN

Configuring IPsec Tunnels to WSS

To configure an IPsec tunnel to WSS:

1. To configure a Branch Gateway group or Branch Gateway complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.

d. Under **Manage**, click **Device**.

The gateway device configuration page is displayed.

2. Click **VPN** > **Cloud Security**.
3. In the **IPSec Maps** section, click **+** to open the **New IPSec map** section.
4. Select **Symantec WSS** as the cloud security provider from the drop-down list.
5. Enter a name for the IPsec map. The allowed character limit is 128.
6. Enter a priority number for the IPsec map within a range of 1 to 10,000. A priority value of 1 indicates the highest priority.
7. Configure a transform set. Transform sets allow you to define a combination of security protocols and algorithms that you can apply to the IPsec traffic flow.

   To add a transform set:
   a. Click **+** under **Transforms**.
   b. From the available transforms set, select **default-aes**. The **default-aes** transform uses AES 256 encryption with SHA1 Hash.
   c. Click **Save Settings**.
8. Select one of the following options in **Tunnel source** based on your requirement. Select the Uplink VLAN to use for bringing up tunnels to WSS (in the case of Branch Gateway) or the source VLAN in the case of VPNCs.
   - **VLAN**—Select a VLAN from the **VLAN** drop-down list.
   - **Uplink VLAN**—Select an uplink VLAN from the **Uplink VLAN** drop-down list.

Ensure that you assign different priorities for different uplinks in the next-hop list configuration.

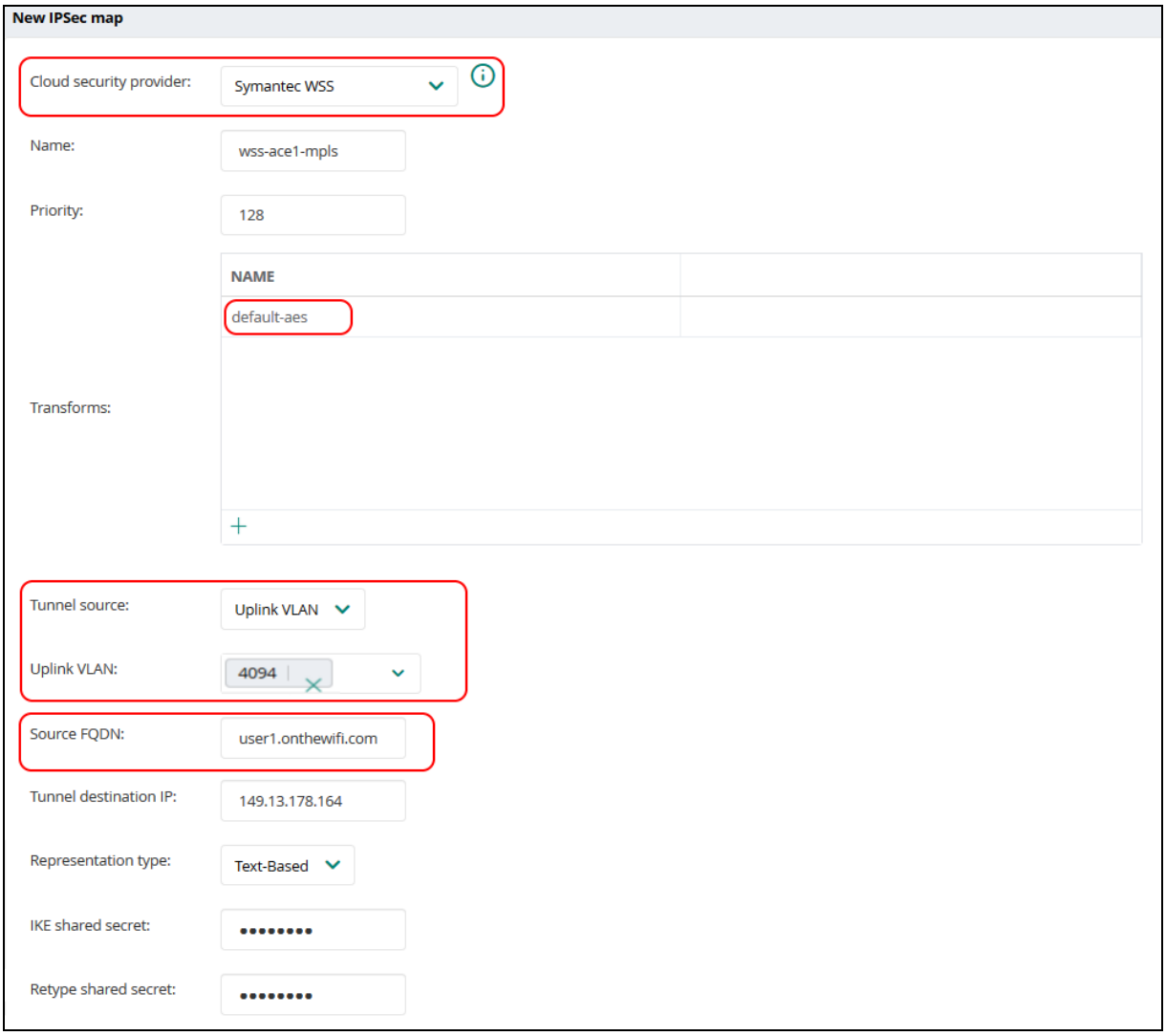
9. Enter the FQDN of the tunnel source in the **Source FQDN** field. The source FQDN must match the FQDN configured on the WSS portal.

The source FQDN is unique for each branch location.

10. In the **Tunnel destination IP** field, specify the IP address of the branch location configured in WSS to which the tunnel will be established.
11. Select one of the following options in the **Representation** type drop-down list:
    - **Text-Based**
    - **Hex-Based**
12. In the **IKE shared secret**, field, enter the IKE pre-shared secret key that you configured on the WSS portal and retype the secret key to confirm.

    The following figure shows the sample configuration values:

Figure 295 *Symantec WSS Configuration*



13. Click **Save Settings**.

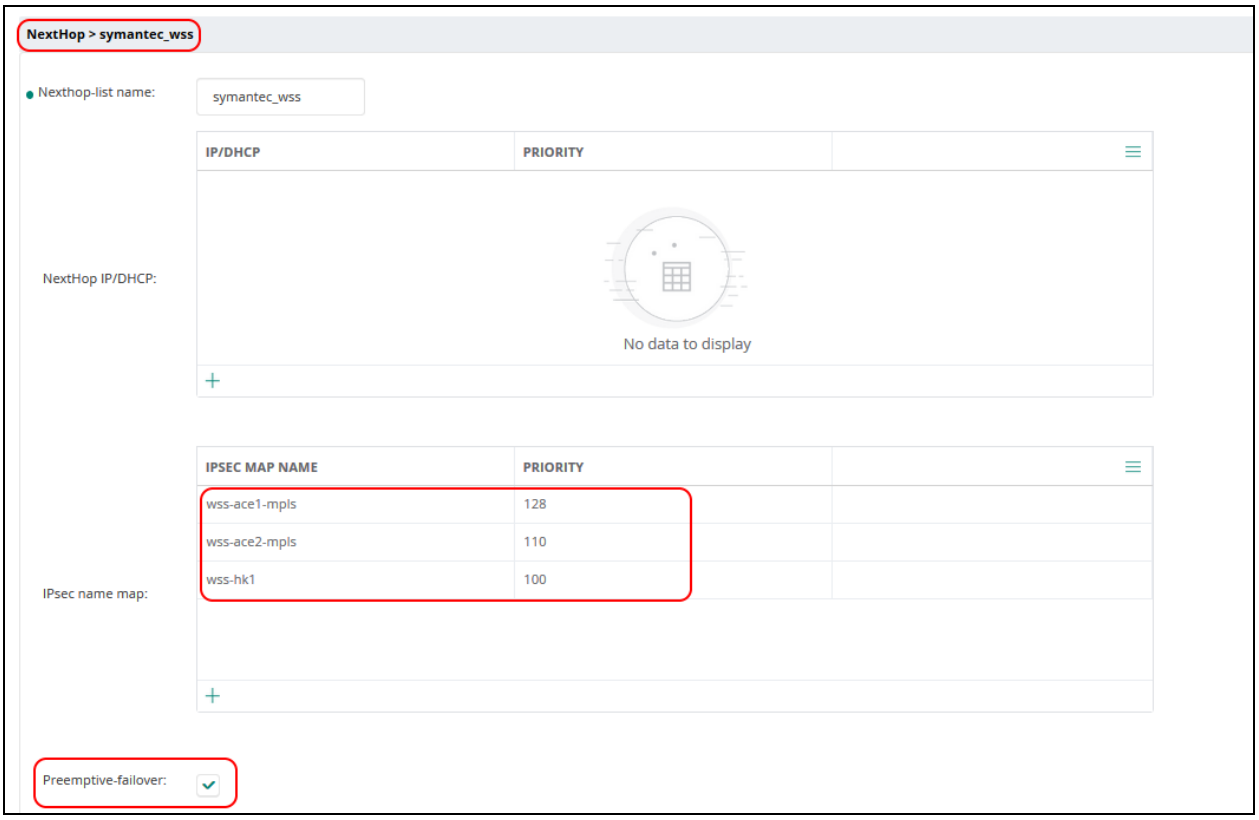
Configuring a Next-hop List

After configuring the tunnels, you can create a next-hop list to group the tunnels inside routing policies. For more information, see Configuring Next Hop Lists for PBR.

When creating a next-hop list:

- Ensure that different priorities are assigned for the tunnels.
- Ensure that **Preemptive failover** is enabled.

Figure 296 *Creating a Next-hop list for Symantec WSS*



Adding the Nexthop List to PBR Policy

After creating the next-hop list, you must add the next-hop list to a routing policy. For more information on adding a next-hop list to a global routing policy, see Configuring Policies for PBR.

In the example shown in the following figures, the routing policy sends all traffic to private subnets (an alias representing 10.0.0.0/8 and 172.16.0.0/12) through the regular path, and all the web traffic to the WSS nodes, and the remaining traffic through the regular ISP lines.

Figure 297 *Creating a Symantec WSS Alias for Web Ports*

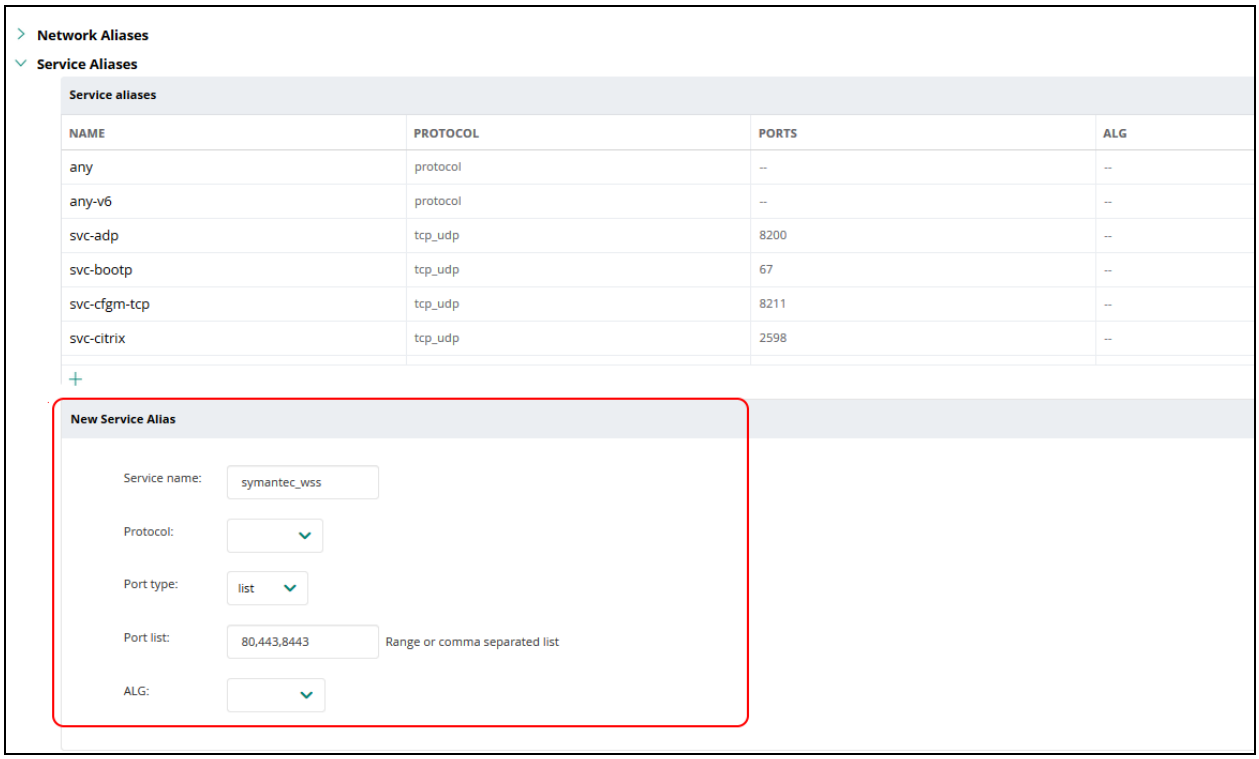
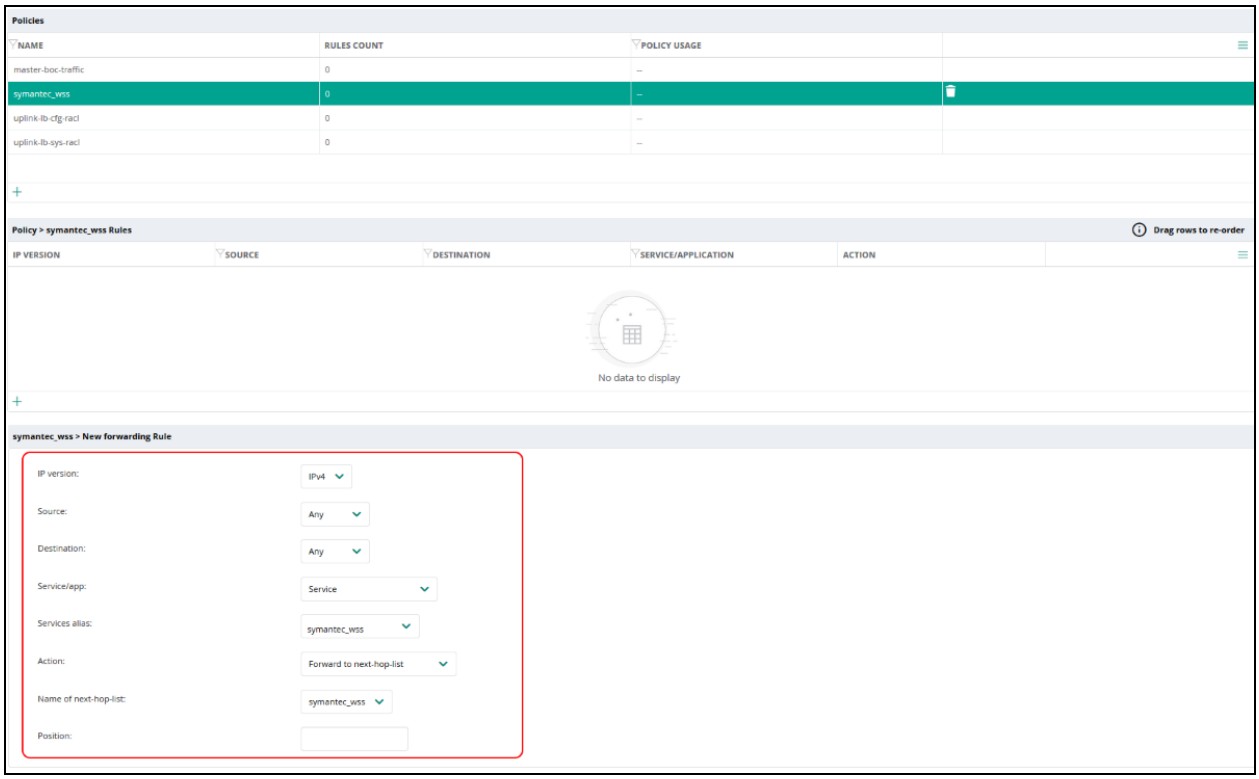


Figure 298 *Routing Policies*



Applying Policies to a Role or VLAN

After you configure a routing policy, apply it to a role or VLAN. For more information, see Applying Policies to Gateway Interfaces.

Verifying Tunnel Status

1. To view the tunnel status on a gateway:
   - In the **Network Operations** app, use the filter to select the gateway.
   - Under **Manage**, click **Overview**.
2. Click **Tunnels**.

For more information, see Gateway > WAN > Tunnels.

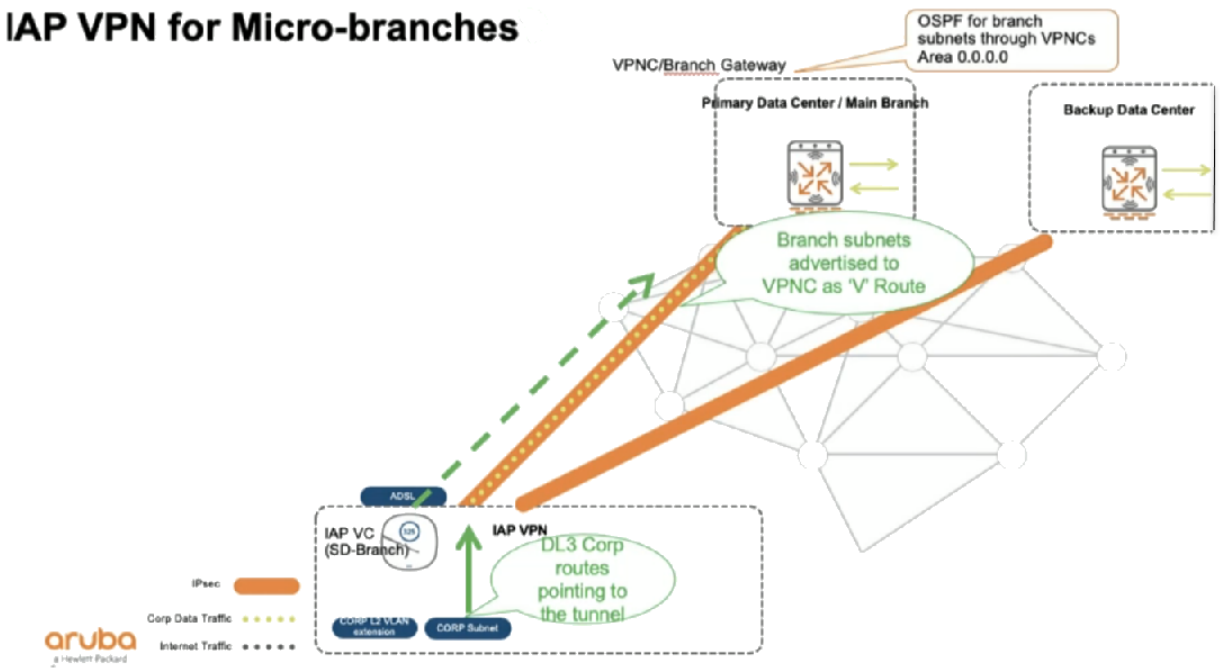
This section describes the high availability (HA) and redundancy features of a Micro Branch. HA is a critical feature in a network to minimize downtime and provide continuous access to systems and applications. Aruba SD-Branch solution provides different types of redundancy in a Micro Branch, based on the size and requirement. In a typical Micro Branch setup, Instant APs (IAP) are deployed at the branch site and VPNCs are deployed at the corporate site or data center.

NOTE

Aruba Micro Branch solution also supports VPNCs deployed in Public Cloud environments such as AWS and Microsoft Azure.

The following image illustrates a Micro Branch with one IAP at the branch and two data centers (primary and backup). In this Micro Branch, the IAP is the Branch Gateway for the entire branch network including both wired and wireless clients. Based on the policies configured, overlay traffic (corporate traffic) is routed through the IPsec tunnels to ensure security while underlay traffic is routed through the WAN uplinks.

Figure 299 *Basic Micro Branch Topology*



Supported Topologies

The following sections explain the different types of topologies that are supported by Aruba to provide high availability in a Micro Branch.

- **Micro Branch with VPNC and WAN Redundancy (L2 Redundancy)**

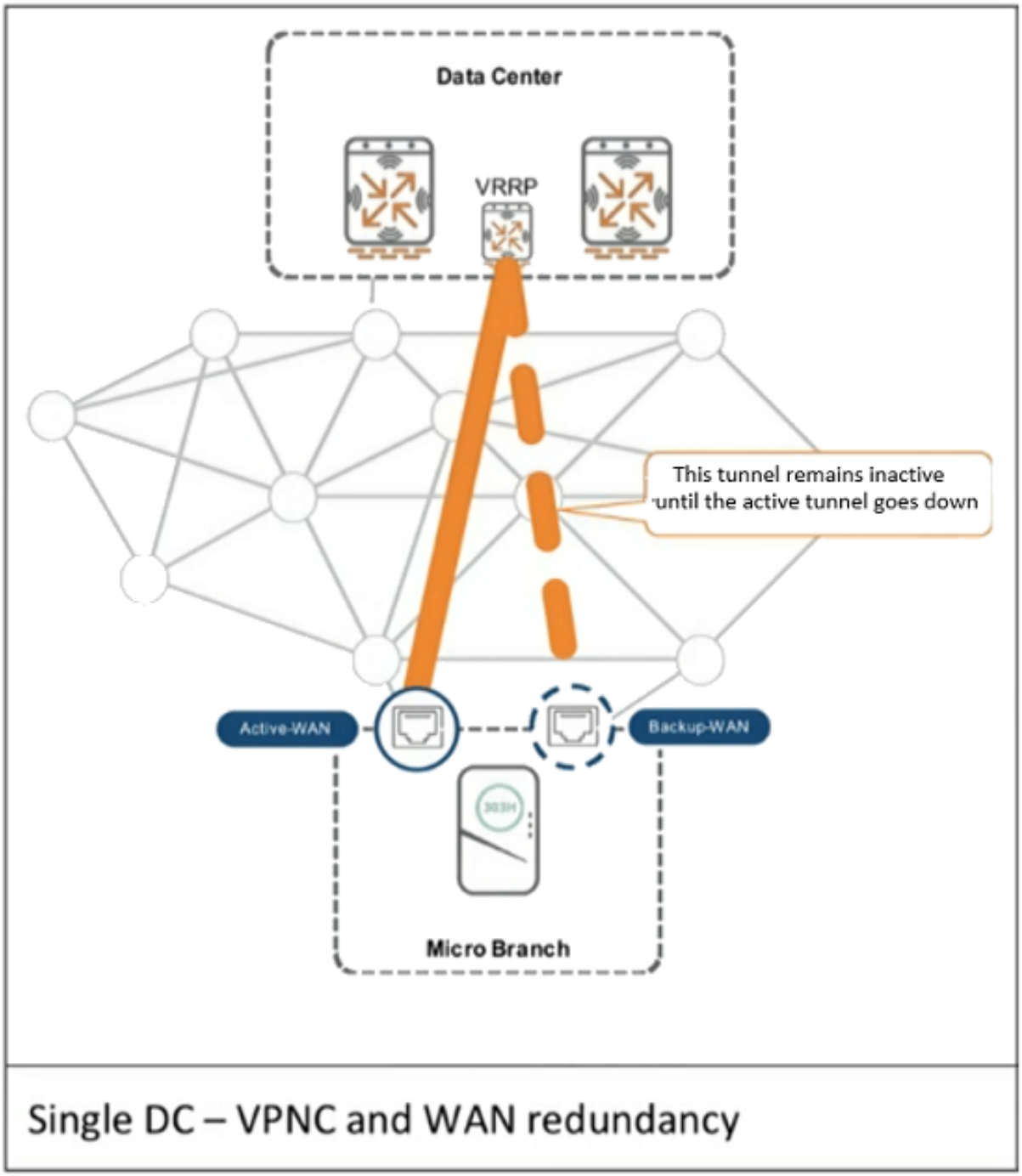
In this type of Micro Branch network, two VPNCs are deployed in a single data center. This is a Layer 2 (L2) redundancy. Both the VPNCs run Virtual Router Redundancy Protocol (VRRP) to dynamically fail over to the standby VPNC if the active VPNC fails. It is important to note that the standby VPNC does not terminate any VPN tunnels or advertise branch routes through OSPFv2 or BGP4 until it transitions to an active state.

At the branch site, two WAN uplinks are available. However, only one active IPsec tunnel is established and this tunnel terminates on the VRRP virtual IP. As most VPNCs are deployed behind an Internet edge firewall, a port-forwarding rule is configured to permit UDP4500 traffic from an outside public IP address to the VRRP virtual IP.

On the IAP, you can either have two ethernet uplinks, or one ethernet and one USB uplink for a 3G/4G connection. You can set priority to choose the active uplink. When the current active uplink goes down, the IAP looks into the priority list and makes the next uplink in the list as the active uplink.

The following image is a sample topology of a Micro Branch network with VPNC and WAN redundancy:

Figure 300 *Micro Branch with VPNC and WAN Redundancy*



- **Micro Branch with Data Center and WAN redundancy (L3 Redundancy)**

To understand this topology, let us consider a setup that includes two hubs to provide High Availability. One of these is a primary hub and the other one is a secondary hub. This deployment model is often referred to as Layer 3 redundancy since OSPFv2 or BGP4 route costs in the corporate network are used to determine which hub site is actively forwarding traffic to the branch sites. The hub that advertises the branch routes at the lowest cost is the preferred path.

In this setup, redundancy is provided by configuring the IAP at the Micro Branch to establish two IPsec tunnels, one to each of the hubs. The active tunnel is terminated on the primary hub and the backup tunnel

is terminated on the back-up hub. When the active tunnel goes down, the back-up tunnel establishes a connection with the secondary hub.

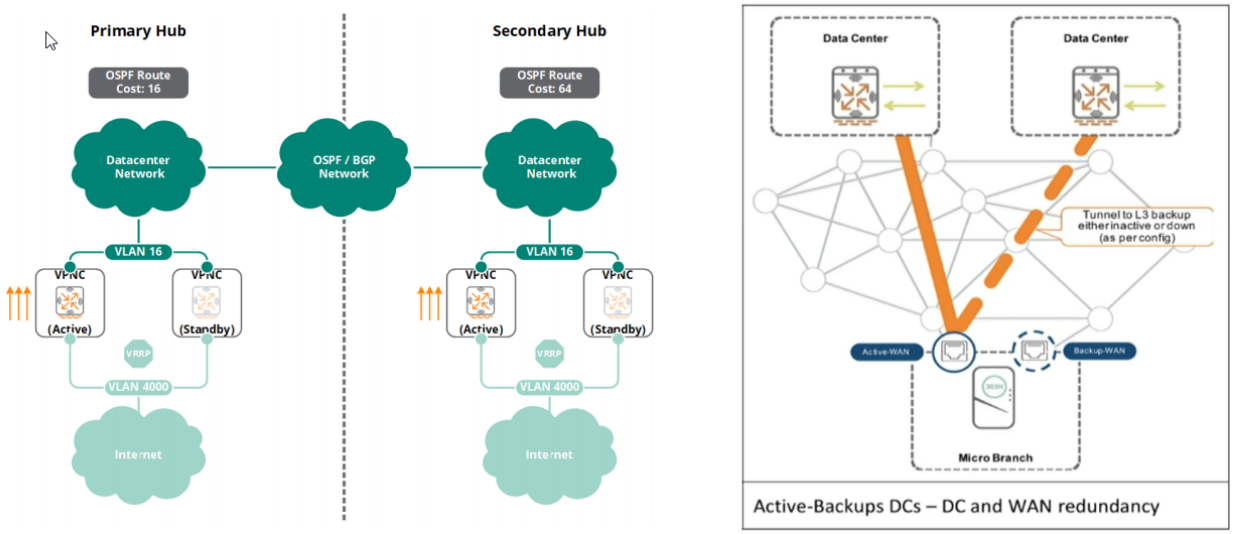
Each hub is therefore assigned a primary or secondary role. The designated VPNCs in each hub advertise the branch routes into OSPFv2 or BGP4 at different route costs. The VPNCs in the primary hub advertise the branch routes at a lower route cost than the VPNCs in the secondary hub. The VPNCs in the primary hub forward hub-to-spoke, spoke-to-hub and spoke-to-spoke traffic during normal operation. If the primary hub fails or becomes unreachable, the VPN tunnels are already established to the secondary hub site.

During a failover, the OSPF/BGP routers will re-converge so that the routes are reachable via the secondary hub with a typical re-convergence occurring in under 1 minute (depending on the IGP configuration).

In this model, it is important to note that while the IAPs establish active VPN tunnels to both hubs, only one hub is actively forwarding traffic for the IAPs at any given time. The ability to simultaneously forward traffic to both hubs at the same time is not supported with the IAP VPN solution.

The following image is a sample topology of a Micro Branch network with DC and WAN redundancy:

Figure 301 *Micro Branch with data center and WAN redundancy*

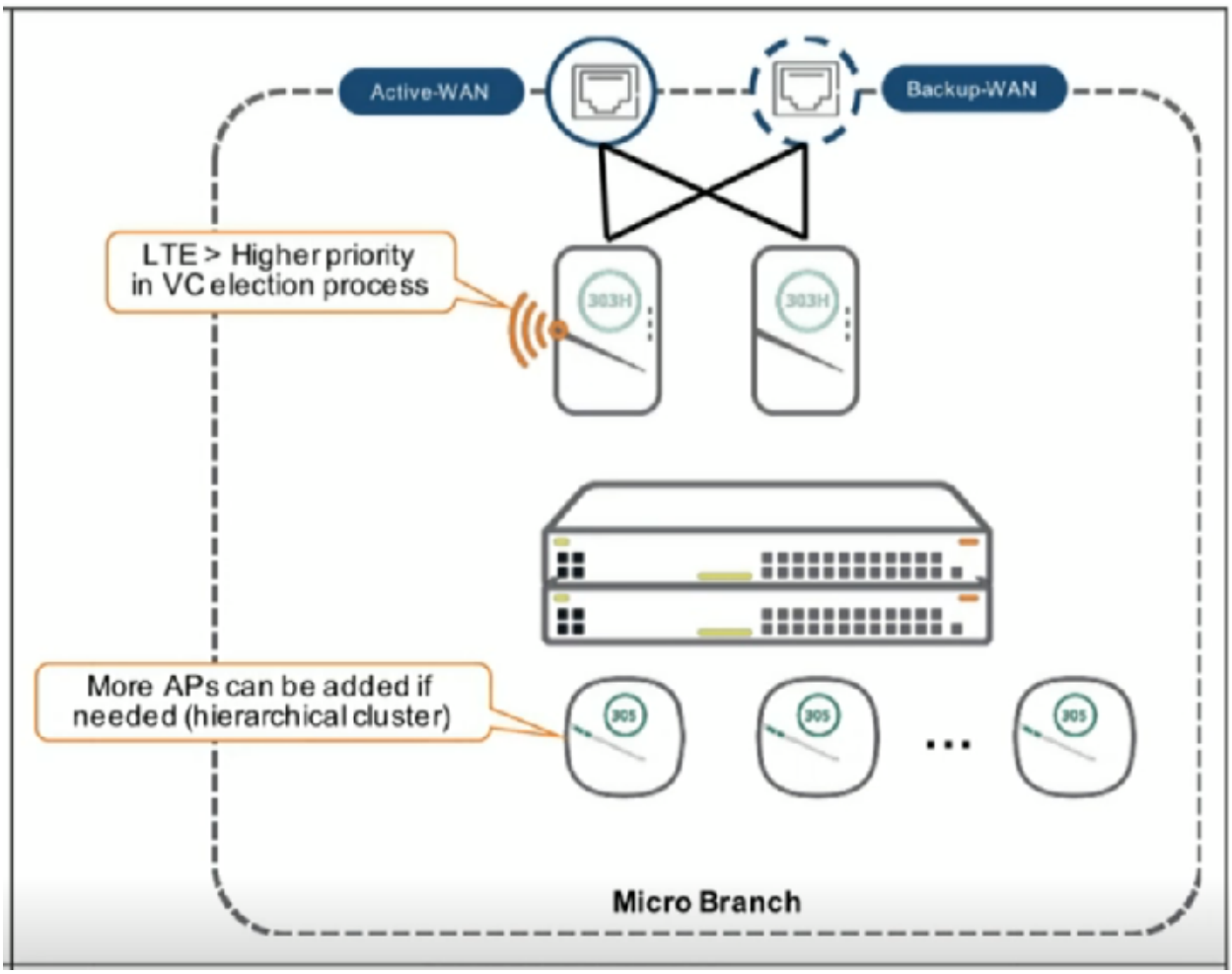


- **A fully redundant Micro Branch**

In this type of a Micro Branch setup, you can have multiple APs, connected to a switch to provide redundancy. One of these APs acts as the conductor and the rest are members. If the conductor fails, another member is chosen as the conductor. An active and a back-up WAN uplink connection is established from the APs. Both of these uplinks can be ethernet or one of them can be a USB uplink to support 3G/4G connections.

The following image is a sample topology of a Micro Branch network with full redundancy:

Figure 302 *Micro Branch with full redundancy*



Configuring a Micro Branch with Instant APs

For small branch deployments, Aruba offers an Instant AP-based SD-WAN solution. In a micro branch deployment, you do not require a Branch Gateway. If you have an Instant AP cluster deployed, the Instant AP acting as a Virtual Controller or a conductor AP can establish secure VPN connections with VPNCs.

To get started with your Micro Branch deployment, complete the following tasks:

Before you begin, ensure that you have provisioned and configured the VPNCs in Aruba Central. If not, see Provisioning Aruba Gateways in Aruba Central.

1. **Tunnel Authentication**—Validate that the VPNC group is using the default setup to authenticate IAP-VPN tunnels. For verification, the settings can be found under **VPNC Group** > **Devices** > **Gateways** > **Security** > **L3 Authentication** > **VPN Authentication** > **default-iap** > **Server Group**.
2. **Dynamic IP Assignment**—When connecting to the VPNC, APs behave like dynamic VPN clients. This means that they are assigned a pool of Inner IP addresses, which can be configured in **VPNC Group** > **Devices** > **Gateways** > **VPN** > **General VPN**.
3. **Route Redistribution**—The Aruba Micro-Branch architecture can work in layer 2 (L2) mode, where VLANs are L2 extended from the APs to the VPNC, or in layer 3 (L3) mode, where branch subnets are

advertised upstream as part of the tunnel negotiation. When working in L3 mode, branch subnets should be redistributed into a dynamic routing protocol such as OSPF and BGP.

The following topics describe the various configurations that need to be done on Instant APs and VPNCs for deploying a Micro Branch solution:

- Configuring VPNCs for Micro Branch Solution
- Configuring Instant APs for Micro Branch Solution

For more information on how to configure IAP-VPN address pools, and enable OSPF and BGP routing protocols, see *Aruba IAP-VPN Solution Guide for Teleworkers and Home Offices*.

Configuring Instant APs for Micro Branch Solution

For a single data center without redundancy, perform the following configuration tasks on the Instant AP:

1. Configure a single VPN using an IPsec tunnel. For more information, see the *Configuring IPsec VPN Tunnel* section in Aruba Central Help Center.
2. Configure a routing profile for split-tunneling of client traffic. For more information, see the *Configuring Routing Profiles for Instant AP VPN* section in Aruba Central Help Center.
3. Configure the Enterprise domains for split-tunneling of DNS traffic from clients. For more information, see the *Configuring Enterprise Domains* section in Aruba Central Help Center.
4. Configure DHCP scope in Distributed, L3 and Centralized, L2 modes. For more information, see the *Configuring DHCP Scopes on Instant APs* section in Aruba Central Help Center.

Configuring VPNCs for Micro Branch Solution

For a successful Instant AP VPN termination on the SD-WAN Gateway, perform the following configuration tasks on the SD-WAN Gateway:

- Configuring Instant AP VPN Pool for Aruba Gateways
- Authentication Servers
- Redistributing Branch Subnets

Configuring Instant AP VPN Pool for Aruba Gateways

The VPN local pool is used to assign an IP Address to the Instant AP after successful Extended Authentication (XAuth) VPN.

To configure the Instant AP VPN Pool, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **VPN** > **General VPN**.
6. Click **+** from the **Address Pools** table to open the **Add New Address Pool** section.
7. Enter the following information in the **Add New Address Pool** section to create a new address pool:

- **Pool name**—Name of the pool
- **Start address(ipv4)**—The starting IPv4 address of the pool.
- **End address(ipv4)**—The ending IPv4 address of the pool

8. Configure the following additional VPN parameters based on your requirements:
   - **Source-nat**—Enable this option if the IP addresses of VPN clients must be translated to access the network and select a NAT pool to be used for address translation from the **NAT pool** drop-down list .
   - **VIA SSL fallback**—Enable this option to allow VIA SSL fallback.
   - **IAP-VPN backward compatible**—Enable this option to allow the Instant APs and Branch Gateways that run on AOS versions earlier than 8.4.x.x to use port 8089 for VPN VLAN subnet registrations.
   - **Primary DNS server**—Specify the IP address of the Primary DNS Server to be pushed to the VPN client.
   - **Secondary DNS server**—Specify the IP address of the Secondary DNS Server to be pushed to the VPN client.
   - **Primary WINS server**—Specify the IP address of the Primary WINS Server to be pushed to the VPN client.
   - **Secondary WINS server**—Specify the IP address of the Secondary WINS Server to be pushed to the VPN client.
9. Save the changes.

Authentication Servers

Instant APs identify themselves using the internal TPM certificate, which has the MAC address as the CN. The Micro Branch solution can use the internal server or an external RADIUS server with the database of all the Instant APs, so that the VPNCs accept the incoming connection from the Instant APs.

If you are using the internal server, see Configuring an Internal Server.

If you are using an external RADIUS server, see Configuring and Mapping External RADIUS Server.

Configuring an Internal Server

When you use the internal server for authenticating the Instant AP, the VPNC validates if the Instant AP is in the same user account with valid subscription assigned and automatically allowlists it.

To enable internal server authentication, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Config** icon.
   The gateway group configuration page is displayed.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Security** > **L3 Authentication**.
6. Select the **default-iap** profile under **VPN Authentication**.
7. In the **default-iap** profile, select **internal** from **Server Group**.
8. Save the changes.

Configuring and Mapping External RADIUS Server

To use an external RADIUS server for authentication, you must configure the server on the VPNC. To configure an external RADIUS server for authentication, see Configuring RADIUS Authentication Server on Aruba Gateways

Aruba recommends to use the ClearPass Policy Manager as it can download the list of Instant APs owned by the customer from the Activate server to automate the allowlisting process. For information on configuring the ClearPass Policy Manager, see *ClearPass Policy Manager User Guide*.

Map the configured RADIUS server to the Instant AP VPN server group using the following steps:

1. In the **Network Operations** app, use the filter to select a Group in which VPNCs are provisioned.
2. Under **Manage**, click **Devices** > **Gateways** and then click the **Config** icon to display the Gateway configuration dashboard.
3. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
4. Click **Security** > **L3 Authentication**.
5. Select the **default-iap** profile under **VPN Authentication**.
6. In the **default-iap** profile, select the configured RADIUS server from **RADIUS Accounting Server Group.**
7. Save the changes.

Redistributing Branch Subnets

The Micro Branch solution provides support to learn branch subnets using the dynamic routing protocol. To redistribute the branch networks in L3 mode, complete the following steps:

1. In the **Network Operations** app, use the filter to select a Group in which VPNCs are provisioned.
2. Under **Manage**, click **Devices** > **Gateways** and then click the **Config** icon to display the Gateway configuration dashboard.
3. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
4. Click **Routing** > **OSPF**.
5. Enable OSPF for routing and configure the area to be used. For more information on configuring OSPF area and other parameters, see Routes Advertisement Using OSPF.
6. Enable **Redistribute overlay routes**, and then specify a cost for the overlay routes. The cost set here applies only to the routes that are learnt from the Aruba Gateways.
7. Save the changes.
8. Click **Interfaces** > **VLANs** and select the uplink VLAN interface from the **VLAN IDs** table.
9. From the **IPv4** tab, select **Enable OSPF** under **Other Options** and configure the OSPF area to be used.
10. Save the changes.

Chapter 26
Configuring Support for Aruba VIA Service

Aruba VIA refers to Aruba Virtual Intranet Access solution for establishing a virtual private network connection. VIA has two primary purposes:

- To provide secure corporate access to employee laptops and smart-phones from anywhere
- To provide ease-of-use for the end users and network administrators

The ease-of-use is what differentiates VIA from other VPN solutions. VIA offers a zero-touch end-user experience and removes the complexity that is associated with configuring VPN clients on end-user devices. VIA not only provides ease-of-use for end users but also simplifies configuration and management for the IT team.

The VIA client that is available for Microsoft Windows computers (Windows XP, Vista, and Windows 7), Apple Mac OS X, and Apple iOS devices is a hybrid Internet Protocol Security (IPsec)/ Secure Sockets Layer (SSL) VPN client. If the user is connected to an untrusted network, the VIA client scans network connections and automatically establishes a secure connection back to the corporate network. Some additional features include Content Security Services (CSS), single-logon, SSL fallback when IPsec is blocked, and the ability to configure Wireless Local Area Network (WLAN) settings using the supplicant provided by the operating system.

Configuring VIA

1. To configure an Aruba VIA solution, complete the following tasks :
   - Configuring VPN IP Pool
   - Defining IKEv1 Shared Secret
   - Configuring VIA User Role
   - Creating VIA Server Group for Authenticating VIA Users
   - Configuring VIA Authentication Parameters
   - Loading and Applying VIA Certificates
   - Configuring and Attaching VIA Connection Profile
   - Uploading VIA Installer to VPNC

Configuring VPN IP Pool

The first step to configure VIA is to create a VPN IP Pool on the VPNC. To configure the VPN IP Pool, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway configured as a VPNC.

   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.

3. Click the **Config** icon.

   The configuration page for the VPNC group is displayed. You can configure VPN IP pool either in **Basic Mode** or in **Advanced Mode**.

4. If you are in the **Basic Mode**, complete the following steps:
   a. Click the **VPN** tab.
   b. Click **+** in the **Address Pools** table to add address pools. These address pools are used as *Inner IPs* for remotely connected IAPs and VIA client.
   c. Enter the following information to add a new address pool:
      - **Pool name**—The name of the pool.
      - **Start address**—The starting IPv4 address of the pool.
      - **End address**—The ending IPv4 address of the pool. The end IP address must be greater than or equal to the start IP address
   d. Select the address pool from the **IAP-VPN pool** drop-down list (Optional). This is the address pool that is used as the Inner IP of APs working in IAP-VPN mode, and is automatically mapped to the default VPN role.
      - You can view the address pools created in the **Basic Mode** page in **Advanced Mode** in the following tabs under **VPN** > **General VPN**.
      - Under **Security** > **Roles**, select **default-vpn-role**. Click **More** and expand **VPN**. The Address Pool is listed in the **L2tp pool** drop-down list.
5. Click **Advanced Mode** to access the advanced configuration options.
   a. Click **VPN > General VPN**.
   b. Click **+** from the **Address Pools** table to open the **Add New Address Pool** section.
   c. Enter the following information in the **Add New Address Pool** section to create a new address pool:
      - **Pool name**—The name of the pool.
      - **Start address(ipv4)**—The starting IPv4 address of the pool.
      - **End address(ipv4)**—The ending IPv4 address of the pool. The end IP address must be greater than or equal to the start IP address.
   d. Configure the following additional VPN parameters based on your requirements:
      - **Source-NAT**—Enable this option if the IP addresses of VPN clients must be translated to access the network and select a NAT pool to be used for address translation from the **NAT pool** drop-down list .
      - **VIA SSL fallback**—Enable this option to allow VIA SSL fallback.
      - **Primary DNS server**—Specify the IP address of the Primary DNS Server to be pushed to the VPN client.
      - **Secondary DNS server**—Specify the IP address of the Secondary DNS Server to be pushed to the VPN client.
      - **Primary WINS server**—Specify the IP address of the Primary WINS Server to be pushed to the VPN client.
      - **Secondary WINS server**—Specify the IP address of the Secondary WINS Server to be pushed to the VPN client.
6. Save the changes.

Ensure that the configured IP addresses are reachable.

Defining IKEv1 Shared Secret

If you are configuring a VPN to support IKEv1 and clients using pre-shared keys, you can configure a global IKE key or IKE key for each subnet. Make sure that this key matches the key on the VPN client.

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the gateway device is displayed.
4. Under **Manage**, Click **Device**.
   The gateway configuration page is displayed.
5. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
6. Click **VPN >Shared Secrets**.
7. In the **IKE Shared Secrets for VPN Clients** table, click **+** to open the **Create IKE Group** section.
8. Enter the **Subnet** and **Subnet** mask. To make the IKE key global, enter 0.0.0.0 for both values.
9. Select the **Representation type** from the drop-down list.
10. Enter a value for **Shared key** and repeat it in the **Retype shared key** field.

Configuring VIA User Role

The VIA user role is assigned to the users who successfully authenticate through their VIA client. The user role defines the access rights of the users that connect using VIA. Aruba recommends that network administrators configure custom user roles that depict the network access policy of their respective organizations. You can also use the predefined **default-via-role** and edit it according to your requirements.

For more information about creating user roles, see Configuring User Roles for Clients.

Creating VIA Server Group for Authenticating VIA Users

A server group is a collection of servers that are used for authentication. By default, the first server on the list is used for authentication unless it is unavailable. A server group can have different types of authentication servers. For example, you can create a server group that uses an LDAP server as a backup for a RADIUS server.

To configure a custom server group for authenticating VIA users, see Configuring Server Groups.

Configuring VIA Authentication Parameters

Configuring VIA Authentication Profile

The VIA authentication profile defines the authentication server group used and the default role assigned to the authenticated users. Multiple authentication profiles can be created. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile.

The VIA authentication profile is a critical part of VIA configuration and it is used for these purposes:

- To determine the authentication server for the XAUTH authentication phase of IKEv1 and EAP authentications of IKEv2.
- To determine the authentication server for the VIA web authentication. The VIA authentication profile is an integral part of the VIA web authentication, which determines the authentication sever used for VIA bootstrap process and for authenticating users on the VIA installer download page of the VPNC. For more information on VIA web authentication, see Configuring VIA Web Authentication.

To configure a VIA authentication profile, complete the following steps:

1. To configure a Branch Gateway group or a Branch Gateway, complete either one of these steps:
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Security > L3 Authentication**.
4. Select **VIA Authentication**.
5. Click **+** to create a new VIA authentication profile or select an existing profile. You can also use the predefined **default** VIA authentication profile.
6. After selecting the required profile, select the role that you defined for the VIA users in the **Default role** field. For more information on configuring the other parameters for this profile, see Table 288.
7. Select the required server group for authentication from the appropriate server group option under the selected profile. The server group options are **RADIUS Accounting Server Group**, **RFC 3576 Server**, and **Server Group**. Optionally you can configure the following options for the selected server group:
   - **Fail through**—Enables the fail through option for the server group.
   - **Load balance**—Enables load balancing among the servers for authentication requests.
8. Save the changes.

Table 288: *VIA Authentication Profile Parameters*

Parameter	Description
Default Role	Select the role that you want to be assigned as the default role for the client when authenticating using this profile. By default, the default-via-role is assigned.
Max Authentication failures	Maximum number of authentication failures allowed for the client. Allowed range is 1-10 and the default value is 0.
Description	Description of the authentication profile.
Check certificate common name against AAA server	Select this option to check for certificate common name against the AAA server. Default: enabled.
Client-certificate based authentication for VIA Profile download	Select this option to enable client-certificate based authentication for VIA Profile download. By default, this is disabled.
Authentication protocol	Select the authentication protocol to be used. The default value is PAP.
Download Role from CPPM	Select this option to download the default role from ClearPass Policy Manager, if the default role is not defined.

Configuring VIA Web Authentication

The VIA web authentication is a list of VIA authentication profiles. The web authentication list allows the users to login to the VIA download page <https://<VPNC IP address>/via> to download the VIA client. To successfully login to the VIA download page, the users must authenticate successfully against the VIA authentication profile in the list. If more than one VIA authentication profile is configured in the web authentication list, the users can view the list and select one authentication profile before authenticating to the VIA installer download page.

The web authentication list is also used during the initial user authentication process that determines the VIA user role. The Branch Gateway has a default web authentication list to which multiple VIA authentication profiles can be added. Additional VIA web authentication lists cannot be created.

To configure the VIA web authentication list, add one or more VIA authentication profiles to the default web authentication list and order them according to the priority. Configuring more than one VIA authentication profile in the VIA web authentication list allows the users to use the backup authentication server when the primary server becomes unavailable temporarily.

To configure the VIA web authentication profile, complete the following steps:

1. To configure a Branch Gateway group or Branch Gateway, complete either one of these steps:
   - For a Branch Gateway group, in the **Network Operations** app, use the filter to select **Groups**.
   - For a Branch Gateway in the **Network Operations** app, use the filter to select the gateway.
2. Under **Manage**, click **Devices** > **Gateways**.
3. Click the 

configuration icon. The gateway configuration page is displayed.
4. Select **VIA Web Authentication** > **default**.
5. Click **+** to add a VIA authentication profile in the **VIA authentication profiles** table.
6. Save the changes.

Loading and Applying VIA Certificates

VIA configuration requires server certificates for both HTTPS as well as VPN. It also requires CA certificates if certificate-based authentication is used on the client devices.

To load and apply VIA certificates, complete the following tasks:

1. Load the required VIA certificates to the certificates store in Aruba Central. For more information on loading certificates using Aruba Central, *see Aruba Central Help Center*.
2. Configure the VPNC to use the required VIA certificate. For more information on configuring certificates for a device, see Configuring Aruba Gateways for Certificate-Based Authentication.

Configuring and Attaching VIA Connection Profile

Configuring VIA Connection Profile

The VIA connection profile is a collection of all the configurations required by a VIA client. The VIA connection profile contains all the details required for the VIA client to establish a secure IPsec connection to the VPNC. A VIA connection profile also defines other optional parameters. Such optional parameters can be client auto-login, split-tunnel settings, and Content Security Services (CSS) settings. You can configure multiple VIA connection profiles.

A VIA connection profile is always associated to a user role, and all users that belong to that role use the configured settings. When a user authenticates successfully to a server in an authentication profile, the VIA client downloads the VIA connection profile that is attached to the role assigned to that user.

Table 289 summarizes the various parameters of a VIA connection profile .

To configure a VIA connection profile, complete the following steps:

1. In the **Network Management** app, use the filter to select a VPNC group or VPNC.
   - To configure a Branch Gateway group or VPNC group, complete the following steps:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the **List** view.
     c. Click **Config**.
        The configuration page is displayed for the selected group.
   - To configure a Branch Gateway or VPNC, complete the following steps:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway device configuration page is displayed.
2. Click **Security > L3 Authentication**.
3. Select **VIA Connection**.

4. Click **+** to create a new VIA connection profile or select an existing profile. You can also use the predefined **default**VIA connection profile.
5. After selecting the required profile, configure the various VIA connection profile parameters as described in Table 289
6. Save the changes.

Table 289: *VIA Connection Profile Parameters*

Parameter	Description
VIA servers	This parameter has the following fields: ■ **Addr**—Add the public IP or DNS hostname of the VPNC. This is the host name or IP address that the users enter as the remote server information on the VIA client. ■ **Internal IP**—Add the IP address of any of the internal VLAN interfaces of the VPNC. This IP address should not be reachable from the public Internet. The VIA client uses this IP address to determine whether or not the user is connected to a trusted network. ■ **Description**—Add a human-readable description of the VIA server. **NOTE:** More than one VIA server can be added to the list.
Client auto-login	Enabling client auto-login makes the VIA client detect untrusted network and connect automatically. If you disable auto-login, VIA stays idle after it comes up and the user has to manually click **Connect** to establish a VPN connection even though an untrusted network is detected. Default: enabled
VIA authentication profiles to provision	This VIA authentication profile is used to determine the authentication server used for the IKE authentication process. If more than one VIA authentication profile is added to this list, the users can choose the VIA authentication profile to be used during IKE authentication. If no VIA authentication profile is defined, the users are authenticated against the server group that is specified by the default VIA authentication profile (predefined).
Allow client to auto-upgrade	This parameter allows the VIA client to automatically upgrade if a newer version of VIA is available on the VPNC. By default this is enabled.
VIA tunneled networks	When split-tunneling is enabled, the VIA client tunnels traffic to the VPNC for all the network destinations (IP address and netmask) listed in this parameter. All other network destinations are bridged appropriately on the client. If split-tunnel is disabled, all the traffic is tunneled to the VPNC irrespective of the destination.
Enable split tunneling	When enabled, all traffic to the VIA tunneled networks goes through the VPNC and the rest is bridged directly on the client. If split-tunnel is disabled, all the traffic is tunneled to the VPNC irrespective of the destination.
Allow client-side logging	This parameter determines whether client side logging is allowed or not. If enabled, VIA client collects logs that can be sent to the support email address for troubleshooting. Default: Enabled
VIA IKEv2 Policy	This IKE policy is used for IKEv2 connections by the VIA client. Remember that IKEv2 using PSK is not supported for VIA. For more information on configuring IKE policies, see Configuring IKE Policies.
VIA IKE Policy	This IKE policy is used for IKEv1 connections by the VIA client. This policy determines whether IKEv1 phase 1 authentication uses PSK or certificates. For more information on configuring IKE policies, see Configuring IKE Policies.

Parameter	Description
Use windows credentials	This parameter determines whether the Windows credentials are used automatically to login to VIA. If enabled, the single sign-on feature can be utilized by remote users to connect to internal resources. Default: Enabled
Enable IKEv2	This parameter enables or disables IKEv2.
Use suite b cryptography	This parameter enables or disables Suite B cryptographic methods.
IKEv2 authentication method	This parameter indicates the IKEv2 client authentication method. It can be one of these settings: l user-cert l EAP-TLS l EAP-MSCHAPv2 Remember that EAP termination on the VPNC is not supported.
VIA IPSec v2 crypto map	This IPsec map is used by IKEv2 VIA client to connect to the VPNC.
VIA IPSec crypto map	This IPsec map is used by IKEv1 VIA client to connect to the VPNC.
Allow user to save passwords	This parameter determines whether the users can save the passwords entered in VIA or not. If this is enabled, the user credentials that were able to successfully establish a VIA connection are saved securely until VIA is uninstalled or until IKE authentication fails with stored credentials. If this option is disabled, VIA prompts for credentials every time it establishes a connection. If secure tokens such as the RSA tokens are used for authentication, disable this option to prompt the user for a password/token for each connection attempt. By default, this is enabled.
Enable supplicant	This parameter enables the supplicant mode.
Enable FIPS module	This parameter enables the VIA FIPS module.
Auto-launch supplicant	This parameter automatically connects to the configured WLAN network.
Lockdown all settings	This parameter locks all the configuration options available on the end-user VIA client. If this option is enabled, a VIA user can only connect, disconnect or send logs. Diagnostics such as traceroute and ping can still be used, but no settings can be changed. **NOTE:** This option is available in VIA 2.1 and later versions.
Domain suffix in VIA authentication	This parameter enables domain suffix in VIA authentication.
Enable Controllers load balance	This parameter enables load balancing of VIA clients by randomly choosing a VPNC from the list of available VIA VPNCs that can be used for connection. This feature does not take the existing load of the VPNC into account. **NOTE:** This option is available in VIA 2.1 and later versions.

Parameter	Description
Enable domain pre-connect	This parameter enables pre-connection to the domain. By default, this is enabled.
VIA banner message reappearance timeout(minutes)	This parameter configures the timeout value in minutes for reappearance of VIA login banner message. The default value is 60 minutes.
VIA client network mask	This network mask is set on the client after the VPN connection is established. The default value is 255.255.255.255.
Validate server certificate	If enabled, the VIA client validates the server certificate presented by the VPNC during the IPsec process. Remember that to validate the server certificate, the CA that signed the VPNC certificate should be a trusted CA in the client certificate store. By default, this is enabled.
VIA client DNS suffix list	This is the DNS suffix that is set on the client after the VPN connection is established.
OCSP cert verification enabled	This parameter enables OCSP certificate verification.
In EAP/IKE, action taken when OCSP cert verification result is unknown	This parameter accepts the certificate when OCSP certificate verification result is unknown for EAP/IKEs.
VIA domain name profile	This parameter allows you to add VIA domain name profiles.
Destination traffic to be blocked	This parameter allows you to configure the IP address and netmask of the destination traffic for blocking.
Block-destination-traffic-selector (on/off)	This parameter enables or disables the blocking of destination traffic.
VIA max session timeout	This parameter defines the maximum time, in minutes, allowed before the VIA session is disconnected. Default: 1440 min
VIA logon script	This parameter specifies the name of the logon script that must be executed after VIA establishes a secure connection. The logon script must reside on the client computer.
VIA logoff script	This parameter specifies the name of the logoff script that must be executed after VIA tears down a secure connection. The logoff script must reside on the client computer.
VIA support e-mail address	This is the support email address to which VIA users send client logs using the VIA client. For information on sending VIA logs using the VIA client, see Chapter 8: Establishing VIA connection.
Maximum reconnection attempts	This parameter defines the maximum reconnection attempts by the VIA client. If the reconnection attempt is exceeded, the VIA client becomes idle. However, if the connection attempt fails due to an IKE authentication failure error, then the user is prompted to reenter username and password. Default: 3

Parameter	Description
VIA external download URL	The VIA installer can be hosted on an external server other than the VPNC for download by the VIA client during VIA upgrades and by the end users. If the VIA installer is hosted on an external server, this parameter should be configured to redirect the VIA clients to the external URL for the upgrade process. If this parameter is not configured, the VIA clients automatically go to https:// <VPNC IP address or FQDN >/via for upgrades.
Allow user to disconnect VIA	This feature determines whether the users can disconnect VIA or not. Remember that a user with administrative rights to a laptop can always uninstall VIA or disable the service running on the laptop. For users with restricted access to the laptops, disabling this feature ensures that users cannot disconnect VIA. By default, his is enabled.
Content security gateway URL	When split-tunnel mode is enabled, traffic to external websites is inspected by the CSS.
Comma separated list of HTTP ports to be inspected (apart fromdefault port 80)	Traffic to the specified list of ports is verified by the CSS provider.
Certificate criteria	Certificate criteria expressed in key-value pairs where keys can be certificate attributes, or certificate OIDs. Multiple key-value pairs can be combined with semi-colon.
Enable content security services	This parameter enables the CSS. The CSS requires the CSS licenses.
Keep VIA window minimized	When this feature is enabled, the VIA client is minimized to the system tray during the connection phase. This feature is applicable only for VIA clients installed on Microsoft Windows laptops. Default: disabled
Block traffic until VPN tunnel is up	This parameter allows blocking of traffic until VPN tunnel is up.
Block traffic rules	This parameter configures the VIA allowlist traffic rules. Specify the IP address, netmask and description for the traffic rules.
User idle timeout	User idle timeout value. Allowed range is 30-15300 seconds in multiples of 30 seconds.
VIA client mtu value	MTU value for the VIA client. Allowed range is 576-5120 bytes. The default value is 1452 bytes.

Attaching the VIA Connection Profile to User Role

VIA connection profile that the VIA client has to download should be attached to the user role to be assigned to the user. When a user goes through the authentication phase it is placed on a role which has a certain connection profile associated. Suppose, the users authenticating to the VIA authentication profile are assigned the **default-via-role**. To assign a specific connection profile to these users, attach the connection profile to the **default-via-role**.

To attach the VIA connection profile to a user role, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
   The dashboard context for a group is displayed.

2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.

3. Click the **Config** icon.

   The gateway group configuration page is displayed.

4. Click **Security > Roles**.
5. Select the role to which you want to associate a VIA connection profile and select the **More** tab.
6. Expand **VPN** and select the required VIA connection profile from the **VIA connection profile** drop-down list.
7. Save the changes.

Uploading VIA Installer to VPNC

VIA installers for Apple iOS and Mac OS X devices are available in the Apple App store. VIA installers for other devices with Windows 32-bit and 64-bit operating systems are available at the Aruba support site.

For end users and VIA client to access the VIA installers during upgrades, the VIA installers require to be uploaded on the VPNC or an external hosting server.

If the VIA installer is hosted on an external hosting server, configure the gateway configuration parameter **VIA external download URL** under **Security** > **L3 Authentication** > **VIA Connection** to redirect the VIA clients to the external URL for the upgrade process. For more information, see Configuring and Attaching VIA Connection Profile.

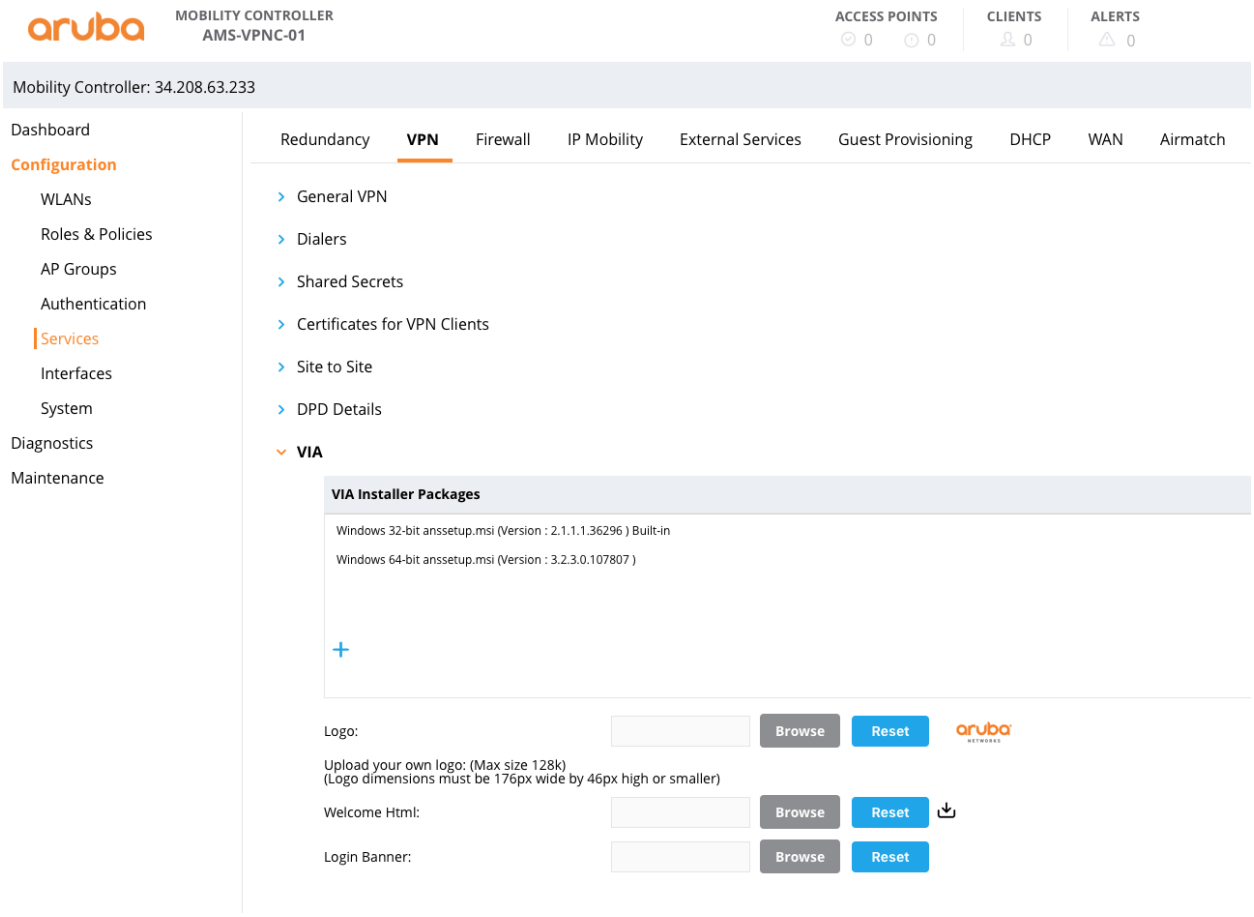
If the VPNC is used to host the VIA images, it automatically detects the operating system of the device that is connecting to the VIA download page. It also learns the parameters of the web browser used to connect to the VIA download page to determine the operating system.

After the users login to the VIA download page, the VPNC presents the appropriate VIA installer image. After the initial installation, the VIA clients are capable of automatically upgrading their image (depending on VIA connection profile setting). If the network administrator uploads a new version of VIA installer to the VPNC or to an external server (indicated by the VIA external download URL parameter of the VIA connection profile), the VIA clients automatically upgrade their image.

To upload the installer packages, complete the following steps:

1. Log into the local WebUI of the VPNC.
2. Navigate to **Configuration** > **Services** > **VPN** > **VIA**.
3. To upload a VIA installer package, expand **VIA**, click **+**, and upload the VIA installer package.

Figure 303 *Upload VIA Installer Package into VPNC*



Chapter 27
Provisioning Gateways Using Configuration Templates

If your deployment has a large number of Aruba Gateways and requires bulk configuration, you can use the configuration template feature in Aruba Central to quickly provision Gateways. The configuration template feature is available for the Gateway devices provisioned in template groups in Aruba Central.

The template groups in Aruba Central allow network administrators to create a common configuration output by using a combination of CLI commands and variables, and apply this configuration to the other Gateway devices provisioned in that group.

Important Points to Note

Before you begin the provisioning procedure, note the following important points and recommendations:

- Aruba recommends that the administrators who are provisioning Gateways using templates familiarize themselves with the Gateway CLI commands. A prior understanding of the Gateway CLI commands helps in determining the service impact and avoiding errors that may occur due to incorrect configuration.
- Before assigning devices to groups, identify the devices that have a common set of CLI commands and configuration requirements.
- The configuration requirements for a Branch Gateway and VPNC are different, so Aruba recommends that you create separate template groups for Branch Gateways and VPNCs.
- If you are provisioning Gateways with factory-default configuration, you can build a template based on the current configuration of the first device that joins a template group.
- If you want to create a template based on the current configuration of an existing Gateway device, access the CLI console of the device and copy the configuration. Use this configuration as the template text when building a new template. You can enhance this template for multi-device use by adding variable definitions.
- For data-vpnc probes, jitter is enabled by default in templates. To disable jitter, ensure that you add **no jitter** in the template. For more information about customizing templates, see Customizing a Template Using Variable Definitions.
- While Aruba Central allows you to move a Gateway device from a UI group to a template group, you must ensure that the current configuration running on the device is backed up and is included in the configuration template created for that template group. However, Aruba recommends that you exercise caution when moving a device from a UI group to a template group as incorrect configuration may lead to service disruption.

Configuring Gateways Using a Template

To provision Gateways in a template group, complete the following procedures:

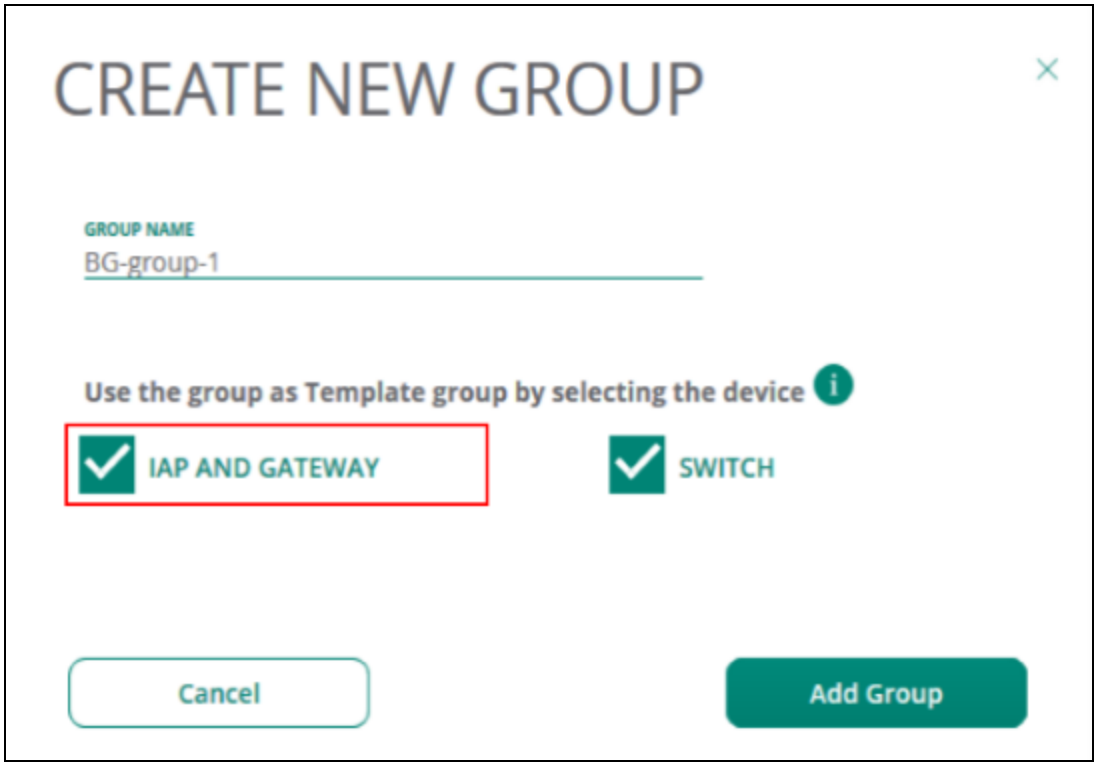
- Verifying Configuration Status
- Backing up and Restoring Templates

Creating a Template Group

To create a template group, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Maintain** > **Organization** > **Groups**. The **Groups** page is displayed.
3. Click **(+) New Group**. The **Create a New Group** pop-up window opens.
4. Enter a name for the group.
5. Select the **IAP and Gateway** check box to create a template group for Gateways.

   Figure 304 *Template Group Creation*



6. Click **Add Group**.

Assigning a Gateway to a Template Group

To assign a Gateway to a group, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway. The dashboard context for a group is displayed.
2. Go to **Maintain** > **Organization** > **Groups**. The **Groups** page is displayed.
3. From the **Devices** > **Gateways** table, select the Gateway that you want to assign to a template

group.

4. Drag and drop the device to the template group that you just created.

Creating a Configuration Template for Gateways

A Gateway configuration template includes a set of common configuration commands that you can apply to multiple Gateway devices provisioned in a group.

Before you Begin

Before generating a configuration template:

- Familiarize with the CLI commands available on the device.
- Identify the commands that you want to use at the group level and the overrides required at the device level.
- Ensure that the Gateways are assigned to a template group.

Best Practices and Recommendations

Note the following recommendations when adding configuration text to a template:

- Verify the CLI syntax on the Gateway device before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- As the command text and definitions are case-sensitive, ensure that there are no errors or discrepancies in the CLI definitions.

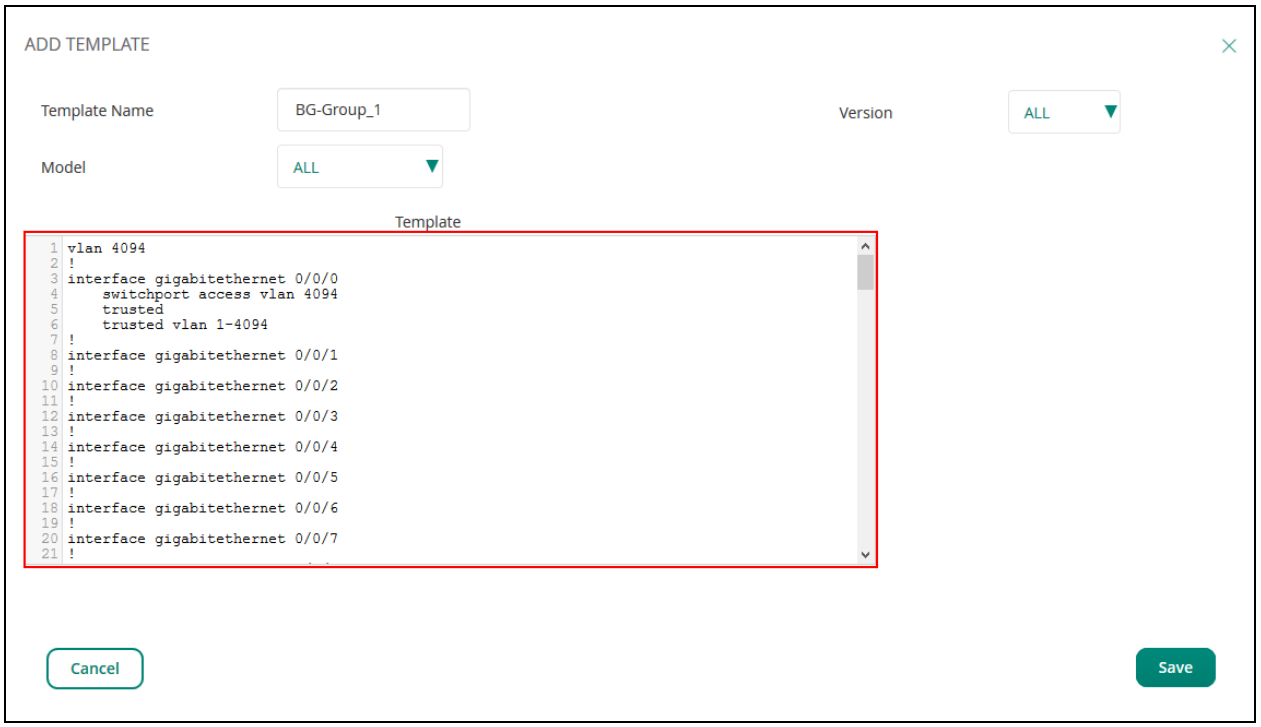
Configuration Steps

To create a template for the Gateways provisioned in a template group:

1. In the **Network Operations** app, set the filter to a group or Branch Gateway. Ensure that you select a group or Branch Gateway for which template-based configuration mode is enabled.
   - To select a Branch Gateway group in the filter:
     a. Set the filter to a group containing at least one Branch Gateway.
        The dashboard context for a group is displayed.
     b. Click **Gateways**.
     c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
   - To select a Branch Gateway in the filter:
     a. Set the filter to **Global** or a group containing at least one Branch Gateway.
     b. Under **Manage**, click **Devices** > **Gateways**.
        A list of gateways is displayed in the List view.
     c. Click a gateway under **Device Name**.
        The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**.
        The gateway configuration page is displayed.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Templates**. The **Templates** page opens.

4. Click **+** to add a new template. The **Add Template** page opens.
5. Add the template name.
6. Select a Gateway hardware model and the Aruba SD-WAN software version for which you want to apply the template.
7. To apply the template to all models and software versions of Gateways, select **All**.
8. Add the template text.

Figure 305 *Creating a Configuration Template*



9. Click **Save**. After you apply the configuration template, Gateways reboot and reconnect to Aruba Central with the new configuration.

Customizing a Template Using Variable Definitions

Variables in Aruba Central refer to the data set in the configuration template that can vary per device.

Aruba Central supports composing the variables in JSON and CSV formats. To add variable definitions, you can download a sample variable file from Aruba Central, add the definitions, and then upload it to Aruba Central.

To view a list of variables in a template, select the template row and click the edit or delete icon respectively.

Downloading a Sample Variables File

To download a sample variables file, complete the following steps:

1. In the **Network Operations** app, set the filter to a group or Branch Gateway. Ensure that you select a group or Branch Gateway for which template-based configuration mode is enabled.

- To select a Branch Gateway group in the filter:
  a. Set the filter to a group containing at least one Branch Gateway.
     The dashboard context for a group is displayed.
  b. Click **Gateways**.
  c. Click the **Config** icon to view the Branch Gateway group configuration dashboard.
- To select a Branch Gateway in the filter:
  a. Set the filter to **Global** or a group containing at least one Branch Gateway.
  b. Under **Manage**, click **Devices** > **Gateways**.
     A list of gateways is displayed in the List view.
  c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
  d. Under **Manage**, click **Device**.

2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Variables**
4. Select a file format. The supported file formats are JSON and CSV.
5. Click **Download Sample Variables File**.

Modifying a Variables File

Note the following conditions when modifying variable definitions:

- The **_sys_serial** and **_sys_lan_mac** are mandatory variables for specifying the serial number and MAC address of each device.
- The < or <= or > or >= operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as %if dpi_value > 2.8%, it is converted as %if dpi_value > 2 for comparison.
- The variable names should not include white space, and the special characters **#**, **&**, and **%**. The variable names must match regular expression [a-zA-Z0-9_]. If a variable defintion includes **%**, add a space before and after the **%** instance.
- The first character of the variable name must be an alphabet. Numeric values are not supported.
- If quotes are required, they must be included as part of the variable value.
- If you are using a CSV file for modifying variable definitions, the **modified** column must be set to **Y** to allow Aruba Central to parse the modified definition.

Uploading a Variables File

To upload a variables file, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or Branch Gateway. Ensure that you select a group for which template-based configuration mode is enabled.
   - To select a Branch Gateway group in the filter:
     a. Set the filter to a group containing at least one Branch Gateway.
2. Click **Gateways**.
   The dashboard context for a group is displayed.
   a. Click the **Config** icon to view the Branch Gateway group configuration dashboard.

3. To select a Branch Gateway in the filter:
   a. Set the filter to **Global** or a group containing at least one Branch Gateway.
   b. Under **Manage**, click **Devices** > **Gateways**.

      A list of gateways is displayed in the List view.
   c. Click a gateway under **Device Name**.

      The dashboard context for the gateway is displayed.
   d. Click a gateway under **Device Name**.
   e. Under **Manage**, click **Device**.
4. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
5. Click **Upload Variables File** and select the variables file to upload.
6. To verify if the variables are added in the template, go to **Gateway Management** > **Templates**.
7. Click the edit icon in the template. Verify the list of variables displayed in the **Edit Template** screen.

Sample Template and Variables Files

Template Text

The following example shows the contents of a Gateway configuration template:

```
vlan 4094
!
interface gigabitethernet 0/0/0
   switchport access vlan 4094
   trusted
   trusted vlan 1-4094
!
interface gigabitethernet 0/0/1
!
interface gigabitethernet 0/0/2
!
interface gigabitethernet 0/0/3
!
interface gigabitethernet 0/0/4
!
interface gigabitethernet 0/0/5
!
interface gigabitethernet 0/0/6
!
interface gigabitethernet 0/0/7
!
interface gigabitethernet 0/0/8
!
interface gigabitethernet 0/0/9
!
interface gigabitethernet 0/0/10
!
interface gigabitethernet 0/0/11
!
interface gigabitethernet 0/0/12
!
interface gigabitethernet 0/0/13
!
interface gigabitethernet 0/0/14
!
interface gigabitethernet 0/0/15
!
```

```
interface gigabitethernet 0/0/16
switchport access vlan %_vlan_id3_%
!
interface gigabitethernet 0/0/17
switchport access vlan %_vlan_id1_%
!
interface vlan 4094
   ip address dhcp-client
!
firewall
   dpi
   cp-bandwidth-contract trusted-ucast 65535
   cp-bandwidth-contract trusted-mcast 3906
   cp-bandwidth-contract untrusted-ucast 9765
   cp-bandwidth-contract untrusted-mcast 3906
   cp-bandwidth-contract route 976
   cp-bandwidth-contract sessmirr 976
   cp-bandwidth-contract vrrp 512
   cp-bandwidth-contract auth 976
   cp-bandwidth-contract arp-traffic 3906
   cp-bandwidth-contract l2-other 1953
!
mgmt-user admin root itsabug
interface vlan 4094
   ip address dhcp-client
!
hostname %_hostname_%
vlan %_vlan_id_%
interface vlan %_vlan_id_%
ip address %_ip_addr_% %_net_mask_%
!
controller-ip vlan %_vlan_id_%
!
wlan virtual-ap %_vap1_%
aaa-profile %_prof_name7_%
vlan %_vlan_id3_%
!
aaa server-group %_svr_grp1_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp2_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp3_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp4_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp5_%
auth-server %_svr1_%
!
aaa server-group %_svr_grp6_%
auth-server %_svr1_%
!
crypto-local pki ServerCert new_svr1_ocsp new_svr1_ocsp
crypto-local pki ServerCert SERVER-CERT SERVER-CERT
crypto-local pki TrustedCA pata_ca pata_ca
crypto-local pki rcp pata_ca
aaa authentication dot1x %_pdot1x_%
server-cert %_svr_cert_%
```

```
ca-cert %_ca_cert_%
!
aaa authentication-server radius %_svr1_%
!
vlan %_vlan_id1_%
wired aaa-profile %_prof_name7_%
!
aaa profile %_prof_name7_%
initial-role %_role1_%
dot1x-default-role %_role1_%
dot1x-server-group %_svr_grp1_%
!
aaa profile %_prof_name5_%
initial-role %_role1_%
dot1x-default-role %_role1_%
!
vlan %_vlan_id2_%
wired aaa-profile %_prof_name5_%
!
user-role %_role1_%
!
vlan %_vlan_id3_%
!
interface vlan %_vlan_id2_%
ip address %_ip_vlan2_% %_net_mask_%
!
ip access-list session %_acl1_%
!
aaa server-group %_svr_grp1_%
auth-server %_svr1_%
!
aaa authentication-server radius %_svr1_%
!
vlan 3434
!
netdestination peds-devices
   %if local_network_ip%
   range %local_network_ip%.91 %local_network_ip%.100
   range %local_network_ip%.101 %local_network_ip%.110
   %endif%
!
aaa profile %_prof_name8_%
%if role_group%
%role_group%
%endif%
!
aaa authentication captive-portal %_cap1_%
redirect-url "https://abc%xyz"
!
user
```

user

Sample Variables File

The following example shows the contents of a sample variables file in the JSON format:

```
"CG0011297": {
"_sys_lan_mac": "00:0B:86:dd:67:80",
"_sys_serial": "CG0011297",
"_hostname_": "Aruba7010_DD_67_80",
"_vlan_id_" : "700",
```

```
"_ip_addr_" : "1.70.70.10",
"_net_mask_" : "255.255.255.0",
"_vlan_id1_" : "225",
"_vlan_id2_" : "226",
"_vlan_id3_" : "227",
"_prof_name5_" : "prof5",
"_prof_name6_" : "prof6",
"_prof_name7_" : "prof7",
"_prof_name9_" : "prof9",
"_role1_" : "role1",
"_ip_vlan2_" : "1.27.26.10",
"_vap1_" : "vap1",
"_svr_grp1_" : "svr_grp1",
"_svr_grp2_" : "svr_grp2",
"_svr_grp3_" : "svr_grp3",
"_svr_grp4_" : "svr_grp4",
"_svr_grp5_" : "svr_grp5",
"_svr_grp6_" : "svr_grp6",
"_svr1_" : "svr1",
"_svr_cert_" :"new_svr1_ocsp",
"_ca_cert_" : "pata_ca",
"_pdot1x_" : "pdot1x",
"_server_ocsp3_" : "server_ocsp3",
"_acl1_" : "acl1",
"local_network_ip" : "34.34.54",
"_prof_name8_" : "prof8",
"role_group" : "initial-role role1\n dot1x-default-role role1",
"_cap1_" : "cap1",
"_url_" : "https://abc/%xyz",
"_role2_" : "\"test%role2\""
},
"CG0007810": {
"_sys_lan_mac": "00:0B:86:dB:B0:C0",
"_sys_serial": "CG0007810",
"_hostname_": "Aruba7010_DB_B0_C0",
"_vlan_id_" : "166",
"_ip_addr_" : "166.10.10.10",
"_net_mask_" : "255.255.255.0",
"_vlan_id1_" : "225",
"_vlan_id2_" : "226",
"_vlan_id3_" : "227",
"_prof_name5_" : "prof5",
"_prof_name6_" : "prof6",
"_prof_name7_" : "prof7",
"_prof_name9_" : "prof9",
"_role1_" : "role1",
"_ip_vlan2_" : "1.27.26.11",
"_vap1_" : "vap1",
"_svr_grp1_" : "svr_grp1",
"_svr_grp2_" : "svr_grp2",
"_svr_grp3_" : "svr_grp3",
"_svr_grp4_" : "svr_grp4",
"_svr_grp5_" : "svr_grp5",
"_svr_grp6_" : "svr_grp6",
"_svr1_" : "svr1",
"_svr_cert_" :"new_svr1_ocsp",
"_ca_cert_" : "pata_ca",
"_pdot1x_" : "pdot1x",
"_server_ocsp3_" : "server_ocsp3",
"_acl1_" : "acl1",
"local_network_ip" : "34.34.54",
```

```
"_prof_name8_" : "prof8",
"role_group" : "initial-role role1\n dot1x-default-role role1",
"_cap1_" : "cap1",
"_url_" : "https://abc/%xyz",
"_role2_" : "\"test%role2\""
}
```

Verifying Configuration Status

- To verify that Gateways are assigned to the template group and the configuration is pushed from Aruba Central, go to **Analyze** > **Audit Trail**.
- To view the configuration sync errors and overrides, use the **Configuration Audit** for Gateways. For more information, see Viewing Gateway Configuration Status.

Backing up and Restoring Templates

Aruba Central supports backing up and restoring configuration templates. The **Configuration Audit** page for Gateways allows you to back up the configuration templates and variables and restore these when required. For more information, see *Backing Up and Restoring Configuration Templates* in *Aruba Central Help Center*.

Chapter 28
Monitoring SD-Branch

After you set up the data center, branch sites, and configure devices deployed in the SD-Branch, the monitoring dashboards allow you to view the branch health and monitor the WAN uplink and gateway performance. This application also provides a dashboard for analyzing application usage by the clients connected in the WAN network. You can also view the branch topology, configure alerts, and create reports.

For more information on details, see the following topics:

- Gateway > Overview > Summary—View details of the gateways deployed in the WAN network.
- WAN Health—Global—View detailed information of the network health status and usage for the sites configured in your setup.
- WAN Health—Transport—View transport health of all uplinks belonging to an end-user.
- WAN Health—Site—View details of a specific site.
- Monitoring Sites in the Topology Tab—View a graphical representation of the network layout.
- Gateway Alerts—Configure and view gateway alerts.
- Reports—Create and view gateway reports.

Monitoring Gateway

You can monitor gateways in Aruba Central from all the available dashboards including **Global**, **Groups**, **Sites**, **Labels**, and **Gateways**.

For a snapshot of all the gateways configured at the global, group or site level, in either list or summary view, see the following topics:

- Monitoring Gateway in the List View
- Monitoring Gateways in the Summary View

Monitoring Gateways in List View

The **List** view for gateways is available from the **Global**, **Group**, **Site**, and **Label** dashboards. In all applicable dashboards, the **List** view is under **Manage** > **Devices** > **Gateways**.

To view the list of gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   Ensure that the selected option has at least one gateway configured.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.

List View

The list view displays the following tabs:

- **Gateways**—Displays the total number of gateways configured.
- **Online**—Displays a list of gateways that are online and connected to Aruba Central.
- **Offline**—Displays a list of Gateways that are currently down.

List View > Gateways

The **Gateways** table displays the following details for **Gateways**, **Online** and **Offline** tabs:

- **Device Name**—Displays the gateway name.
- **Model**—Displays the model of the gateway.
- **Firmware Version**—Displays the firmware version of the gateway.
- **Uptime**—Displays the time period for which the gateway has been functioning.
- **IP Address**—Displays the IP address of the gateway.
- **Site**—Displays the site information.
- **MAC**—Displays the MAC address of the gateway.
- **Group**—Displays the gateway group name.
- **Labels**—Displays the labels assigned to the gateway.
- **Serial**—Displays the gateway serial number.

Apart from the above fields, you can see the following fields if IDPS is enabled:

- **Inspection Engine**—The Aruba IDPS engine version number.
- **Ruleset**—The ruleset version currently running on the device.
- **Last Successful Ruleset Update**—The timestamp of the last successful ruleset update.
- **Ruleset Update Status**—The ruleset update status could be one of the following:
  - **Failed**
  - **Success**
  - **Initialized**

Click the download icon to download the gateways details as a .csv file. For more information, see Downloading Gateway Details.

Click the ellipsis icon to perform the following additional operations:

- Select the columns that you want to display in the table.
- Adjust the column width of the table to fit the page evenly.
- Reset the table view to the default columns.

Monitoring Gateways in Summary View

The **Summary** view for gateways is available from the **Global**, **Groups**, **Sites**, and **Labels** dashboards. In all applicable dashboards, the **Summary** view is under **Manage** > **Devices** > **Gateways**. Displays a graphical representation of the gateway operations.

To view the summary of gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   Ensure that the selected option has at least one gateway configured.

   The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Devices**>**Gateways**.
   A list of gateways is displayed in the **List** view.
3. Click the **Summary** icon.
   A graphical representation of the gateway operations is displayed.

You can change the time range by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

If you have just set up a gateway, you may not see relevant data immediately.

Summary View

The **Summary** view displays a graphical representation for the following:

- **Usage**—Displays the overall usage metrics for the gateways provisioned in your Aruba Central account. Displays the incoming and outgoing traffic for the gateways with time plotted on the x-axis. You can hover over the chart to see the incoming and outgoing traffic for a particular time frame.
- **WAN Compression**—Displays the data packet compression statistics for the WAN network. You can view the compressed, uncompressed, and saved bandwidth. By default, traffic between the Branch Gateway and VPNC is subject to compression. You can hover over the chart to see the compressed and uncompressed statistics for a particular time frame.
- **WAN Tag Provider Distribution**—Displays the number of online and offline uplinks per WAN provider.
- **WAN Transport Health**—Displays the Mean Opinion Score (MOS) score trends for each uplink for the selected time range. The uplink health trend is plotted using health indicators such as Good, Fair, and Poor. You can hover over the chart to see the uplink scores for a particular time frame. Click an uplink name to show or hide MOS score trends for that uplink.
- **WAN Type Provider Distribution**—Displays the number of online and offline uplinks per WAN circuit type.
- **Model Distribution**—Displays the total percentage of gateways distributed per hardware platform. You can hover over a donut slice to display the percentage for a specific hardware model. Click a hardware platform number to show or hide the distribution percentage for that platform.
- **Firmware Distribution**—Displays the total percentage of gateways distributed by software versions. Click a firmware number to show or hide the distribution percentage for that firmware.

Gateway > Overview > Summary

The **Summary** tab under **Manage** > **Overview** in the gateway dashboard displays the following three sections:

- Device Info
- WAN Summary
- Health Status

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.

3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.

4. Under **Manage**, click **Overview** > **Summary** .

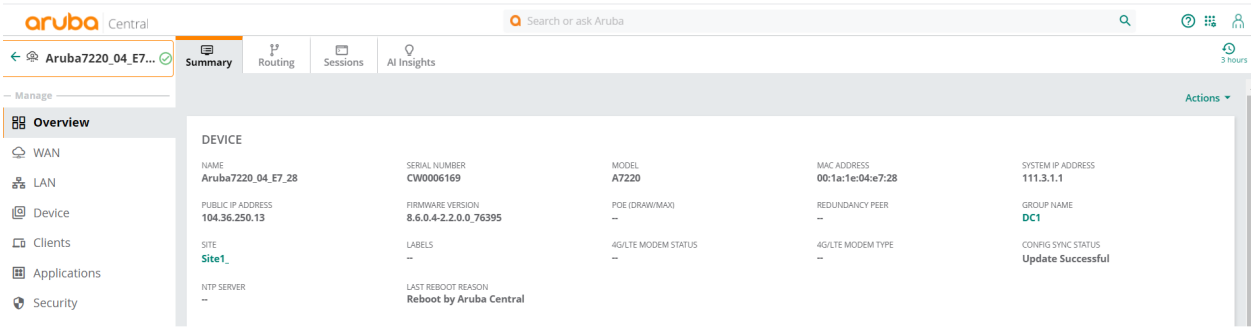
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Device Info

The **Device Info** section displays the following details.

Figure 306 *Device Info*



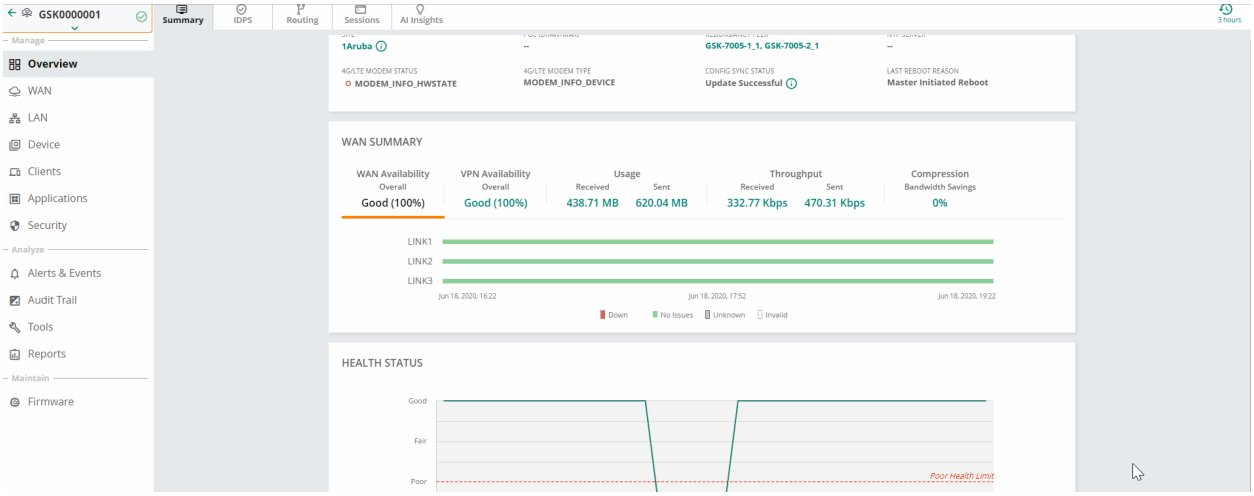
- **Name**—The name of the gateway.
- **Serial Number**—The serial number of the gateway.
- **Model**—The hardware model of the gateway.
- **MAC Address**—The MAC address of the gateway.
- **System IP address**—The IP address of the gateway.
- **Public IP address**—The public IP address of the gateway.
- **Firmware Version**—The firmware version running on the gateway. If a new version of the firmware is available, this information is also displayed. Clicking on the new firmware version redirects you to the **Maintain** > **Firmware** > **Gateways** page in the gateway dashboard, where you can select the gateway to be upgraded.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the Branch Gateway consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **Redundancy Peer**—Displays the redundant gateway if it is configured. Click the link to view the redundant gateway details.
- **Group Name**—The name of the group, if the gateway is configured as part of a group. Click the group name to go to the **Overview** > **Summary** page for that group.
- **Site**—The name of the site, if the gateway is configured as part of a site. Hover over the i icon to display the complete address of the site. Click the site name to go to the **Overview** > **Site Health** page for that site.
- **Labels**—The name of the label, if the gateway is configured as part of a single or multiple labels.

- **4G/LTE Modem Status**—Displays the modem connectivity status. The status shows only 'Connected' when the modem type is not internal.
- **4G/LTE Modem Type**—Displays the LTE connection type.
- **Config Sync Status**—The status of the configuration sync. Hover over the information icon to display the last successful configuration sync time.
- **NTP Server**—The name of the NTP server configured and its synchronization status.
- **Last Reboot Reason**—The reason for the last reboot.
- **Internal Modem Status** (Only for Gateway model: 9004-LTE)—Displays the name of the service provider and the signal strength. Hover over the information icon to view details about the active SIM, the IMEI number and the phone number.

WAN Summary

The **WAN Summary** section displays information of WAN Availability, VPN Availability, Usage, Throughput, and Compression.

Figure 307 *WAN Summary*



- **WAN Availability**—Provides a graphical representation of the WAN uplink availability for the Branch Gateway. The graph displays each WAN uplink availability for the selected time range. Availability is determined by the default gateway and monitored IP reachability. You can hover over the chart to see the WAN availability statistics for a particular time frame.
  - Red—Down
  - Yellow—(>50) Partial availability
  - Green—No Issues
  - Gray—Unknown
  - Dotted lines—Invalid
- **VPN Availability**—Provides a graphical representation of the VPNC reachability for the Branch Gateway. Availability is determined by the probe settings configured using the **Health Check** option.
  - Red—Down
  - Yellow—>50 percent availability
  - Green—No Issues

- Gray—Unknown
- Dotted lines—Invalid

- **Usage**—Displays the aggregate sent and received traffic usage by the WAN interface for the Branch Gateway. Displays the incoming and outgoing traffic for the gateways with time plotted on the x-axis. You can hover over the chart to see the incoming and outgoing traffic for a particular time frame. Select one of the following options from the drop-down list:
  - All
  - Internet
  - VPN

Click the following icons to see the chart in logarithmic scale or linear scale.

- Logarithmic Scale—Click this icon to view chart in logarithmic scale.
- Linear Scale—Click this icon to view chart in linear scale.

Click **Received** or **Sent** at the bottom of the chart to view or hide the usage chart for received or sent data.

- **Throughput**—Provides a graphical representation of the aggregated WAN interfaces throughput. The graph displays the transmit and receive performance in bps for a WAN interface. Displays the incoming and outgoing traffic for the gateways with time plotted on the x-axis. You can hover over the chart to see the received and sent throughput for a particular time frame.

Click the following icons to see the chart in logarithmic scale or linear scale.

- Logarithmic Scale—Click this icon to view chart in logarithmic scale.
- Linear Scale—Click this icon to view chart in linear scale.

Click **Received** or **Sent** at the bottom of the chart to view or hide the usage chart for received or sent data.

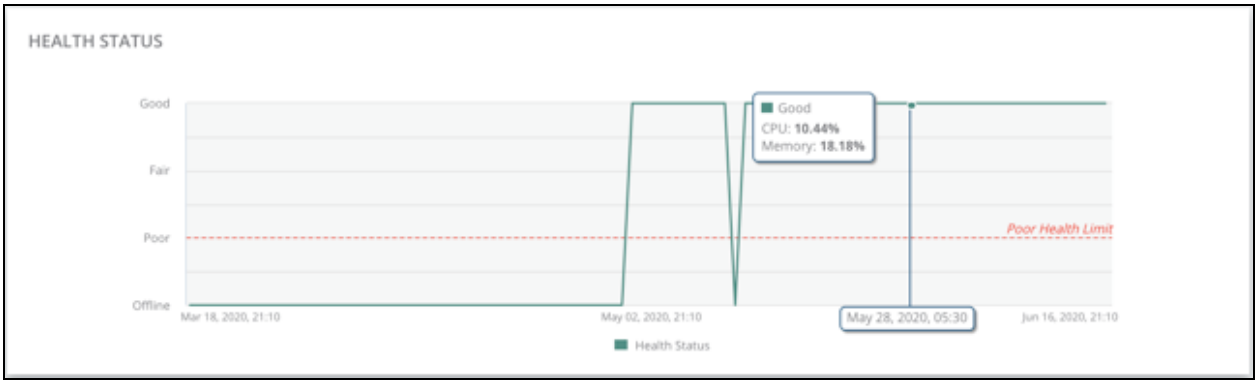
- **Compression**—Displays the aggregate WAN compression details across all uplinks. The average bandwidth savings is displayed as a percentage. The compressed and uncompressed bandwidth is displayed as vertical grouped bar graphs. You can hover over the chart to see the bandwidth savings statistics for a particular time frame.
  - Gray—Optimized
  - Red—Non Optimized

Health Status

The **Health Status** section displays the health of the gateway in terms of CPU, Memory, and device connectivity to Aruba Central.

The health status is plotted using health indicators such as Good, Fair, Poor, and Offline. You can hover over the chart to see the health status for a particular time frame.

Figure 308 *Health Status*



NOTE

The default view of gateways table shows only a few columns. To view the hidden columns, click the settings icon at the right side of the table. To reset the columns, click **Reset Columns**.

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

1. Under **Manage**, click **Devices** > **Gateways**.
2. Click a gateway under **Device Name**.
3. Under **Manage**, click **Overview.** By default, the **Summary** tab is displayed.

- **WAN**—Displays the total number of WAN interfaces that are currently operational or down. On clicking a port, the dashboard displays WAN interface details.
- **LAN**—Displays the total number of LAN interfaces that are currently operational or down. On clicking a port, the dashboard displays LAN and VLAN interface details.
- **Tunnels**—Displays the total number of VPN tunnels that are currently active or down. On clicking a port tunnel, the dashboard displays VPN tunnel details.
- **IDPS**—Displays details pertaining to the IDPS traffic inspection engine health and the number of packets dropped. The **IDPS** tab is displayed for 9004 gateways with a valid IDPS subscription.
- **Routing**—Displays details pertaining to the routing protocols such as BGP, OSPF, RIPv2 and Overlay.
- **Path Steering**—Displays the total number of path steering policies that are compliant with the performance criteria (SLAs) defined for each type of traffic.
- **Sessions**—Displays detailed information about the running sessions.

- **AI Insights**—Displays a report of network events that could possibly affect the quality of the overall network performance.
- **Alerts**—Displays the total number of open alerts that are yet to be acknowledged.

Gateways > Overview > IDPS

The **IDPS** tab under **Manage** > **Overview** in the gateway dashboard displays the following sections:

- Traffic Inspection Engine Status
- Traffic Inspection Engine CPU Usage
- Traffic Inspection Engine Memory Usage
- Dropped Packets

After you on-board the gateways and configure IDPS, you can view the IDPS traffic engine health and the number of packets dropped.

Viewing the Overview > IDPS Tab

To navigate to the **IDPS** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites** that has IDPS supported gateways. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.
   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **IDPS** .

To exit the gateway dashboard, click the back arrow on the filter.

You can change the time range for the **IDPS** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

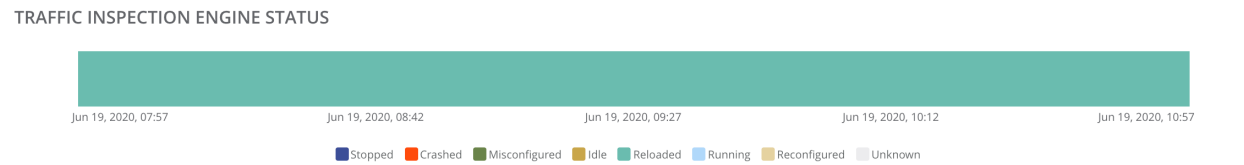
To set the charts to show data for specific duration, use the options in the time range filter. By default, the data is displayed for a duration of 3 hours. To view the graphs for different durations, click the time filter icon and select a time range of your choice. You can view data for 3 hours, 1 day, 1 week, 1 month, or 3 months. The **IDPS** tab is displayed for 9004 gateways with a valid IDPS subscription.

Traffic Inspection Engine Status

The **Traffic Inspection Engine Status** chart displays the status of the traffic inspection engine for the selected period in a timeline chart. Hover over the graph to view the status of the traffic inspection engine at a particular time. The legends represent different status of the traffic inspection engine.

The **Traffic Inspection Engine Status** chart is available for a period of 3 hours, 1 day, 1 week, or 1 month.

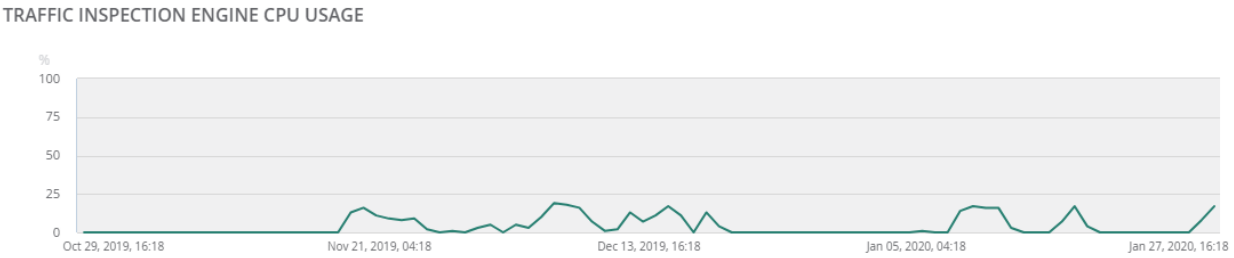
Figure 309 *Traffic Inspection Engine Status*



Traffic Inspection Engine CPU Usage

The **Traffic Inspection Engine CPU Usage** chart displays the CPU usage percentage of the traffic inspection engine for the selected period in a line chart. Hover over the graph to view the CPU usage percentage at a particular time.

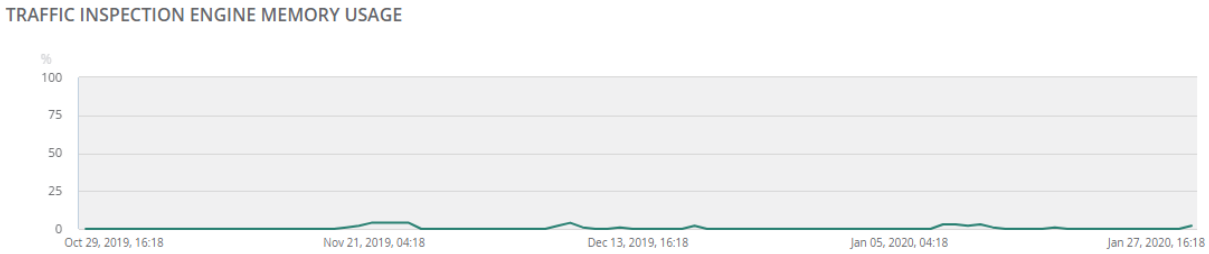
Figure 310 *Traffic Inspection Engine CPU Usage*



Traffic Inspection Engine Memory Usage

The **Traffic Inspection Engine Memory Usage** chart displays the percentage of memory usage by the traffic inspection engine for the selected period in a line chart. Hover over the graph to view the memory usage percentage at a particular time.

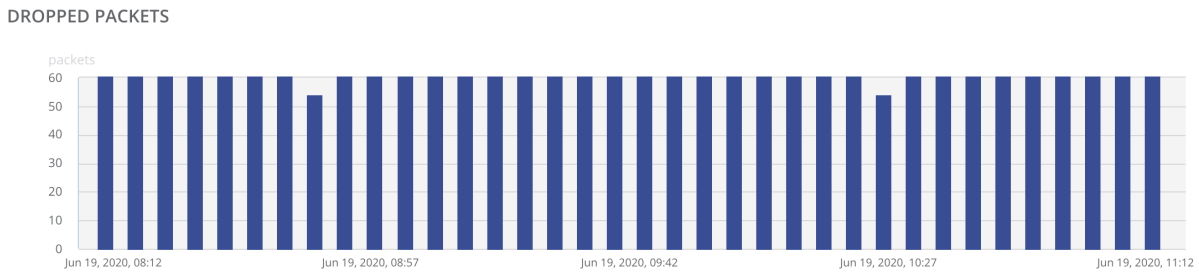
Figure 311 *Traffic Inspection Engine Memory Usage*



Dropped Packets

The **Dropped Packets** chart displays the number of packets dropped for the selected period in a vertical bar chart. Hover over the graph to view the packets dropped at a particular time.

Figure 312 *Dropped Packets*



Gateway > Overview > Routing

The **Routing** tab under **Manage** > **Overview** in the gateway dashboard displays the following sections:

- Gateway > Overview > Routing > Route Table
- Gateway > Overview > Routing > BGP
- Gateway > Overview > Routing > OSPF
- Gateway > Overview > Routing > Overlay
- Gateway > Overview > Routing > RIP

Viewing the Overview > Routing Tab

To navigate to the **Routing** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** .

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Gateway > Overview > Routing > Route Table

The **Route Table** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- Routes Summary
- Routes

Viewing the Overview > Routing > Routes Table Tab

To navigate to the **Routes Table** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **Routes Table**.

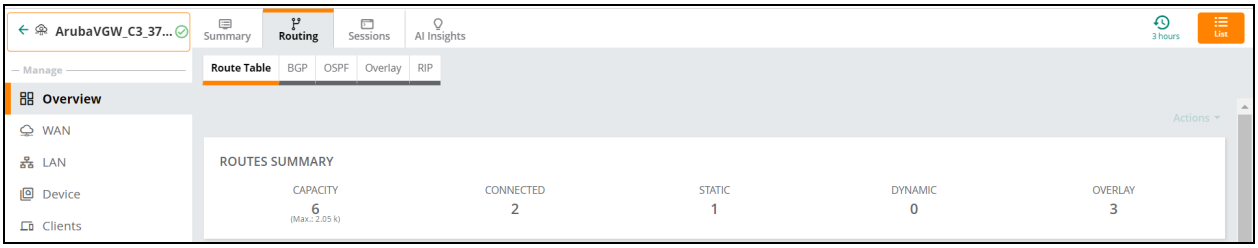
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Routes Table** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Routes Summary

- **Capacity**—Number of routes currently configured. Also displays the maximum number of allowed routes.
- **Connected**—Number of connected routes.
- **Static**—Number of static routes.
- **Dynamic**—Number of dynamic routes.
- **Overlay**—Number of overlay connections.

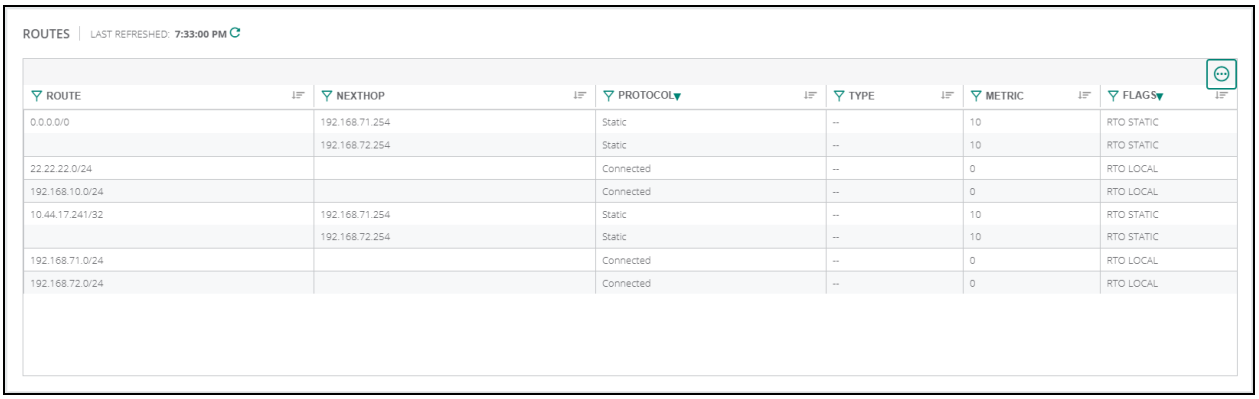
Figure 313 *Routes Summary*



Routes

- **Last Refreshed**—Indicates the time, in hr:mm:ss format, when the routes were last refreshed.
- **Prefix**—Controller prefix for the route.
- **Length**—Prefix length.
- **Address**—Destination IP address of the route.
- **Route**—The route IP address and subnet.
- **Nexthop**—The IP address of the next hop.
- **Protocol**—Routing protocol. Possible values are Unknown, Connected, Static, IKE, Overlay, BGP, OSPF, BOC, RAPNG, RIP, VPN, Application and Default
- **Type**—The type of connection.
- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
- **Flags**—Route flags that indicate the flags for the selected routes.

Figure 314 *Routes details*



NOTE

Click the settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to type in an applicable value, and then display the corresponding row. For Protocol column you can select a value from the drop-down list.

Click the icon on on each column header row to arrange the data in ascending or descending order.

Click the refresh icon on the Routes table to refresh the table data.

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Overview > Routing > BGP

The **BGP** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- BGP Summary
- BGP Details
- BGP Details > Neighbors
- BGP Details > Routes

Viewing the Overview > Routing > BGP Tab

To navigate to the **BGP** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in List view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **BGP**.

   To exit the gateway dashboard, click the back arrow on the filter.

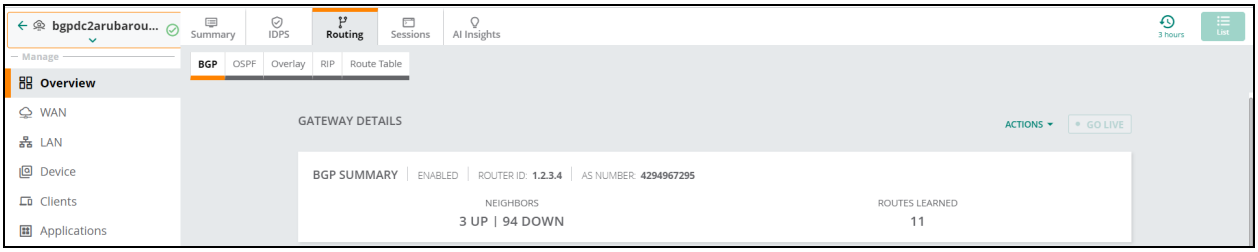
   You can change the time range for the **BGP** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

BGP Summary

The **BGP Summary** section displays the following information:

- **Router ID**—Displays the Router ID.
- **AS Number**—Displays the private Autonomous System (AS) number.
- **Neighbors**—Displays the number of neighboring connections.
- **Routes Learned**—Displays the number of routes that have been learned.

Figure 315 *BGP—Summary*



BGP Details

The **BGP Details** section displays the information categorized by **Neighbors** and **Routes**.

BGP Details > Neighbors

- **Total Neighbors**—Displays the total number of neighbors.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Neighbor**—Displays the available neighbors.
- **ASN**—Displays the private Autonomous System (AS) number.
- **State**—Displays the current state.
- **Type**—Neighbor type.
- **Last State Change**—Displays the last state change.
- **Down Count**—Displays the number of neighbors that are down.
- **Up Count**—Displays the number of neighbors that are up.
- **Hold Time**—Displays the time spent on hold.
- **Keep Alive Interval**—Displays the time set for the Keep Alive Interval.

- **Router ID**—Displays the Router ID.
- **Neighbor Version**—Displays the firmware version of the connected neighbors.
- **IP Precedence Value**—Displays the IP precedence.
- **Datagrams (Max = 1400Bytes)**—Displays existing datagrams.
- **Route Refresh**—Displays the latest route refresh.
- **Graceful Restart Capability**—Displays whether graceful restart is supported.
- **BGP Addtl-Paths Computation**—Displays the additional paths computation.
- **Recv Paths**—Displays the receive path information. A red dot in this field indicates that the number of routes received has exceeded the configured limit. Hover over for more information.
- **Send Paths**—Displays the send path information. Clicking the number of routes opens the **Routes Advertised** table which displays the routes advertised to that neighbor.
- **Sent**—Displays the number of routes sent.
- **Received**—Displays the number of routes received. Clicking the number of routes opens the **Routes Learned** table. This table displays a small red circle if the number of routes received exceeds the configured route limit and the corresponding action being taken on the routes (**Drop** or **Warning**) as configured in the BGP configuration page.
- **Recv Path Limit**—Displays the Route Limit per neighbor configured in the BGP configuration page.
- **Recv Path Action**—Displays the action specified in the BGP configuration page when the number of routes exceeds the route limit.
- **Source Address**—Displays the source information.
- **Nexthop**—Displays information about the next hop.
- **Link Address**—Displays the link address.
- **CFfg Hold Time**— Displays the minimum acceptable hold time.
- **CFfg Keep Alive Time**— Displays the configuration keep alive time.
- **IS Route Reflector**—Displays the net hop path.
- **IS Router Server**—Displays the IS Router Server details.
- **BGP Advertise-Best_External**—Displays the backup external route.
- **Up Time**—Displays the time that the connection has been up.

Figure 316 *BGP—Neighbors Details*

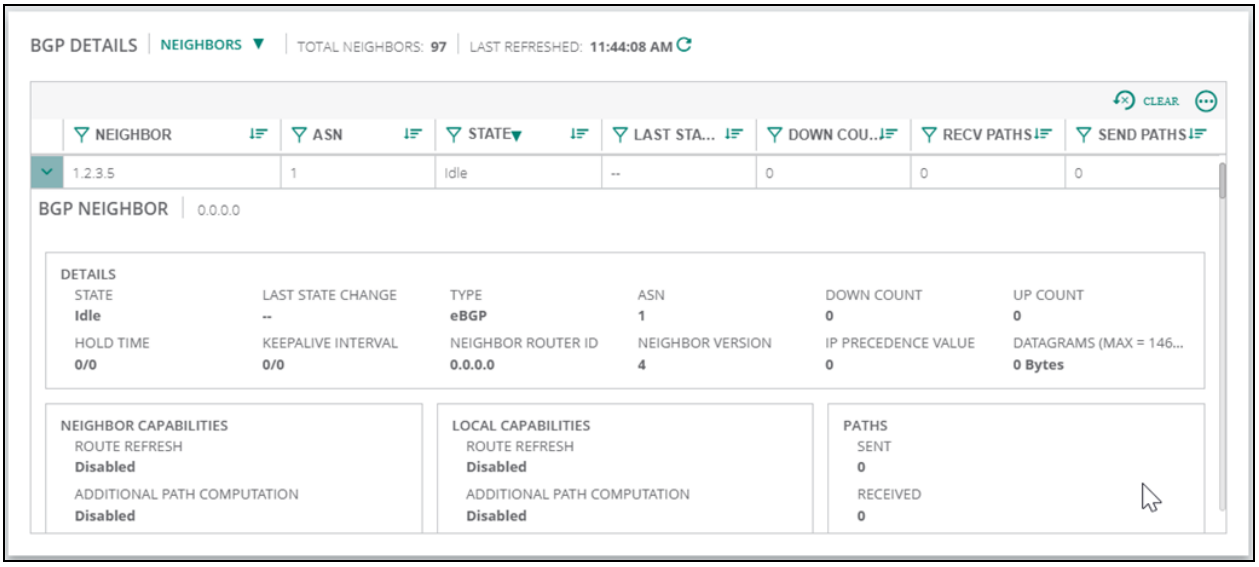
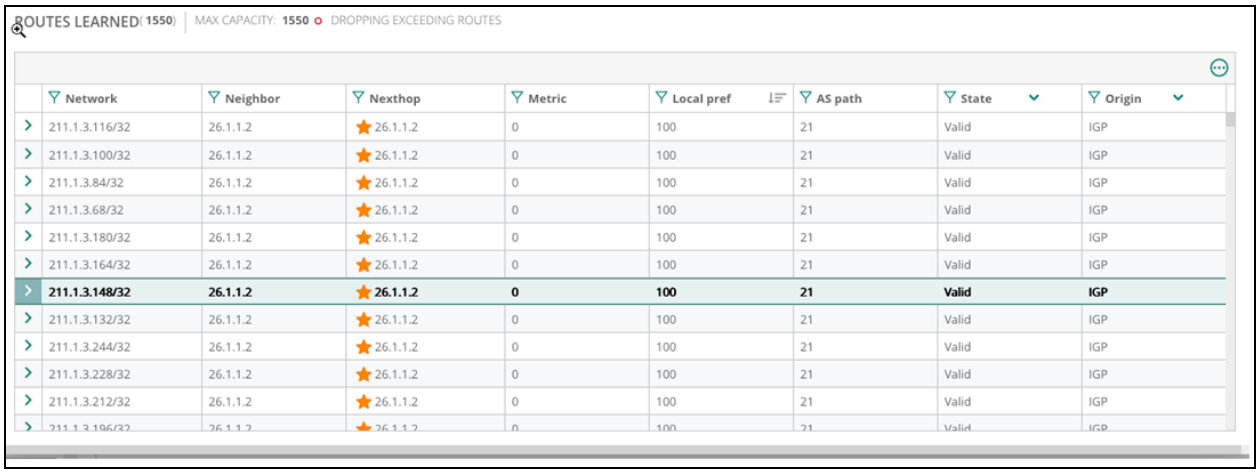


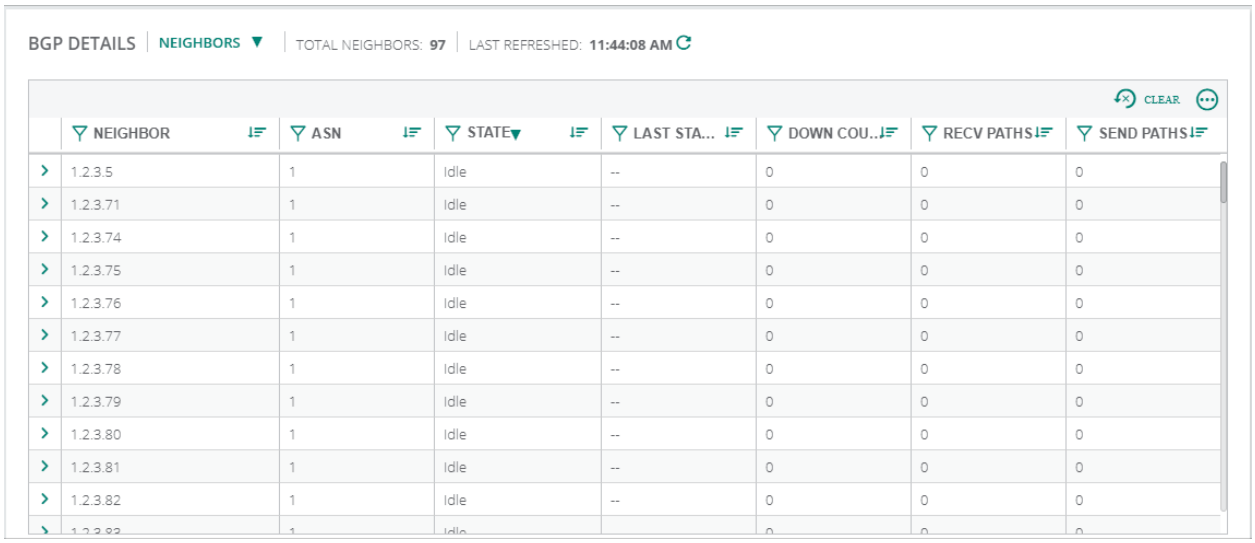
Figure 317 *BGP Routes Learned*



Clear Neighbor Sessions

- The **Clear** button allows you to clear BGP neighbor sessions.
- **Clear a neighbor session**—To clear a specific neighbor session, use the **Clear** button available for that particular neighbor row.
- **Clear all neighbor sessions**—To clear all neighbor sessions, use the **Clear** button available on the table header.

Figure 318 *BGP—Clear Neighbors*

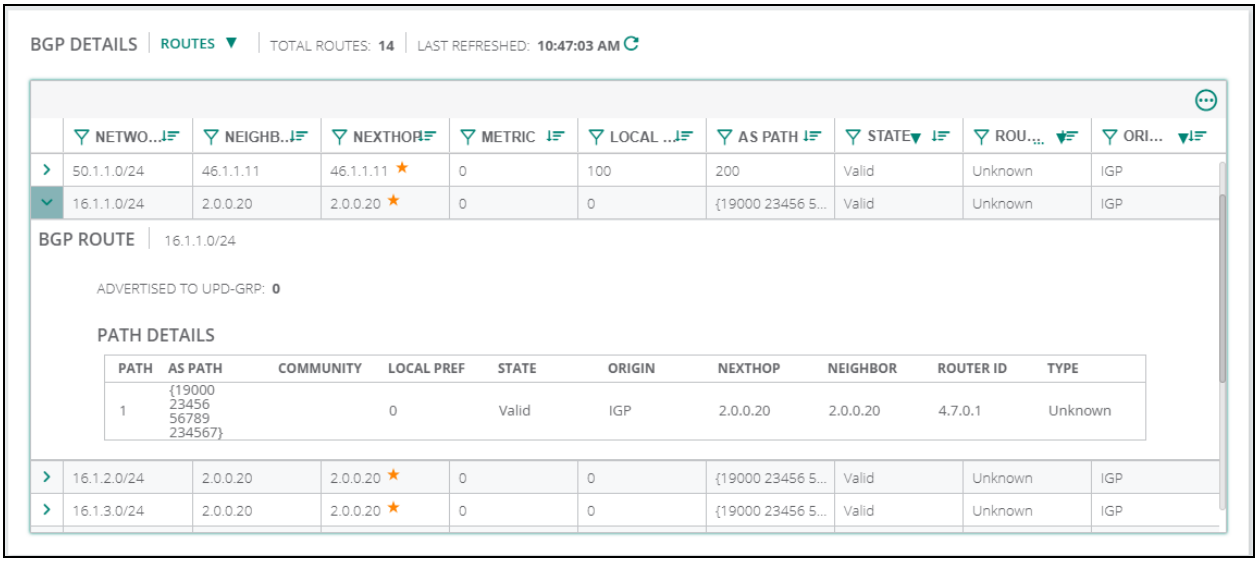


BGP Details > Routes

- **Total Routes**—Displays the total number of routes.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Network**—Connected network.
- **Neighbor**—Displays the available neighbors.
- **Nexthop**—Displays information about the next hop.

- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
- **Local Pref**—Displays the outbound external path.
- **AS Path**—Displays the private Autonomous System path.
- **State**—Displays the connection state of the connection.
- **Route Source**—Displays the specific route the packet should take.
- **Origin**—Displays the origin attribute value.
- **Advertised to Upd-Grp**—Displays the Advertised Update-Group status.
- **Router ID**—Displays the router ID.

Figure 319 *BGP—Routes Details*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Gateway > Overview > Routing > OSPF

The **OSPF** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- OSPF Summary
- OSPF Details

Viewing the Overview > Routing > OSPF Tab

To navigate to the **OSPF** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **OSPF**.

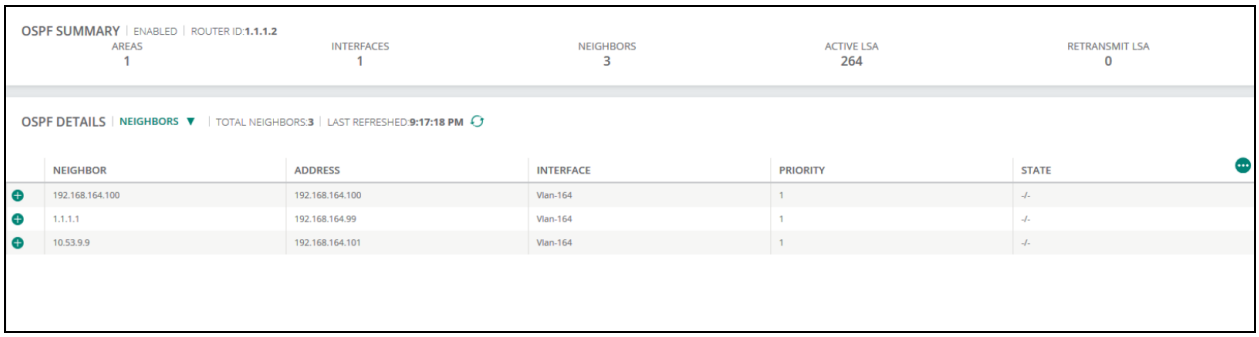
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **OSPF** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

OSPF Summary

- **Status**—Status is either Enabled or Disabled.
- **Router ID**—The routers identification details.
- **Areas**—Area type as specified in the OSPF parameters.
- **Interfaces**—Displays the current interface.
- **Neighbors**—Displays the number of neighbors available.
- **Active LSA**—Displays the Active Link-State Advertisements.
- **Retransmit LSA**—Displays the Retransmitted Link-State Advertisements.

Figure 320 *OSPF—Summary*



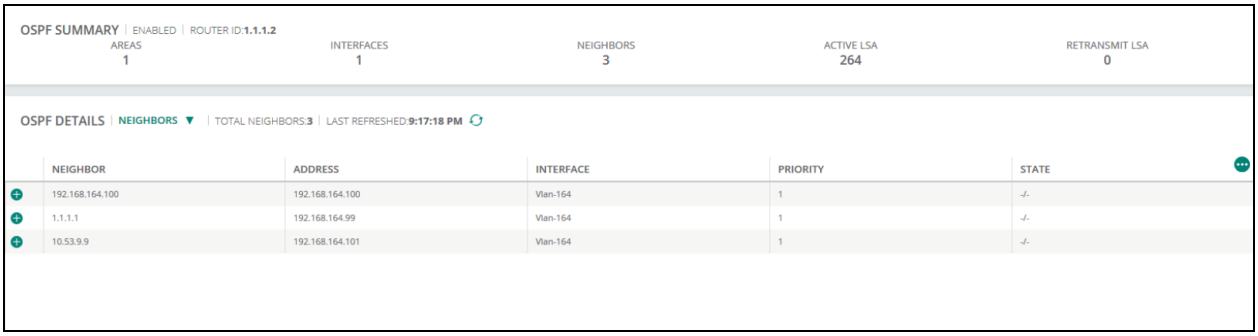
OSPF Details

Displays the information categorized by **Neighbors**, **Interfaces**, **Areas**, and **Link State Databases**.

- **Neighbors**
  - **Total Neighbors**—The total number of neighbors.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Neighbor**—Details of the neighbors.
  - **Address**—IP address of the neighbor.

- **Interface**—Displays the current interface for the neighbor.
- **Priority**—Displays the priority of each neighbor.
- **State**—Displays the state of the connection.
- **Area**—Displays the area of the neighbor.
- **Options**—Available neighbor options.
- **Dead Timer**—Displays the required time to wait before the neighbor connection is dead.
- **Retransmit Timer**—Displays the time between OSPF and LSA retransmissions.

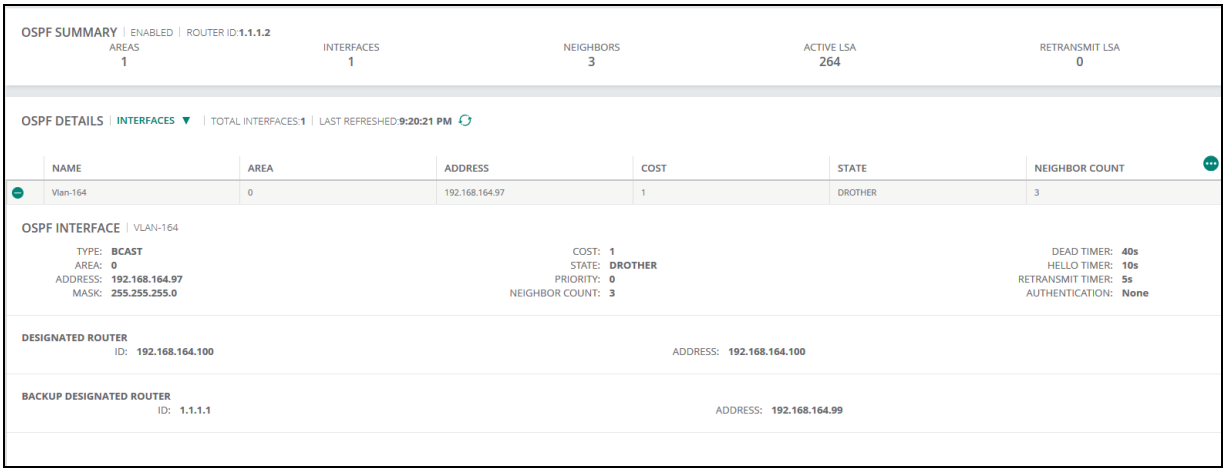
Figure 321 *OSPF—Neighbor details*



- **Interfaces**
  - **Total Interfaces**—The total number of interfaces.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Name**—Name of the interface.
  - **Area**—Displays the logical collection of devices that share the same area.
  - **Address**—IP address of the interface.
  - **Mask**—IP mask of the interface.
  - **State**—Displays the state of the connection.
  - **Type**—Displays the type of connection.
  - **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
  - **Neighbor Count** —Displays the number of neighbors.
  - **ID**—Displays the interface ID.
  - **Address**—Displays the IP address of the interface.
  - **Priority**—Displays the priority of the interface to determine the default router.
  - **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.
  - **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
  - **Retransmit Timer** —Displays the retransmit interval time for link state advertisements.
  - **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.
    Click on an interface listed in the table to view the following details:
  - **Type**—Displays the type of connection.
  - **Area**—Displays the logical collection of devices that share the same area.
  - **Address**—IP address of the interface.
  - **Mask**—IP mask of the interface.

- **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
- **State**—Displays the state of the connection.
- **Priority**—Displays the priority of the interface to determine the default router.
- **Neighbor Count**—Displays the number of neighbors.
- **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
- **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.
- **Retransmit Timer**—Displays the retransmit interval time for link state advertisements.
- **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.

Figure 322 *OSPF— Interfaces details*



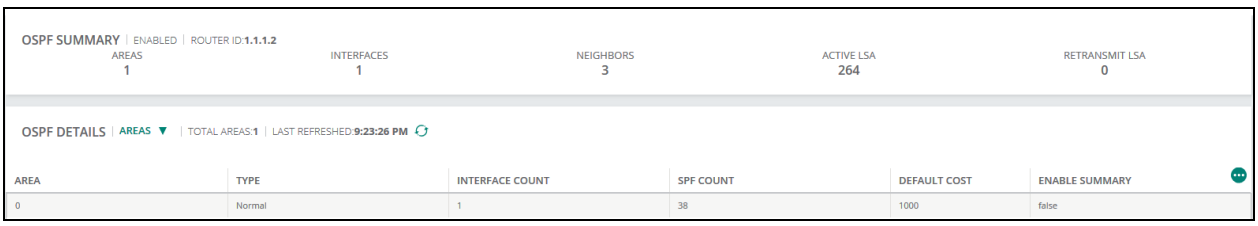
Areas

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Areas**—The total number of areas.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Area**—Displays the logical collection of devices that share the same area.
- **Type**—Displays the type of connection.
- **Interface count**—Displays the interface count.
- **SPF Count**—Displays the Shortest Path First count.
- **Enable Summary**—Displays if summary collection is enabled.

Figure 323 *OSPF— Areas details*



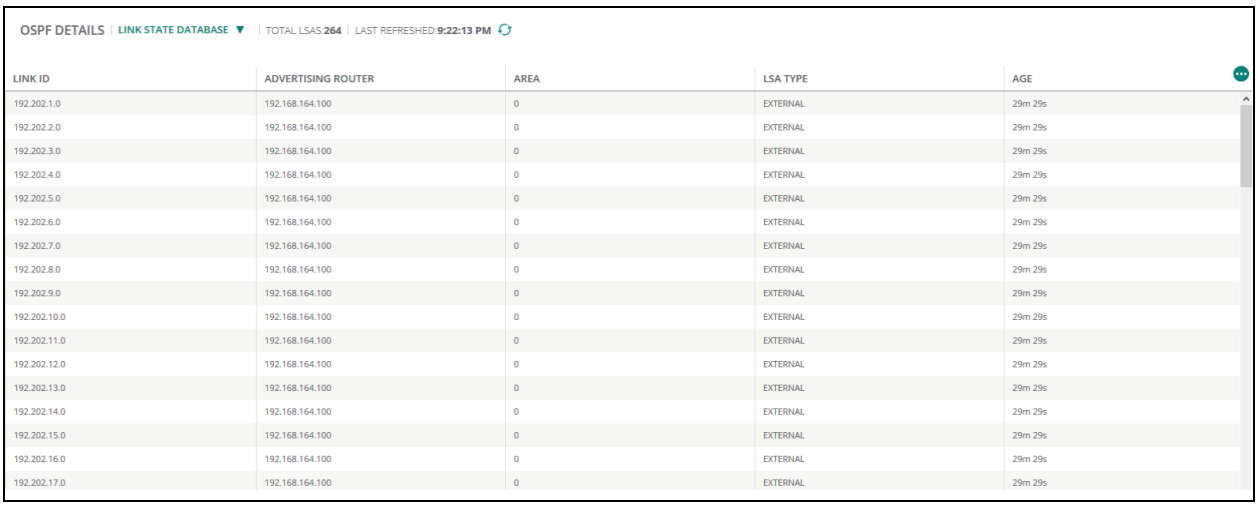
- **Link State Databases**

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

  - **Total Link State Database**—The total number of Link State Databases.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Link ID**—Displays the router ID of the originating router.
  - **Advertising Router**—Displays the routes that is advertising the link-state.
  - **Area**—Displays the logical collection of devices that share the same area.
  - **LSA Type**—Displays the aggregation type.
  - **Age**—Displays the age of the OSPF LSA.
  - **State**—Displays the state of the connection.
  - **Seq No.**—Displays the 32-bit OSPF Sequence number.
  - **Checksum**—Displays the 16-bit checksum for the OSPF packet.

Figure 324 *OSPF—Link State Databases details*



- **LSA types**—There are various LSA types available and they are listed here:
  - **Router**—The Router page displays the following details:
    - Flags
    - Link ID
    - Link Data
    - Link Type
    - Metric
  - **Network**—The Network page displays the following details:
    - Mask
    - Attached router
  - **Network Summary**—The Network Summary page displays the following details:
    - Address
    - Mask
    - Metric

- **ASBR Summary**—The ASBR Summary page displays the following details:
  - ASBR
  - Metric
- **External**—The External page displays the following details:
  - Mask
  - Metric
  - Type
  - Route Tag
  - Forwarding Address

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Overview > Routing > Overlay

The **Overlay** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- Overlay Summary
- Overlay Details

Viewing the Overview > Routing > Overlay Tab

To navigate to the **Overlay** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **Overlay**.

   To exit the gateway dashboard, click the back arrow on the filter.

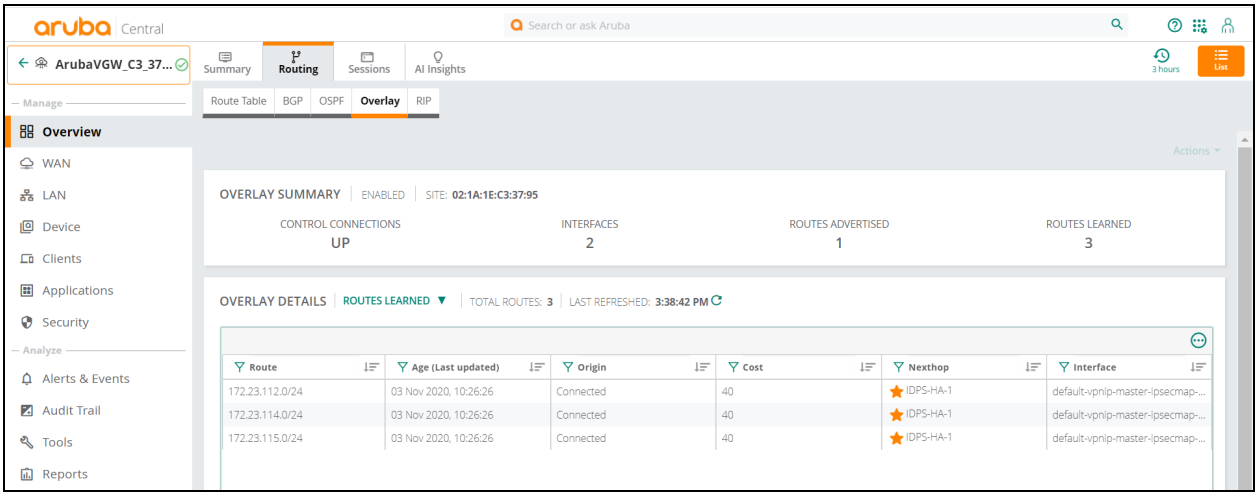
NOTE

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

Overlay Summary

- **Status**—Status is either Enabled or Disabled.
- **Site**—Displays the site location.
- **Control Connections**—Displays the control connection as either **Up** or **Down**.
- **Interfaces**—Displays the number of active interfaces.
- **Routes Advertised**—Displays the number of routes that are advertised.
- **Routes Learned**—Displays the number of routes that are learned.

Figure 325 *Overlay—Summary*



Overlay Details

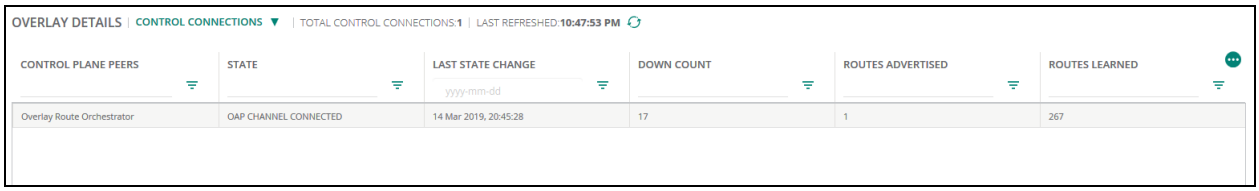
- Displays the information categorized by **Control Connections**, **Interfaces**, **Routes Advertised**, and **Routes Learned**.
- **Control Connections**

NOTE

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

  - **Total Control Connections**—Displays the total number of control connections.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Control Plane Peers**—Displays the Control Plane Peers.
  - **State**—Displays the state of the connection.
  - **Last State Change**—Indicates the Last State Change.
  - **Down Count**—Displays the Down Count.
  - **Routes Advertised**—Displays the advertised routes.
  - **Routes Learned**—Displays the number of routes that are learned.

Figure 326 *Overlay Details —Control Connections*



- **Interfaces**

NOTE

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

- **Total Interfaces**—Displays the total number of interfaces.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Interfaces**—Displays the number of active interfaces.
- **State**—Displays the state of the interface.
- **Tunnel Destination**—Displays the destination address.
- **Uptime**—Amount of time the tunnel has been active since it was last reset.
- **Routes Learned**—Displays the number of routes that are learned.

Figure 327 *Overlay Details —Interfaces*

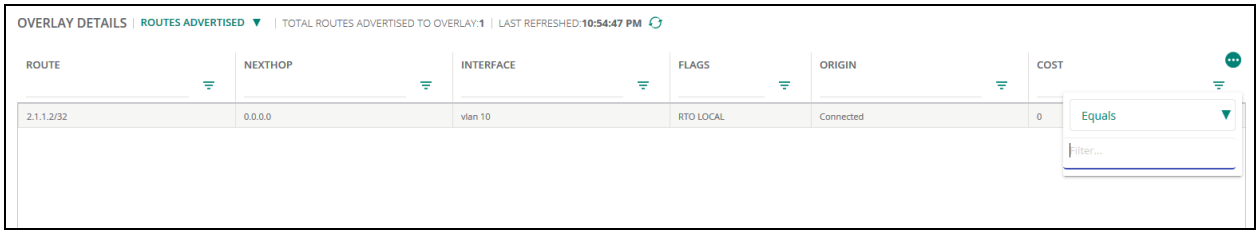
- **Routes Advertised**

NOTE

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

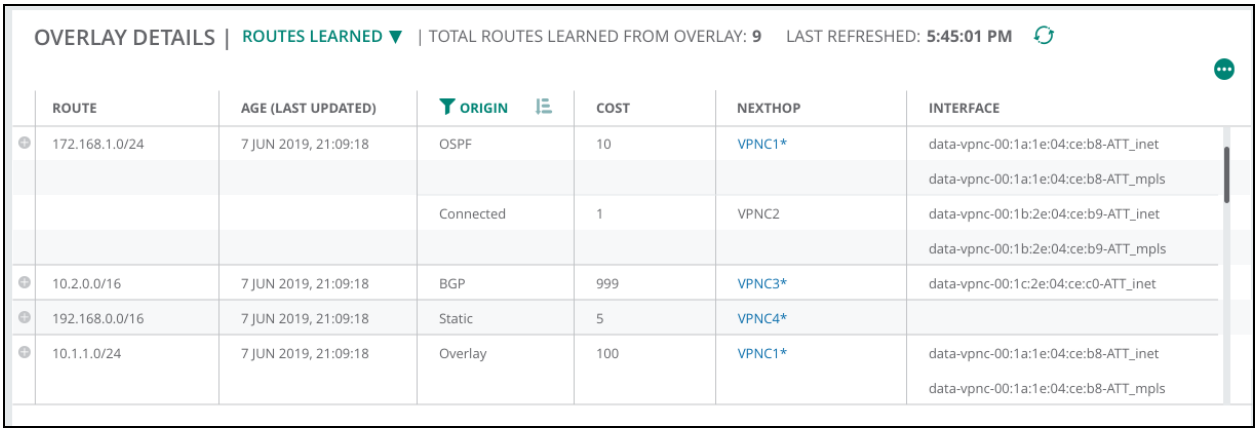
- **Route**—Displays the route name.
- **Nexthop**—Displays information about the next hop.
- **Interface**—Displays the number of active interfaces.
- **Flags**—Lists the number of active flags.
- **Origin**—Origin of the route.
- **Cost**—Cost associated with the route.

Figure 328 *Overlay Details—Routes Advertised*



- **Routes Learned**
- **Total Routes Learned**—Displays the total number of routes that are learned.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Route**—The route IP address aand subnet.
- **Age (Last Updated)**—Last updated date.
- **Origin**—Orging of the connection, for example, Connected or Overlay.
- **Flags**—Lists the number of active flags.
- **Nexthop**—Displays information about the next hop.
- **Interface**—Displays the number of active interfaces.

Figure 329 *Overlay Details—Routes Learned*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Overview > Routing > RIP

The **RIP** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- RIP Summary
- RIP Details

Viewing the Overview > Routing > RIP Tab

To navigate to the **RIP** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **RIP**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **RIP** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

RIP Summary

The **RIP Summary** section displays the following information:

- **Enabled**—Implies that RIPv2 is enabled on the gateway device.
- **Version**—Displays the RIP version, RIPv1 or RIPv2. Currently, Arubasupports only RIPv2.
- **Interfaces**—Displays the number of interfaces that participates in the routing process.
- **Neighbors**—Displays the number of neighboring connections.
- **Routes**—Displays the number of routes advertised.
- **ECMP**—Displays the number of ECMPs available.
- **Infinity**—The hop count (16) assigned to unreachable devices (typically, any route that requires more than 15 hops).
- **Timers**—RIP uses timers to regulate its performance:
  - **Update** timer displays the interval between periodic routing updates. By default this is set to 30 seconds.
  - **Invalid** timer displays the time in seconds after which the route is marked invalid but is still available in the table. By default this is set to 180 seconds.
  - **Flush** timer displays the time duration after which the route is flushed out or removed from the table. By default this is set to 120 seconds.

Figure 330 *RIP—Summary*

RIP Details

Displays the information categorized by **Interfaces**, **Neighbors**, and **Routes**.

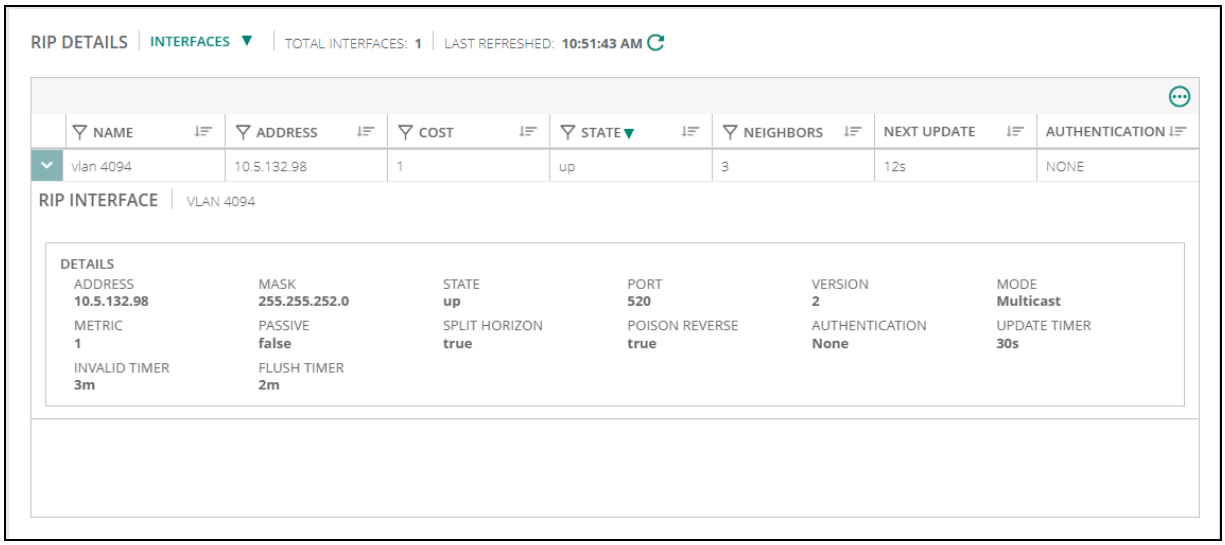
- **Interfaces**
  - **Name**—Displays the name of the interface.
  - **Address**—Displays the IP Address of the interface.
  - **Cost**—Displays the cost associated.

- **State**—Displays the state of the connection (Up pr Down).
- **Neighbors**—Displays the number of neighbors.
- **Authentication**—Displays the status of this option that is used for enabling RIP authentication mode for MD5.
- **Next Update**—Time in seconds for the next update

Click on an interface listed in the table to view the following details:

- **RIP Interface**—Displays the name of the interface.
- **Address**—Displays the IP Address of the interface.
- **Mask**—Displays the subnet mask.
- **State**—Displays the state of the connection (Up or Down).
- **Port**—Displays the port number of the interface.
- **Version**—Displays the RIP protocol version.
- **Mode**—Displays the interface configuration mode.
- **Metric**—Displays the number of hop counts.
- **Passive**—Indicates whether the interface is operating in passive mode.
- **Split Horizon**—Indicates whether Split Horizon is implemented.
- **Poison Reverse**—Indicates whether Poison Reverse is implemented.
- **Authentication**—Displays the status of this option that is used for enabling RIP authentication mode for MD5.
- **Update Timer**—Displays the interval between periodic routing updates, by default this is set to 30 seconds.
- **Invalid Timer**—Displays the time in seconds after which the route is marked invalid but is still available in the table.
- **Flush Timer**—Displays the time duration after which the route is flushed out or removed from the table.

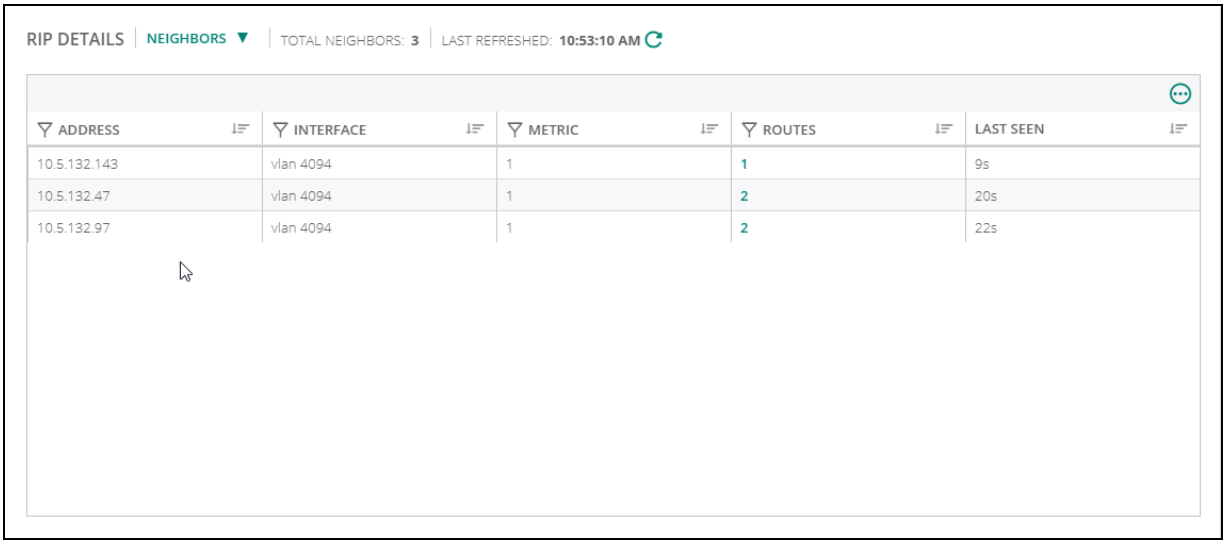
Figure 331 *RIP—Interfaces Details*



- **Neighbors**
  - **Address**—Displays the IP address of the neighbor.
  - **Interface**—Displays the name of the interface.

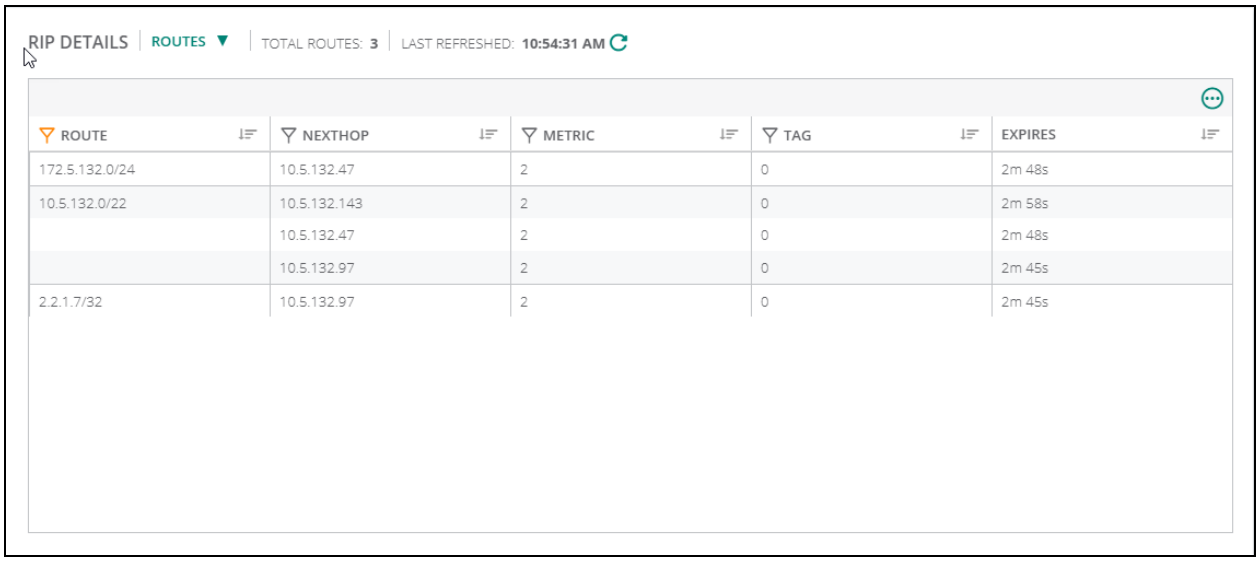
- **Metric**—Displays the number of hop counts.
- **Routes**— Displays the number of routes learned. Click the number for details of the routes learned.
- **Last Seen**— Displays the last seen time duration in *nD nH nM nS* format.

Figure 332 *RIP—Neighbors Details*



- **Routes**
  - **Route**—Displays the route.
  - **Next Hop**—Displays information about the next hop.
  - **Metric**— Displays the number of hop counts.
  - **Tag**—Displays the tag number associated with the route attribute that is set.
  - **Expires**—Displays the time in *nD nH nM nS* format after which the route expires.

Figure 333 *RIP—Routes Details*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway Details - Overview Tab

After you onboard and configure the gateways, you can view the branch health, monitor the WAN uplink, and view the performance from the **Gateways** page.

To view the gateway overview page, complete the following steps:

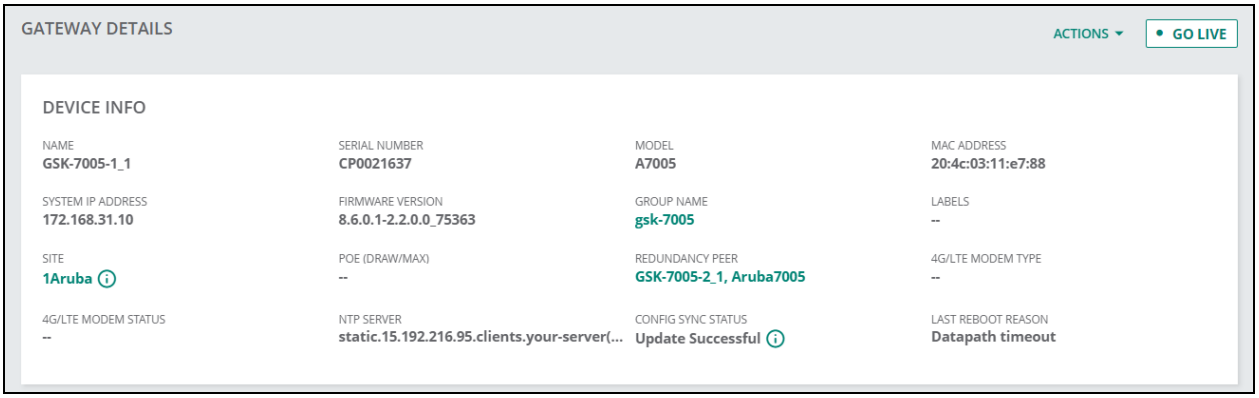
1. In the **Network Operations** app, use the filter to select a Branch Gateway
2. Under **Manage**, click **Overview > Summary**. The **Gateway Details** page is displayed. .

The **Overview** dashboard provides gateway device details, WAN availability and performance information, and the list of top applications. The **Overview** tab displays the following details:

Device Info

Displays the gateway device details.

Figure 334 *Device Info*



Device Info section displays the following details:

- **Name**—The name of the gateway.
- **Serial Number**—The serial number of the gateway.
- **Model**—The hardware model of the gateway.
- **MAC Address**—The MAC address of the gateway.
- **System IP address**—The IP address of the gateway.
- **Firmware Version**—The firmware version running on the gateway.
- **Group Name**—The name of the group to which the gateway belongs.
- **Labels**—The labels attached to the gateway.

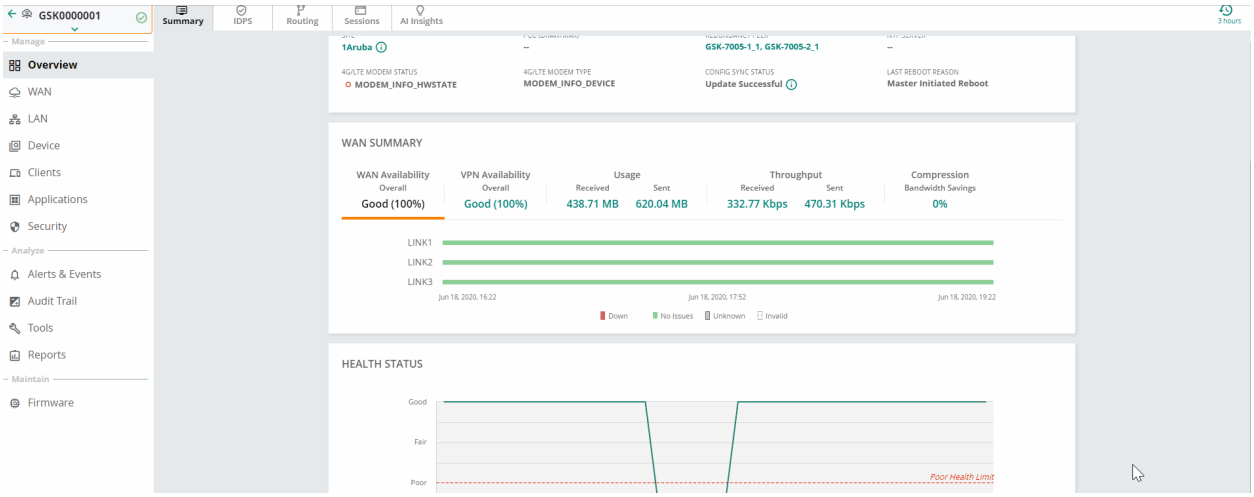
- **Site**—The site name of the gateway location.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the Branch Gateway consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **Redundancy Peer**—Displays the redundant gateway. Click the link to view the redundant gateway details. See the *Setting up Redundant Gateways for High Availability* section in the *Aruba Central Help Center*.
- **4G/LTE Modem Type**—Displays the LTE connection type.
- **4G/LTE Modem Status**—Displays the modem connectivity status. A green check-mark icon indicates that the connection is successful. This field also displays the name of the service provider and the signal strength. Hover over the information icon to view details about the active SIM, the IMEI number, and the phone number. You can view the signal strength classification based on the RSSI value provided in the following table:

SIGNAL STRENGTH	VALUE	REPRESENTATION
Good	> –65 dBm	All four bars are shaded green
Average	> –80 dBm	From the left, first 2 or 3 bars are shaded green
Poor	<–80 dBm	From the left, only one bar is shaded green

- **NTP Server**—The name of the NTP server configured.
- **Config Sync Status**—The status of the configuration sync.
- **Last Reboot Reason**—The reason for the last reboot.
- **Internal Modem Status** (Only for Gateway model: 9004-LTE)—Displays the name of the service provider and the signal strength. Hover over the information icon to view details about the active SIM, the IMEI number and the phone number. You can view the signal strength classification based on RSSI value, in the following table:

WAN Summary

Displays overview information about WAN and VPN.



WAN Availability

Provides a graphical representation of the Branch Gateway's WAN uplink availability. The graph displays each WAN uplink availability for the selected time range. Availability is determined by default gateway, monitored IP, and data VPNC reachability.

VPN Availability

Provides a graphical representation of the Branch Gateway's tunnel availability. Availability is determined by the probe settings configured using the **Health Check** option.

Usage

Displays the Branch Gateway's aggregate inbound and outbound traffic usage by WAN interface. Select one of the following options from the drop-down list:

- **All**
- **Internet**
- **VPN**

Throughput

Provides a graphical representation of the selected WAN interface's throughput. The graph displays the WAN interface's transmit and receive performance in Kbps. The graph also displays information that is sent and received.

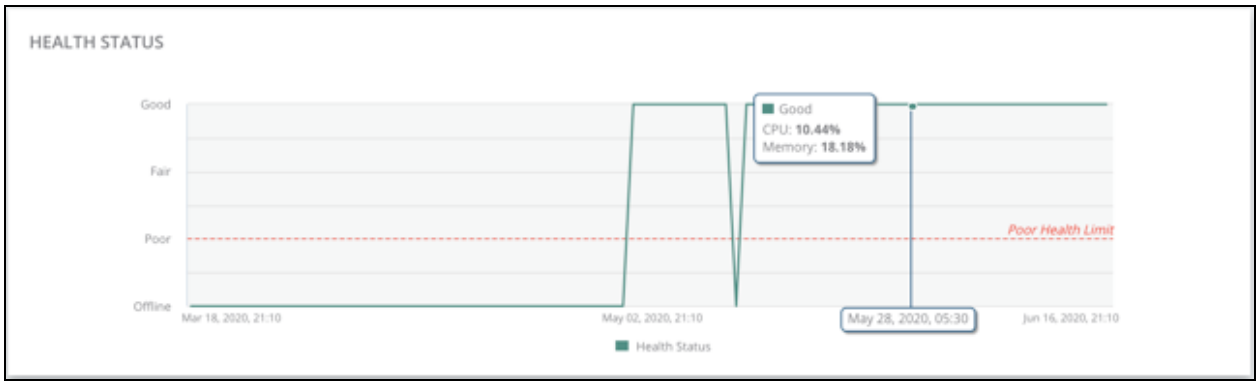
Compression

Displays the aggregate WAN compression details across all uplinks. The average bandwidth savings is displayed as a percentage. The compressed and uncompressed bandwidth is displayed as vertical grouped bar graphs. For more information about the process to enable data compression, see the *Configuring Uplink Interfaces* section in the *Aruba Central Help Center*.

Health Status

Displays the health of the gateway in terms of CPU and memory usage.

Figure 335 *Health Status*



Gateway > Overview > AI Insights

In the gateway dashboard, the **AI Insights** tab displays information on gateway performance issues such as tunnel up, tunnel down, airtime utilization, and memory utilization.

Viewing Gateways > AI Insights

To navigate to the **AI Insights** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active gateway.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.

   The dashboard context for the gateway is displayed.
4. In the gateway dashboard context, click the **AI Insights** tab.

   The **Insights** page is displayed.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **AI Insights** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

NOTE

AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** ( ) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

- Red—High priority
- Orange—Medium priority
- Yellow—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network

performance. Each insight report provides specific details on the occurrences of these events for ease in debugging.

Gateway > WAN > Summary

The **Summary** tab under **Manage** > **WAN** page in the gateway dashboard displays the following sections:

- Port Status
- WAN Interfaces
- Go Live

You can view and monitor your WAN interfaces, the tunnels configured, and the path steering data for all the DPS policies configured.

Viewing the WAN > Summary Tab

To navigate to the **WAN > Summary** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Summary**.

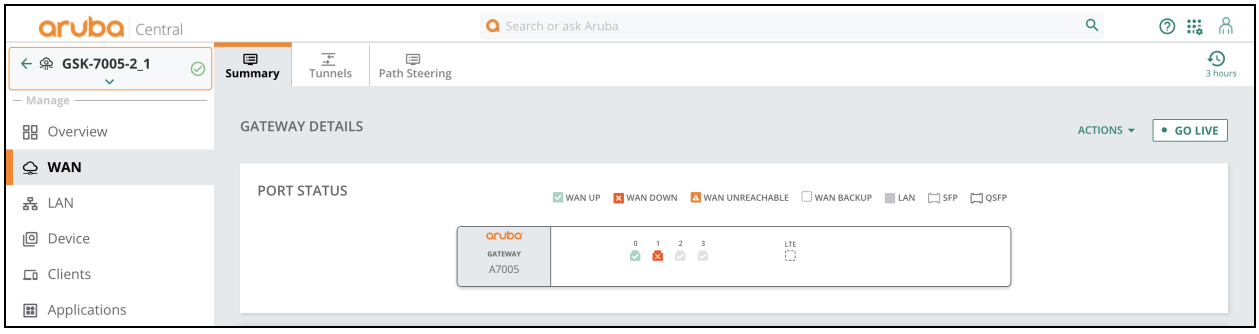
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Port Status

- Displays the WAN port status. Click a WAN port for more details.

Figure 336 *Port Status*

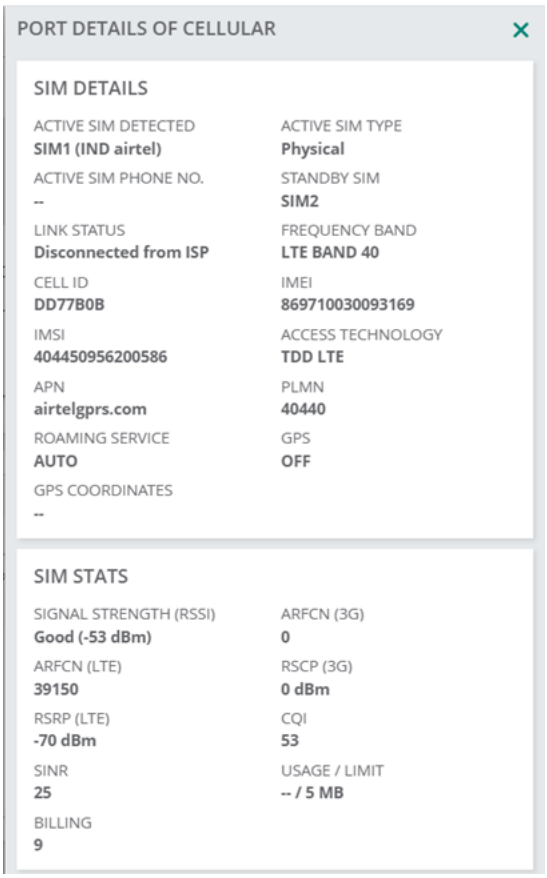


For a 9004-LTE Branch Gateway, the **Port Status** displays the LTE uplink details and when you hover over **Internal LTE**, you can view details about the active SIM, the name of the service provider, and the signal strength.

Figure 337 *Port Status of a 9004-LTE Gateway*

You can click on the active SIM to view the port details of cellular.

Figure 338 *Port Details*



WAN Interfaces

- Lists the WAN interfaces and provides the total number of WAN interfaces. Displays the summary of WAN uplinks. The following details are displayed for the port:

NOTE

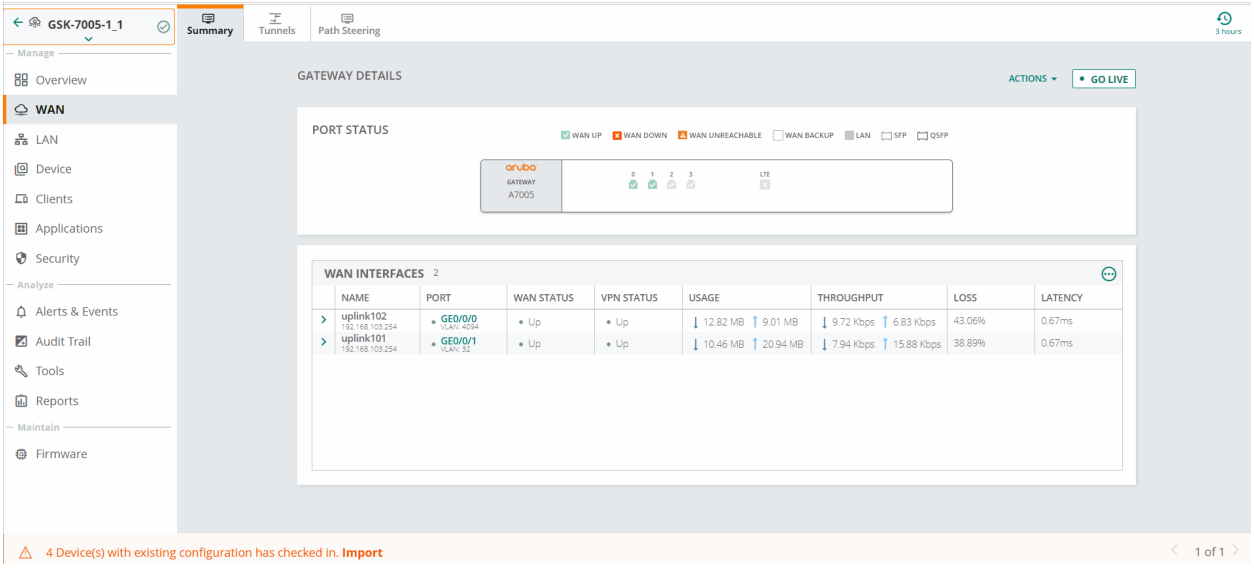
Click the Settings icon to reset or set the default columns that are displayed.

  - **Total WAN Interfaces**—Total number of WAN interfaces available.
  - **Name**—Name of the WAN interface.
  - **Port**— Port number along with the associated VLAN ID.
  - **WAN Status**—WAN reachability status.
  - **VPN Status**—VPNC reachability status.

- **Usage**—WAN interface usage (Sent and Received).
- **Throughput**—WAN interface transmit and receive performance in Kbps.
- **Loss**—Loss percentage.
- **Latency**—The latency in milliseconds.

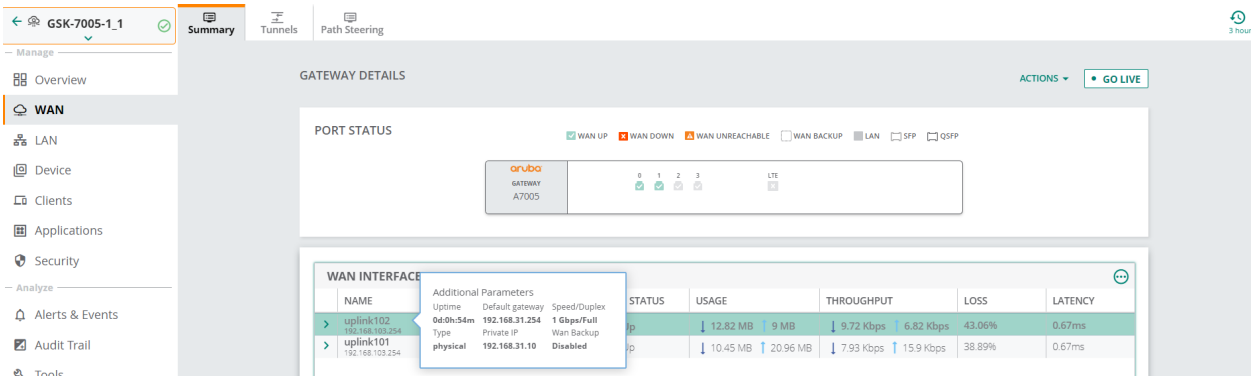
In the **WAN Interfaces** table, click a port number to display the **Packets** and **Errors** details.

Figure 339 *WAN Interfaces Packets and Errors*



- The following graphs are displayed under the **Packets** tab:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.
- The following graphs are displayed under the **Errors** tab:
  - **CRC Errors**—The number of cyclic redundancy errors logged.
  - **Error Frames**—The number of error frames logged.
  - **Collisions**—The number of collisions encountered.
- **Additional Parameters**—In the **WAN Interfaces** table, hover on the WAN interface name to view the additional parameter for the WAN interface.

Figure 340 *Additional Parameters*



The following additional parameters are displayed for the WAN interface:

- **Uptime**—Uptime of the uplink (DD-HH-MM).
- **Default Gateway**—Default gateway.
- **Speed/Duplex**—Port speed.
- **Type**—Service provider uplink type (Physical / Virtual).
- **Private IP**—Private IP address.
- **WAN Backup**—Backup of WAN interface (Enabled or Disabled).

Expand the **WAN Interface** name to see the following details.

- **WAN Availability**—Provides an overall graphical representation of the selected interface's WAN availability based on reachability. The graph shows the selected WAN port's ability to reach its default gateway and health check IP.
- **VPN Availability**—Provides an overall graphical representation of the selected interface's VPN availability based on reachability.
- **Usage**—Provides a snapshot of the WAN usage and is available for **All Traffic**, **Internet**, and **VPN** specific information. You can see the incoming and outgoing traffic for the gateways with time plotted on the x-axis. Hover over the chart to see the incoming and outgoing traffic for a particular time frame.
  - **Top Applications**—Displays application level WAN usage per-uplink for top ten applications. Click the **Go to Applications** link to view details in the **Applications** tab.
    The WAN visibility is available only for 3 hours time range.

  Click the following icons to see the chart in logarithmic scale or linear scale.
  - Logarithmic Scale—Click this icon to view chart in logarithmic scale.
  - Linear Scale—Click this icon to view chart in linear scale.

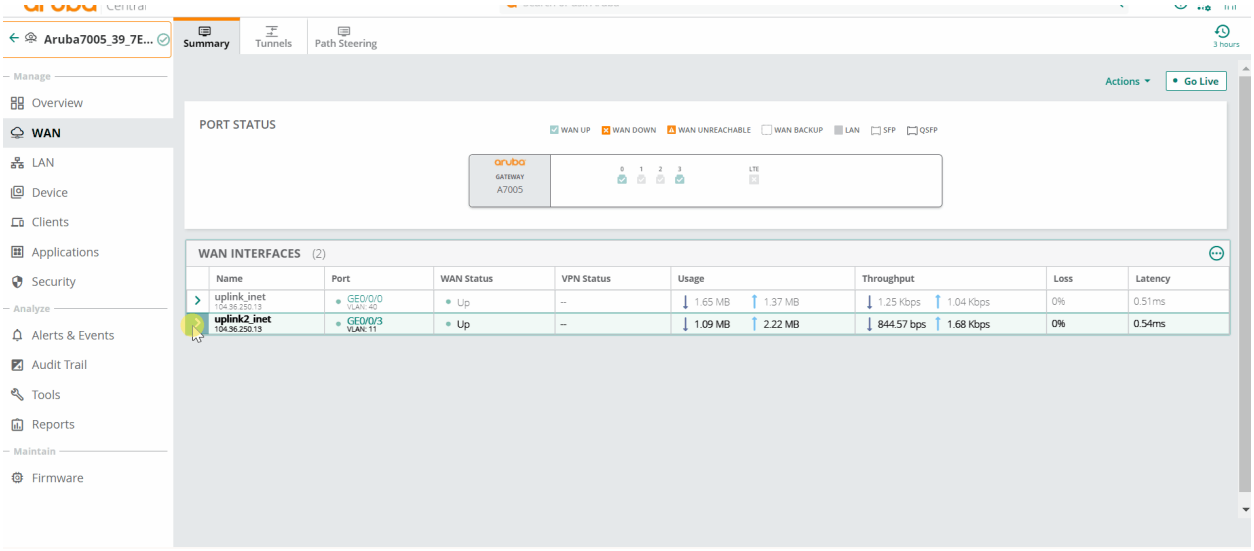
  Click Received or Sent at the bottom of the chart to view or hide the usage chart for received or sent data.
- **Throughput**—Provides a graphical representation of the selected WAN interface's throughput. The graph displays the WAN interface's transmit and receive performance in bps.

  Click the following icons to see the chart in logarithmic scale or linear scale.
  - Logarithmic Scale—Click this icon to view chart in logarithmic scale.
  - Linear Scale—Click this icon to view chart in linear scale.

  Click Received or Sent at the bottom of the chart to view or hide the usage chart for received or sent data.

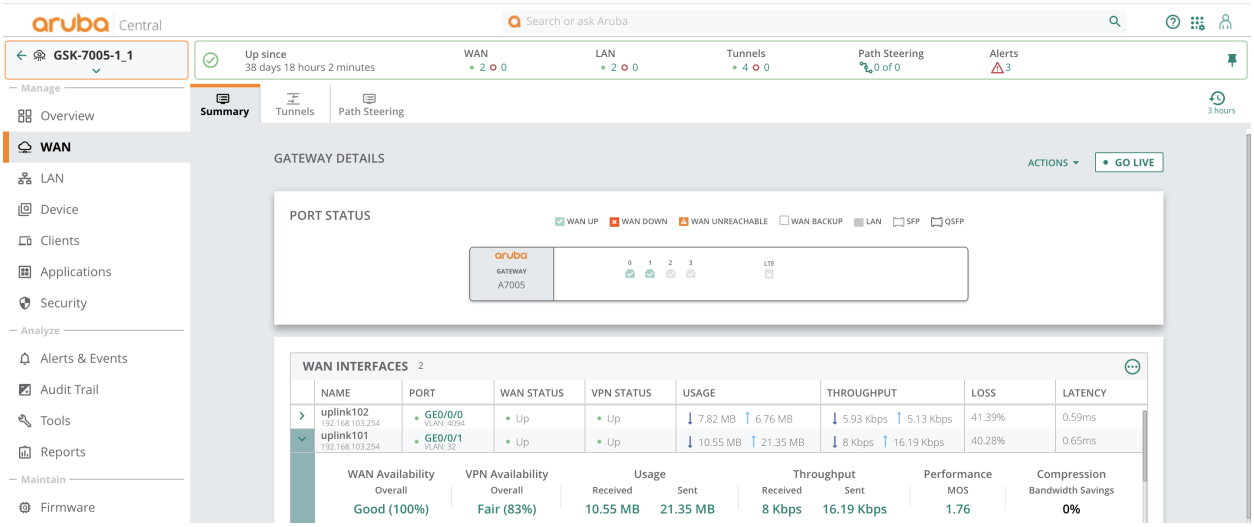
- **Performance**—The Performance section displays the MOS score of interface and the following graphs based on the probe that is selected. For a health check probe, only Latency and Packet Loss graphs are displayed.
  - **Latency**—The latency in milliseconds.
  - **Packet Loss**—Displays the packet loss in percentage.
  - **Jitter**—Displays the jitter in milliseconds.
  - **MOS Score**—Displays the MOS score.
- **WAN Compression**—Provides bandwidth savings of WAN compression uplink, along with optimized and non optimized packets and the average bandwidth saved in percentage.

Figure 341 *WAN Interfaces Availability*



Live Monitoring for Device State is enabled for **Status Header Tile**, **Port Status** and **WAN Interfaces**.

Figure 342 *WAN_Live Monitoring*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** option allows you to view the WAN interface data in real-time. The details about individual WAN interfaces are updated every five minutes in the normal WAN page view, whereas the details displayed in Live mode are updated every five seconds. This feature allows you to compare the statistics of two WAN interfaces. By default, the first two are displayed. You can select the uplinks for which you want to view the data. This feature is especially useful to troubleshoot issues.

The **Downstream** graph displays data on download speed and the **Upstream** graph provides data on upload speed. The X-axis in the graph indicates the time and the Y-axis indicates the throughput in Bytes per second (bps).

The Live session is active for 15 minutes and automatically returns to normal view at the end of 15 minutes. A timer displays the number of minutes since the live session started.

To view the live statistics of the WAN interfaces, click the **GO LIVE** button. To go back to normal view, click the **STOP LIVE** button.

Figure 343 *GO LIVE page*

Gateway > WAN > Tunnels

The **Tunnels** tab under **Manage** > **WAN** page in the gateway dashboard displays the following sections:

- Tunnels Summary
- Tunnels
- Tunnel Info

The Tunnels tab displays the status and health details for Branch Gateway tunnels and IAP-VPN tunnel.

Viewing the WAN > Tunnels Tab

To navigate to the **Tunnels** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Tunnels**.

   To exit the gateway dashboard, click the back arrow on the filter.

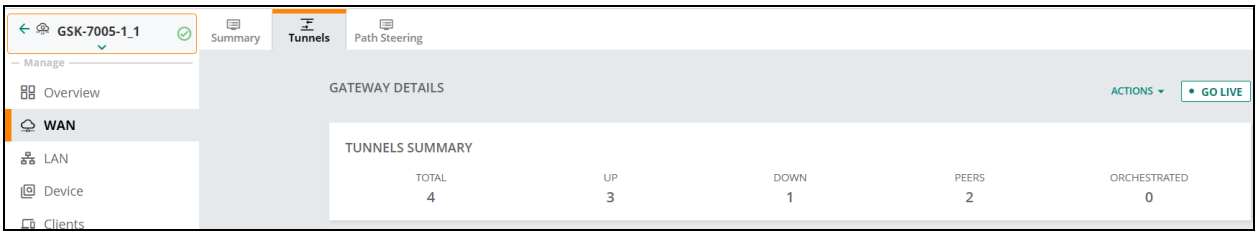
   You can change the time range for the **Tunnels** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Tunnels Summary

The following details are displayed in the **Tunnels Summary** table:

- **Total**—Total number of VPN tunnels.
- **Up**—Number of VPN tunnels in UP state.
- **Down**—Number of VPN tunnels in DOWN state.
- **Peers**—Total number of VPN peers.
- **Orchestrated**—Total number of VPN tunnels running in orchestrated mode.

Figure 344 *Tunnels Summary*



Tunnels

The following details are displayed in the **Tunnels** table:

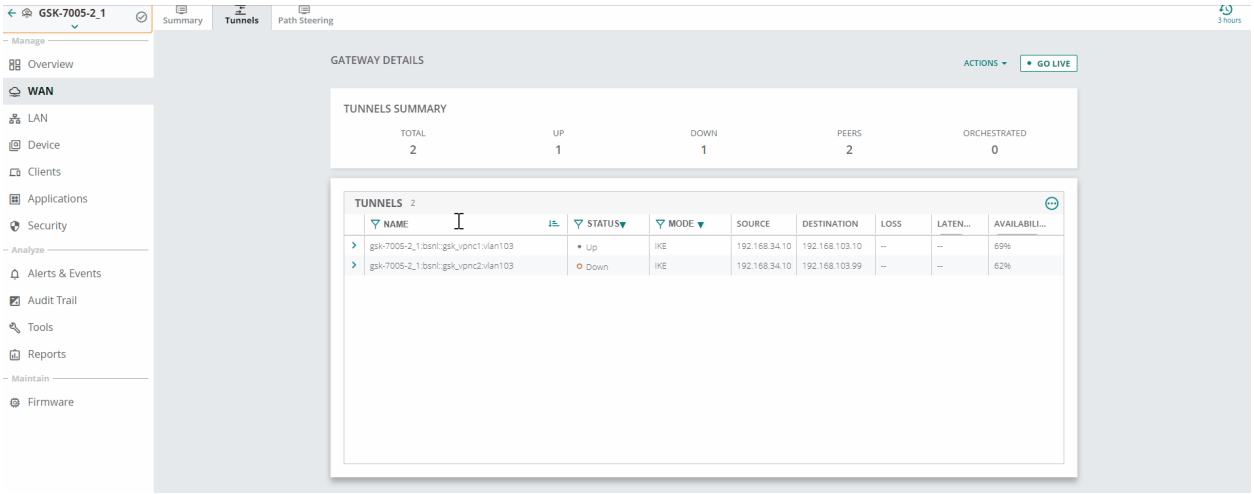
- **Name**—Tunnel name.
- **Status**—Status of the tunnel (Up or Down).
- **Mode**—Displays the type of tunnel. The tunnel configurations displayed are:
  - **Orch**—Identifies tunnels that have been orchestrated.
  - **Orch-Srv**—Identifies the orchestrated tunnels that are in survivability state.
  - **Orch-IKE**—Orchestrated tunnels which use the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite with 3rd party devices such as Zscaler.
  - **IKE**—Identifies tunnels created manually using the IKE protocol.
- **Source**—Source IP address of the tunnel.

- **Destination**—Destination IP address of the tunnel.
- **Loss**—Percentage of packet loss.
- **Latency**—The latency in microseconds.
- **Last Change Reason**—Reason for the last status change of the tunnel.
- **Availability**—Availability graph of the tunnel. Displays the percentage of time the tunnel was in UP state.

NOTE

The default view of gateways table shows only a few columns. To view the hidden columns, click the settings icon at the right side of the table. To reset the columns, click **Reset to default**.

Figure 345 *Tunnels Details*



Tunnel Info

- Expand a tunnel name to view the following details:
  - **Uptime**—Amount of time the tunnel has been active since it was last reset.
  - **Link**—Tunnel link.
  - **WAN IP**—WAN IP address.
  - **Uplink Port**—Uplink port details.
  - **Last Change Reason**—Reason for the last status change of the tunnel.
  - **Peer IP**—Peer IP address.
  - **VLAN**—VLAN ID.
  - **Source MAC**—Source MAC address.
  - **Next Rekey**—Next Rekey time.
  - **Auth**—Authentication methods such as SHA1, DES, and 3DES.

NOTE

From SD-Branch 2.3.0.0 version, Overlay Tunnel Orchestration supports the SHA2-256 authentication method. The Tunnel Orchestration creates IPSec tunnels with SHA2-256 authentication algorithm, only when both the tunnel endpoints (Initiator and Responder) support SHA2-256 authentication (that is, both the tunnel endpoints are running on SD-Branch 2.3.0.0). Else, the Tunnel Orchestration triggers the default authentication (SHA1).

- **In SPI**—Inbound Security Parameter Index (SPI).
- **Out SPI**—Outbound Security Parameter Index (SPI).
- **Encryption**—Encryption.

- **Availability**—Availability information of the tunnel.
  - **Tunnel Status**—Provides an overall graphical representation of the selected tunnel's availability based on VPNC reachability.
  - **Usage**—Displays the tunnel's traffic usage.
  - **Throughput**—Displays the inbound and outbound traffic rates for the selected tunnel. The graph displays the tunnel's performance in Kbps. The graph also displays information that is sent and received.
  - **Performance**—The Performance section displays the details based on the interface that is selected.

  Live monitoring is enabled for sections that display the status, such as:
- The **Tunnels Summary**
- Status of the **Tunnels Details**

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

- **Utilization**—Displays the utilization in percentage terms. The average, minimum, and maximum packet utilization is displayed.
- **SLA Policy Compliance**—Displays the SLA policy compliance details.

Gateway > WAN > Path Steering

In the **Path Steering** tab, you can view traffic path steering details for the Dynamic Path Steering policies configured on the Branch Gateway. This tab also displays the number of policies that are compliant along with the total number of policies configured on the Branch Gateway.

From the list of Dynamic Path Steering polices, select the policy for which you want to view the path steering details.

The **Pathsteering** tab under **Manage** > **WAN** page in the gateway dashboard displays the following sections:

- Path Steering Summary
- Path Steering Details

Viewing the WAN > Path Steering Tab

To navigate to the **Path Steering** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Path Steering**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Path Steering** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Path Steering Summary

Displays the following information.

- **State**—Displays whether the path steering feature is enabled.
- **Policy Compliance**—Displays the compliance status of all the configured policies.

Path Steering Details

Displays the following information.

- **Expected Threshold Values**
  - **Policy Name**—The name of the Dynamic Path Steering policy
  - **Bandwidth**— The threshold percentage set for bandwidth utilization
  - **Latency**—The threshold value set for a round-trip ping time in milliseconds
  - **Jitter**—The threshold value set for jitters in packet transmission in milliseconds
  - **Packet Loss**—The percentage of packet loss allowed for the traffic type
  - **Path Preference**—The path preference in the primary, secondary, and tertiary order
  - **Status**—The compliance status of the uplinks
  - **Overall Compliance**—Overall compliance (%) of the policy

Figure 346 *Path Steering Details*

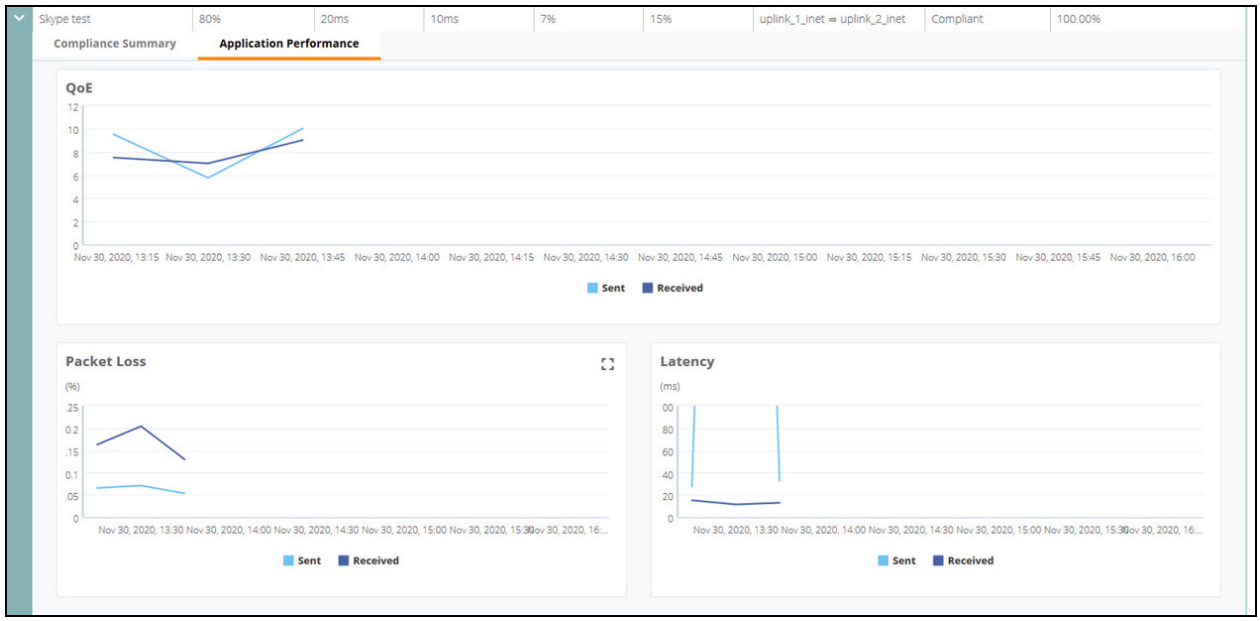
Click a policy to view the **Compliance Summary** that consists of the **Status** and **Session** information and the **Application Performance**.

- **Status**—Provides a graphical representation of the configured uplink statuses. The following details are displayed:
  - Overall status
  - The status of each of the uplinks configured for the Dynamic Path Steering policy on that gateway. Hover over the status bar to view the compliance status details of all the configured uplinks. You can view the compliance status of the uplinks and the probe IPs. If the probe IPs are non-compliant, it displays the reason for non-compliance such as latency, jitter, or packet loss. The following list contains the various colors and the corresponding compliance status:
    - **Green**—An uplink is **Compliant** when all of the associated probe IPs meet the set SLAs and threshold settings.
    - **Orange**—An uplink is **Partially Compliant** when you have multiple probe IPs and not all of them are compliant.
    - **Red**—An uplink is **Non-Compliant** when all of the probe IPs are non-compliant.
    - **Yellow**—This is the **Hold Period** when an uplink changes it's status from Non-compliant to Compliant (usually the first 3 minutes of the transition phase).
    - **Grey**—Uplink status is **Unknown** when the Dynamic Path Steering feature does not send any compliance information to the cloud.
    - **Purple**—The uplink is compliant and **FEC Protected** because of the redundant packets sent by FEC even though the packet loss percentage has exceeded the configured SLA.
- **Sessions**—Provides a graphical representation of the total number of sessions. The following details are displayed:
  - Overview
  - The sessions count on each of the uplinks configured for the Dynamic Path Steering policy on that gateway

Figure 347 *Path Steering Details—Compliance Summary*

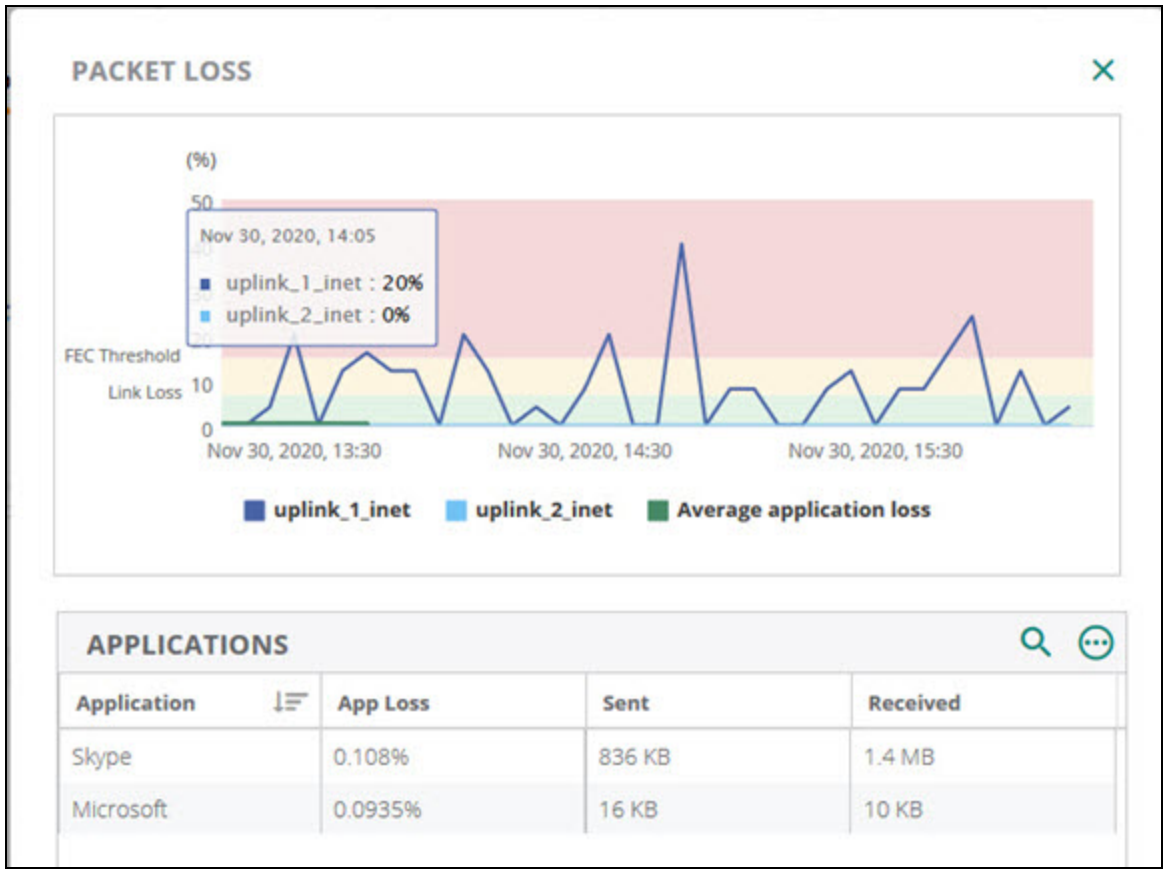
- **Application Performance**—Provides a graphical representation of the performance of the application for QoE, Packet Loss, and Latency. The passive application monitoring data is tagged with the DPS policy ID and the scores for both Sent and Received traffic are displayed in this chart. QoE is the average of the Packet Loss and Latency scores.

Figure 348 *Application Performance*



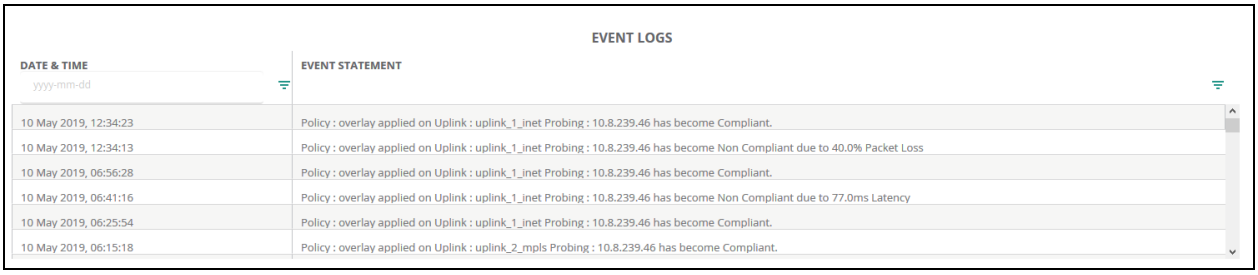
Click the Expand icon to drill down the packet loss data. The following image displays the Packet Loss data with respect to the configured FEC threshold. The uplink_1_inet has reached the FEC threshold which is 20% in this case, beyond which the uplink becomes non-compliant.

Figure 349 *Packet Loss*



- **Event Logs**—When an uplink becomes non-compliant, an event is recorded. When the same uplink becomes compliant adhering to the set SLAs, another event is recorded. The **Event Logs** table provides information about all such events. It displays the timestamp and a detailed event statement that contains the policy name, the uplink name, the probe IP, and the reason for non-compliance, if it is a non-compliance event.

  Figure 350 *Event Logs*



  Live monitoring is enabled for sections that display status, such as:

- The **path Steering Summary**
- Real time state of the **Event Logs**
- **Path Steering Summary**—Path steering summary of the primary, secondary, and standby uplinks.
- **Path Steering Details**—Displays the following path steering details:
- **Traffic Path**—Displays traffic path steering status for each link associated with the WAN policy.
- **Status**—Provides a graphical representation of the status of uplinks.
- **MPLS (Primary)**
- **Comcast (Secondary)**
- **LTE (Standby)**
- **Traffic Steer**
- **Traffic Classification**—Displays charts showing client traffic trends to application, application categories, website categories, and websites of a specific security reputation score. The **Traffic Classification** section also shows application with the highest security threat score. To view the traffic classification based on application, application category, and website category, you must enable **Deep Packet Inspection** on the Branch Gateways.

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > LAN > Summary

The **Summary** tab under **Manage** > **LAN** page in the gateway dashboard displays the following sections:

- Port Status
- LAN Interfaces Summary
- VLAN Interfaces Summary

Viewing the LAN > Summary Tab

To navigate to the **LAN > Summary** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **LAN** > **Summary**.

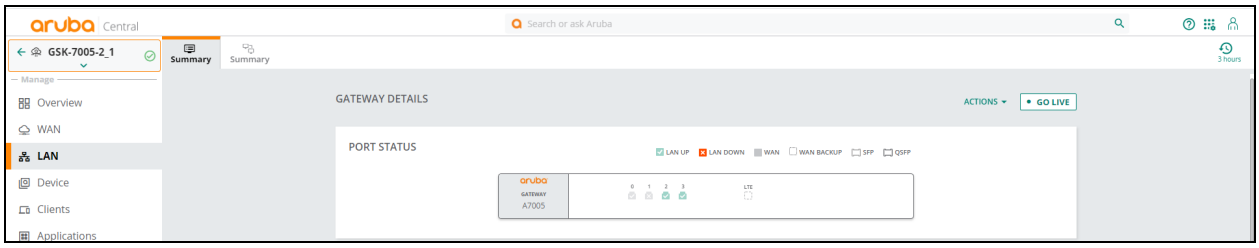
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Port Status

Provides a graphical representation of the LAN link availability of the Branch Gateway. Also provides a quick view of the LAN port status. Click a LAN port to view the **Port Details** pop-up page.

Figure 351 *LAN port status*



LAN Interfaces Summary

The table displays the summary of LAN interfaces and total number of LAN interfaces. The following details are displayed for the port:

- **Port**—Port number. Click on the Port to open the **Port Details** pop-up page.
- **Admin State**—Administrative state of the LAN interface. Values are **Enabled** or **Disabled**.
- **Operational State**—Operational state of the LAN interface. Values are **Up** or **Down**.
- **Port Speed**—Port speed.
- **VLANs**—Range of VLANs.
- **MTU**—MTU value.

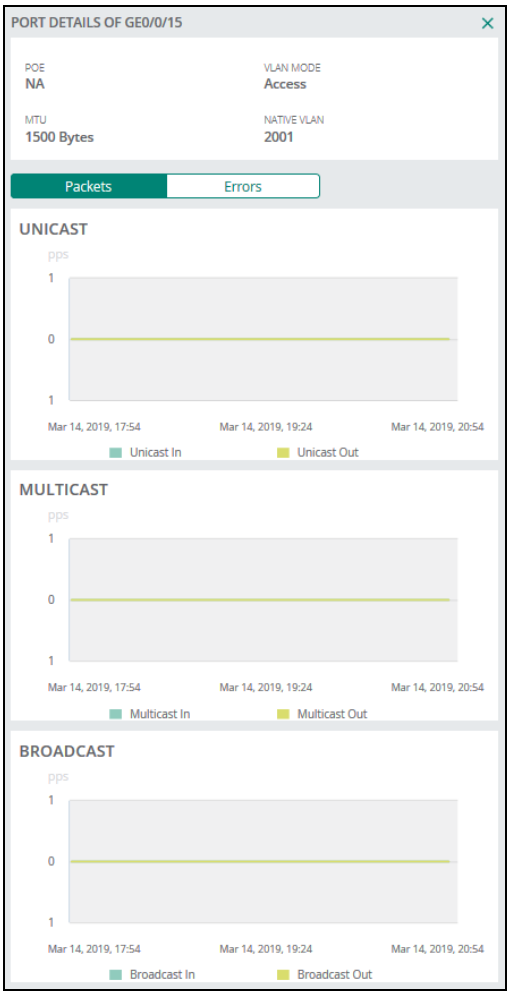
Port Details Pop-Up page

Click on a port in the **Port Status** or **LAN Interfaces Summary** page to display the **Port Details** pop-up page. The page has two tabs, **Packets** and **Errors**.

- The following graphs are displayed under the **Port Details > Packets** tab:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.

  Hover over any point of time on the x-axis to get data about packets for that instant of time.

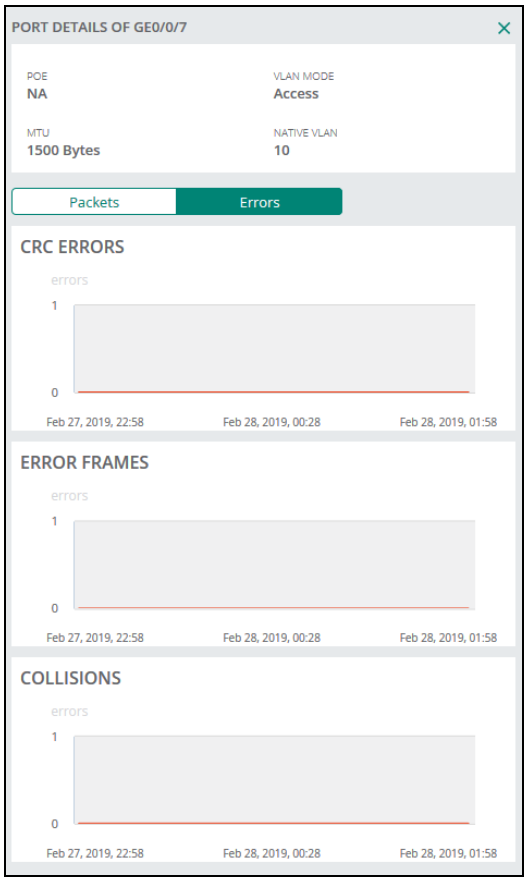
Figure 352 *Port Details—Packets*



- The following graphs are displayed under the **Port Details** > **Errors** tab:
  - **CRC Errors**—The number of cyclic redundancy errors logged.
  - **Error Frames**—The number of error frames logged.
  - **Collisions**—The number of collisions encountered.

Hover over any point of time on the x-axis to get data about packets for that instant of time.

Figure 353 *Port Details—Errors*

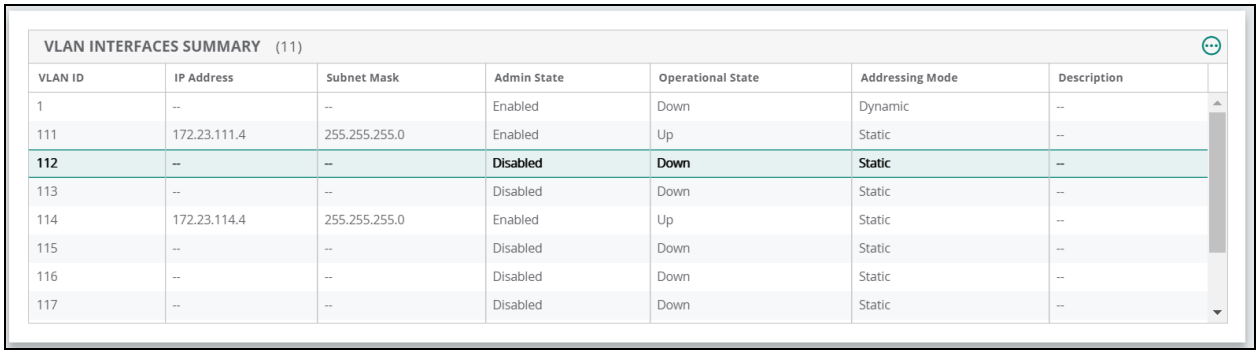


VLAN Interfaces Summary

The table displays the summary of VLAN interfaces and total number of VLAN interfaces. The following details are displayed:

- **VLAN ID**—VLAN ID number.
- **IP Address**—IP address.
- **Subnet Mask**—Subnet mask of the IP address.
- **Admin State**—Administrative state of the VLAN interface.
- **Operational State**—Operational state of the VLAN interface.
- **Addressing Mode**—Type of addressing mode.
- **Description**—Description of the VLAN.

Figure 354 *VLAN Interfaces Summary*



VLAN ID	IP Address	Subnet Mask	Admin State	Operational State	Addressing Mode	Description
1	--	--	Enabled	Down	Dynamic	--
111	172.23.111.4	255.255.255.0	Enabled	Up	Static	--
112	--	--	Disabled	Down	Static	--
113	--	--	Disabled	Down	Static	--
114	172.23.114.4	255.255.255.0	Enabled	Up	Static	--
115	--	--	Disabled	Down	Static	--
116	--	--	Disabled	Down	Static	--
117	--	--	Disabled	Down	Static	--

Live monitoring is available for the following:

- **Port Status**
- Operational state of the LAN interface in **LAN Interfaces Summary** table

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > LAN > DHCP

The **DHCP** tab under **Manage** > **LAN** page in the gateway dashboard displays the following sections:

- DHCP Pools
- Active Leases

Viewing the LAN > DHCP Tab

To navigate to the **WAN > DHCP** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **LAN** > **DHCP**.

   To exit the gateway dashboard, click the back arrow on the filter.

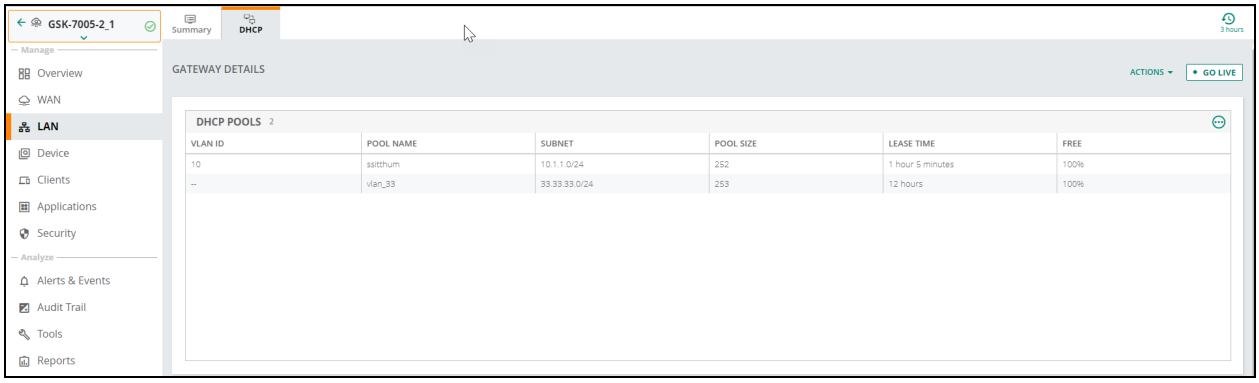
   You can change the time range for the **DHCP** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

DHCP Pools

- The table displays the summary of DHCP pools and total number of DHCP pools. The following details are displayed:

- **VLAN ID**—VLAN ID number.
- **Pool Name**—Name of the DHCP pools.
- **Subnet**—IP address of the client subnet.
- **Pool size**—Size of the pool.
- **Lease time**—Lease time of the pool.
- **Free**—Number of addresses available.

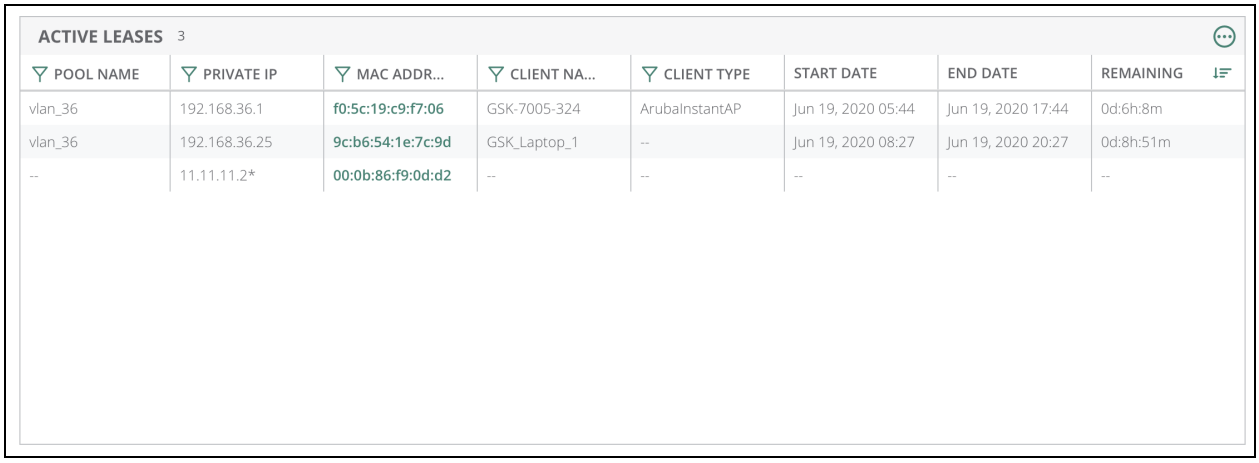
Figure 355 *DHCP Pools*



Active Leases

- The table displays the summary of active leases total number of active leases. The following details are displayed:
  - **Pool Name**—Name of the DHCP pools.
  - **Private IP**—IP address of the client subnet. The IP address with asterisk symbol (*) indicates it is a reserved IP address.
  - **MAC Address**—MAC address of the client. Clicking on the address takes you to the Client page.
  - **Client Name**—Client name.
  - **Client Type**—Client type.
  - **Start Date**—Start date and time of the lease.
  - **End Date**—End date and time of the lease.
  - **Remaining**—Remaining time for the lease to expire.

Figure 356 *Active Leases*



Live monitoring is available for the following:

- **Port Status**
- Operational state of the LAN interface in **LAN Interfaces Summary** table

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Applications > Visibility

The **Visibility** tab under **Manage** > **Applications** in the gateway dashboard displays the following tabs:

- Applications Tab in List View
- Websites Tab in List View

The **Visibility** dashboard displays charts showing client traffic trends with respect to application, application categories, website categories, and websites of a specific security reputation score. To view the traffic classification based on application, application category, and website category, you must enable **Application Visibility** service on Branch Gateways.

To view the application usage metrics for gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one Branch Gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Applications** > **Visibility** .

   The Visibility dashboard is displayed with two second-level tabs, **Applications** and **Websites**.

   You can change the time range for the **Visibility** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

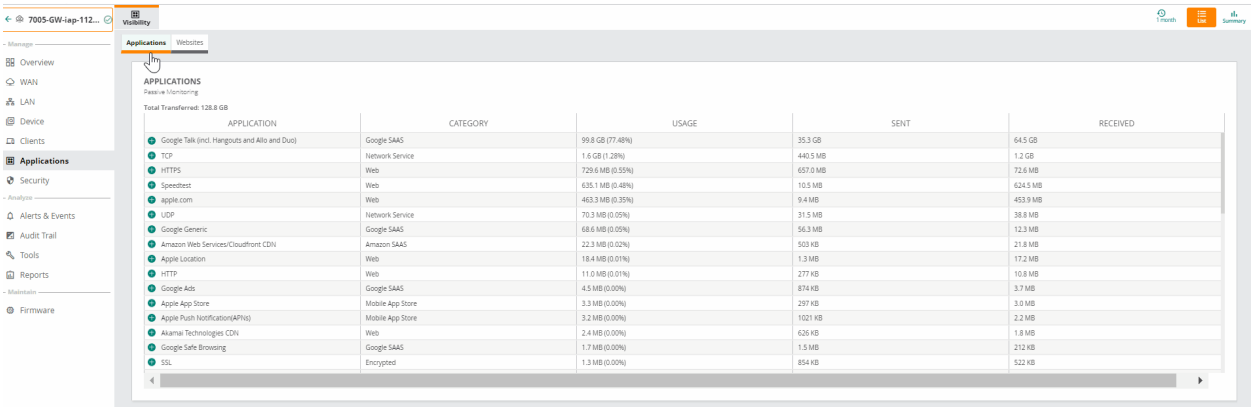
Click the **List** and the **Summary** icons on the **Application** and **Websites** sections to toggle between the dashboard views.

Applications Tab in List View

The **Visibility** > **Applications** tab in **List** view displays the following:

- **Application**—Displays the top N applications based on total bandwidth usage. Apart from the top N, the rest of the applications are grouped under the **Unclassified** category. Click the **+** sign next to the service name to expand an application in List view. A graph is displayed with date and time on the x-axis and usage on the y-axis. The graph displays the amount of data sent and received by the application over a period of time. To get the data sent and data received information for a specific day, hover over a point on the x-axis.
- **Category**—Displays the top N web categories based on total bandwidth usage. Apart from the top N, the rest of the web categories are grouped under the **Unclassified** category.
- **Usage**—Displays the bandwidth usage of each application.
- **Sent**—Displays the amount of data sent by the application.
- **Received**—Displays the amount of data received by the application.

Figure 357 *Visibility > Applications in List View*

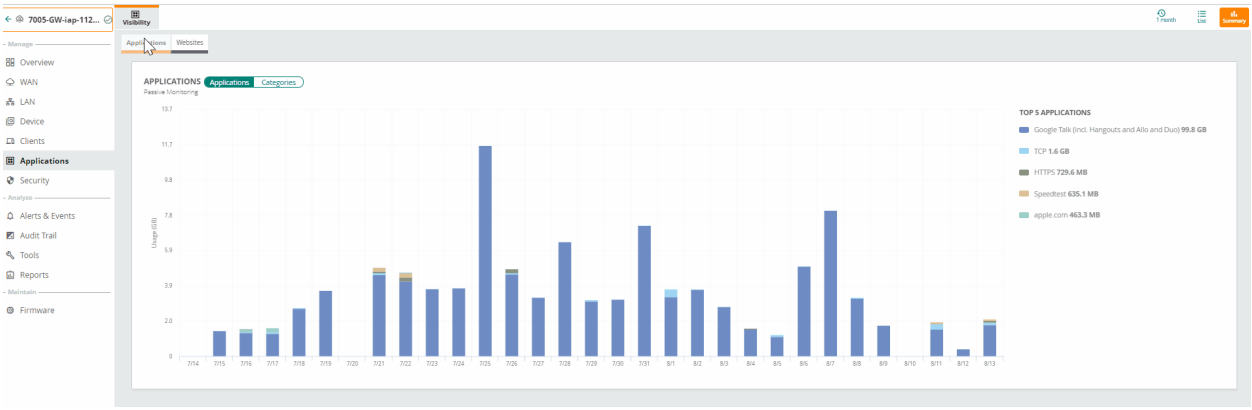


Applications Tab in Summary View

The **Visibility** > **Applications** tab in **Summary** view displays the following:

- **Applications**—Displays the graph top 5 applications based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover over a bar on the x-axis.
- **Categories**—Displays the top 5 web categories based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover over a bar on the x-axis

Figure 358 *Visibility > Applications in Summary View*

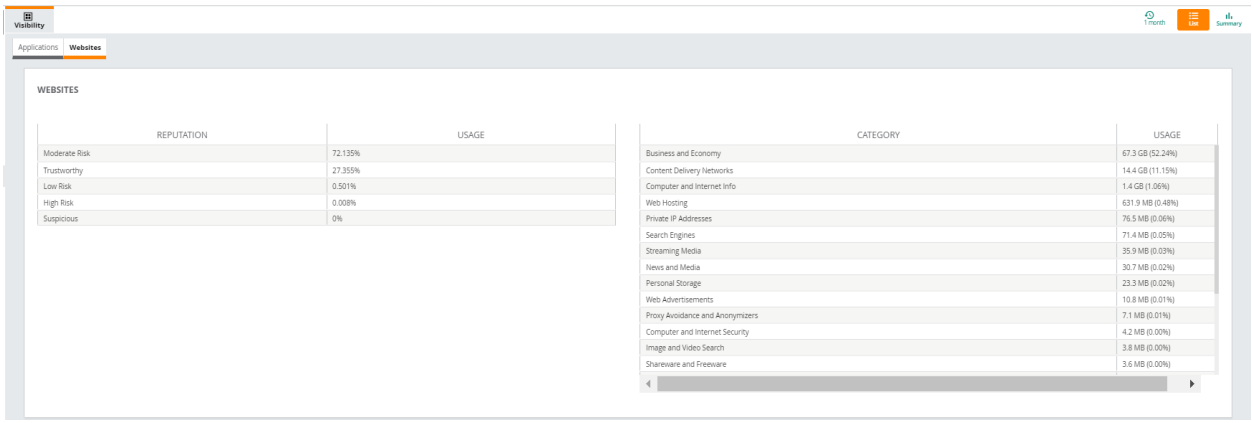


Websites Tab in List View

The **Visibility** > **Websites** tab in **List** view displays the following:

- **Reputation and Usage**—Displays the reputation and usage percentage.
- **Category and Usage**—Displays the WebCC category and the usage percentage.

Figure 359 *Visibility > Websites in List View*

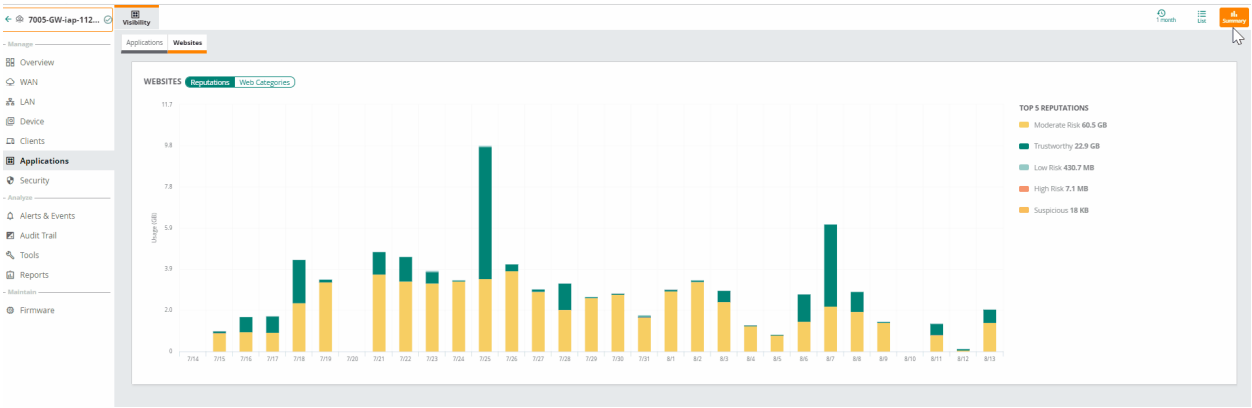


Websites Tab in Summary View

The **Visibility** > **Websites** tab in **Summary** view displays the following:

- **Reputations**—Displays the top 5 reputations based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover over a bar on the x-axis.
- **Web Categories**—Displays the top 5 WebCC categories based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover over a bar on the x-axis.

Figure 360 *Visibility > Websites in Summary View*



Downloading Gateway Details

You can download the gateway details as a .csv file.

To download the gateway details, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. In the **Gateways** table, click the download icon to download the gateways details as a .csv file.

   A .csv file is downloaded.

Related links:

Deleting a Gateway

Rebooting a Gateway

Rebooting a Gateway

Aruba Central allows you to reboot a gateway. The **Reboot Gateway** option is available under the **Actions** drop-down for many gateway pages. The following procedure explains how to reboot a gateway in the **Manage** > **Overview** > **Summary** page for a gateway.

NOTE

The **Reboot Gateway** option is only available for online gateways.

To reboot a gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the Gateways table, click the gateway to reboot.

5. You can delete the gateway in multiple ways. Perform one of the following steps:
   - In the **Actions** drop-down list, click **Reboot Gateway**.
   - Click the **Reboot** button available at the end of the row for that gateway.
   - Click the **Reboot** button at the bottom of the page.

   A **Reboot** dialog box is displayed.
6. Click **Yes** to reboot the gateway.

   All clients connected to this gateway are disconnected and gateway reboots.

The **Gateway Details** page takes less than a minute to update the interface status after the gateway is rebooted and reconnected to Aruba Central.

Opening a Remote Console

Aruba Central allows you to open the remote console for a CLI session through SSH for a gateway. Ensure that you allow SSH over port 443.

To open the remote console for a gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the Gateways table, click the gateway for which you want to open the remote console.

   The **Overview** > **Summary** page corresponding to the gateway is displayed.
5. In the **Actions** drop-down list, click **Open Remote Console**.

   A CLI session dialog box is displayed. The default user ID is **Admin**, but you can edit and customize the user ID. Ensure that the custom user ID is mapped to the device.

Deleting a Gateway

Aruba Central allows you to delete a gateway only when the device is offline. To delete an offline gateway, complete the following steps:

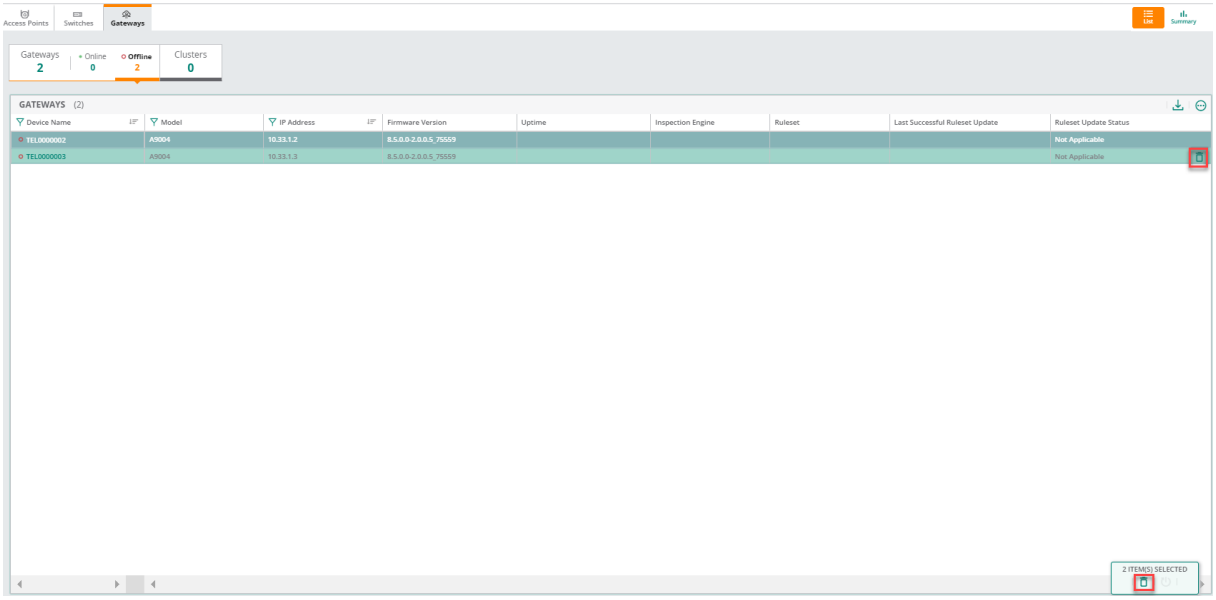
1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view under the second-level **Gateways** tab.
3. Click **Offline** to display a table with the list of offline gateways.
4. From the **Gateways** table, select the gateway(s) that you want to delete. To select a gateway, click on any column except **Device Name**.

Clicking on a device name in the Device Name column opens the gateway dashboard.

5. Click the **Delete** button at the bottom of the page to delete all the selected gateways. To delete a particular gateway, click the **Delete** button available at the end of the row for that gateway.



6. Confirm deletion.

The offline gateway is deleted. However, the device still can be found in Aruba Central database, as the device entry remains in the **Device Inventory** page.

Clearing IPSec SA

Aruba Central allows you to clear the IPsec Security Association (SA) for a gateway. The **Clear IPSec SA** option is available under the **Actions** drop-down for many gateway pages. The following procedure explains how to clear **IPSec SA** in the **Manage** > **Overview** > **Summary** page for a gateway.

NOTE

The **Clear IPSec SA** option is only available for online gateways.

To clear IPSec SA for a gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the **Gateways** table, click the gateway for which you want to clear the **IPSec SA** option.

   The **Overview** > **Summary** page corresponding to the gateway is displayed.
5. In the **Actions** drop-down list, click **Clear IPSec SA**.

Clearing ISAKMP SA

Aruba Central allows you to clear the ISAKMP Security Association (SA) for a gateway. The **Clear ISAKMP SA** option is available under the **Actions** drop-down for many gateway pages. The following procedure explains how to clear **ISAKMP SA** in the **Manage** > **Overview** > **Summary** page for a gateway.

NOTE

The **Clear IPSec SA** option is only available for online gateways.

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the Gateways table, click the gateway for which you want to clear the **ISAKMP SA** option.

   The **Overview** > **Summary** page corresponding to the gateway is displayed.
5. In the **Actions** drop-down list, click **Clear ISAKMP SA**.

   The clear command is sent successfully and a success message is displayed.

WAN Health—Global

The **WAN Health** tab provides detailed information of the network health status and usage for the sites in which Branch Gateways and VPNCs are configured in your setup.

To navigate to this page:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Overview** > **WAN Health**.
3. Click the **List** icon to navigate to the list view of **Transport** and **Site** pages.

Page Views

The **WAN Health** page offers the following views:

- **Summary**—This view provides a pictorial view of the network across various sites. The sites are color coded; red indicates potential issues and green indicates that there are no issues. To change the zoom level, click the zoom icons. You can click the different site on the map to view details.
- **List**—Primarily provides numerical representation of data under **Transport** and **Site** tabs.
  - **Transport**—The columns categorized under **Uplink** and **Performance** provide textual values. You can select a device from the **Name** column to view the details about that device's health.
  - **Site**—The **Site Type** and **Connectivity Status** columns provide textual values. You can select the site from the **Site Name** column to view details about that site's health.

This page uses the following indicators to present information on status of the network health:

- Grey ● bullet icon—Indicates no issues.
- Red ● bullet icon—Indicates potential issues.

WAN Health

Table 290: *Gateways Network Health Page*

Header	Totals	Description
Site Name	Displays the total number of sites.	Name of the site. Use the column filter bar to search for a particular site. Click the site name to open the **Site Health** page. For more information, see the *Site Health* section in the *Aruba Central Help Center*.
Site Type	Displays the total number of sites for each site type.	Displays whether the device is deployed as a hub or spoke. ■ To filter gateways provisioned as a hub, click **Hub**. ■ To filter gateways provisioned as a spoke, click **Spoke**. ■ To filter gateways deployed as cloud instances, click **Cloud**. Only hubs can be deployed as cloud instances, so if a hub is deployed as a cloud instance, the site type is **Cloud**.
Device Status	Displays the total number of devices in Up and Down state.	Displays the total count of devices in the UP and DOWN states. ■ To filter devices in UP sate, click **Up**. ■ To filter devices in DOWN sate, click **Down**.
Connectivity	Displays the total number of links.	Displays the following information: ■ **Status**—Displays the overall connectivity status. One of the following statuses is displayed: ◦ Up ◦ Partial ◦ Down Hover over the column to view the circuit status, tunnel status, overlay status, and underlay status separately.
Performance	Displays the average value for site availability.	Displays the following metrics: ■ **Site Availability**—Displays the site availability. The range is from 0 to 100 percent. To filter site availability, click the column filter bar and enter values in the **Min** and **Max** text boxes. Hover your mouse over the column to view site availability on a per provider basis.

For information about a particular site, see WAN Health—Site.

WAN Health—Transport

The **WAN Health—Transport** page displays the transport health of all uplinks belonging to an end-user. This page helps in monitoring network health of all uplinks based on active monitoring probes.

To launch the **WAN Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Overview** and select the **WAN Health** tab.
3. Click **List** view to launch the **Transport** page.

You can change the time range for the **Transport** tab by clicking the time range filter and selecting one of the available options: 3 hours, 1 day, and 1 week.

The **Transport** page displays the following information :

Table 291: *WAN Health—Transport*

Content	Description
Name	Displays the name of the device. **Search Options**: ■ The icon allows you to search a particular gateway by its name. Clicking on the gateway name redirects you to the Device overview dashboard. ■ The and icons allow you to sort the gateways in ascending or descending order.
Site	Displays the name of the site. Type the name of a site in the filter field to display the list of gateways from a particular site. **Search Options**: ■ The icon allows you to search a particular site by its name and display the list of gateways belonging to the site. ■ The and icons allow you to sort the sites in ascending or descending order.
Status	Displays the gateways whose uplinks are in Up or Down state. **Search Options**: ■ Select **Up** or **Down**from the drop-down filter to display the gateways of a particular state. ■ The and icons allow you to sort the status in ascending or descending order.
Transport	Displays the transport type used by the uplink. Supported transport types are: ■ MPLS ■ LTE ■ Internet ■ Metro-Ethernet Select one of the transport types from the drop-down filter to display the uplinks of a particular transport type. The and icons allow you to sort the transport type in ascending or descending order.
Carrier	Displays the uplink carrier. **Search Options**: ■ The icon allows you to search a particular carrier by its name. Clicking on the carrier name redirects you to the **WAN Summary** dashboard > **WAN Availability** tab. ■ The and icons allow you to sort the carrier names in ascending or descending order.
Type	Displays whether the uplink is Primary or Backup. **Search Options**: ■ Select **Primary** or **Backup** from the drop-down filter to display the gateways of a particular type. ■ The and icons allow you to sort the type in ascending or descending order.
Availability	Displays whether the uplink availability is good, fair, or poor based on the availability percentage. ■ Good > 90% ■ Fair > 70% ■ Poor < 70% Select one of the availability options from the drop-down filter to display the gateways of a particular availability percentage.

Table 291: *WAN Health—Transport*

Content	Description
	The  and  icons allow you to sort the availability in ascending or descending order.
Usage	Displays the uplink usage in gigabytes. The  and  icons allow you to sort the usage in ascending or descending order.
Throughput	Displays the uplink throughput. The  and  icons allow you to sort the throughput in ascending or descending order.
Loss	Displays the uplink packet loss is good, fair, or poor. ■ Good < 0.5% ■ Fair < 2% ■ Poor > 2% Select either **Good**, **Fair**, or **Poor** from the drop-down filter to display the uplinks with a particular packet loss percentage. The  and  icons allow you to sort the loss in ascending or descending order.
Latency	Displays whether the uplink latency is good, fair, or poor. ■ Good < 200ms ■ Fair < 400ms ■ Poor > 400ms Select either **Good**, **Fair**, or **Poor** from the drop-down filter to display the uplinks with a particular latency calculation. The  and  icons allow you to sort the latency in ascending or descending order.
Jitter	Displays whether the uplink jitter is good, fair, or poor. ■ Good < 200ms ■ Fair < 400ms ■ Poor > 400ms Select either **Good**, **Fair**, or **Poor** from the drop-down filter to display the uplinks with a particular jitter calculation. The  and  icons allow you to sort the jitter in ascending or descending order.
MOS	Displays the uplink quality based on the Mean Opinion Score (MOS) calculated using loss, latency, and jitter. The  and  icons allow you to sort the MOS in ascending or descending order.

WAN Health—Site

The **WAN Health** page displays details for the wired, wireless, and gateway devices deployed on the site.

To launch the **WAN Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to a site.
2. Under **Manage**, click **Overview > WAN Health** to launch the **WAN Health** dashboard.
3. Click the **Site** tab.

   The site health information is displayed in the **List** view.

The following indicators are used for the status of the site health:

- Grey ● bullet icon—Indicates no issues.
- Red ● bullet icon—Indicates potential issues.

The **WAN Health** dashboard for the site displays the following information:

Table 292: *Gateways Network Health Page*

Header	Totals	Description
Site Name	Displays the total number of sites.	Name of the site. Use the column filter bar to search for a particular site. Click the site name to open the **Site Health** page. For more information, see Site Health.
Site Type	Displays the number of sites for each site type.	Displays whether the device is deployed as a hub or spoke. Only hubs can be deployed as cloud instances, so if a hub is deployed as a cloud instance, the site type is **Cloud**.
Device Status	Displays the number of devices in **Up** and **Down** state.	Displays the total count of devices in the Up and Down states for each site.
Connectivity	Displays the number of links.	Displays the overall connectivity status and it can be one of the following: ■ Up ■ Partial ■ Down Hover over the value to view the circuit status, tunnel status, overlay status, or underlay status in a text box.
Performance	Displays the average value for site availability.	Displays the site availability. The range is from 0 to 100 percent. To filter site availability, click the column filter bar and enter the **Min** and **Max** values in the text boxes. Hover over the value to view site availability for each provider.

Monitoring Sites in the Topology Tab

In Aruba Central, the **Topology** tab in the site dashboard provides a graphical representation of the site including the network layout, details of the devices deployed, and the health of the WAN uplinks and tunnels.

The Topology feature is available for Foundation and Advanced licenses for APs, switches, and gateways.

This section includes the following topics:

Before You Begin

The following types of devices are displayed as part of the **Topology** tab:

- Access Point (AP)
- Gateway
- Switch—AOS-Switch, AOS-CX switch
- Stack—AOS-Switch stack, AOS-CX VSF stack
- AOS-CX VSX Switch

In the topology map, Aruba Central only supports third-party routers, switches, gateways, and APs from the vendors listed below:

- Cisco
- Procurve
- Juniper
- HPE Comware
- Meraki
- Cumulus
- Huawei
- Mikrotik
- Extreme
- HPE OfficeConnect Switch
- Arista
- 3Com
- Ruckus
- Mojo
- Mist
- Motorola
- Netgear
- Dell
- Comware
- Hirschmann Railswitch
- Ubiquiti

This section discusses the pre-requisites associated with the devices so that they are displayed correctly in the **Topology** tab:

- The topology map filters devices based on sites. To view the topology map, ensure that you have assigned the devices to sites.
- The minimum required ArubaOS version for access points (APs) and gateways in the topology map is ArubaOS version 8.1.0.0-1.0.1.1.
- To view the topology map, ensure that LLDP is enabled. On switches, LLDP is enabled by default. On Branch Gateways, if the port type is LAN, LLDP is enabled by default.
- To view AOS-CX switches in the topology map, you must create a template configuration for the switch with the password in plaintext.

The guidelines for grouping VPNCs are:

- If the tunnels in the overlay are orchestrated, the VPNCs are grouped according to their hub groups. You can also see the group preference order marked as primary, secondary, or tertiary.
- If the tunnels are configured manually, the VPNCs are grouped according to their sites. If the VPNCs are not associated with any site, they are grouped based on their hub groups. For manual tunnels, the Data Center group preference is not displayed.
- If you have a combination of gateways in a single site, with one gateway configured as a manual tunnel and the other gateway configured as an orchestrated tunnel, both the tunnels are treated as manual and the VPNCs are grouped based on their sites. If there are no associated sites, they are grouped according to their hub groups.

NOTE

Do not install VPNCs with orchestrated tunnels and VPNCs with manual tunnels together in a single site.

Viewing the Topology Tab

To view the topology tab, complete the following steps:

1. In the **Network Operations** app, set the filter to a site for which you want to view the topology map.

   The dashboard context for the site is displayed.
2. Under **Manage**, click **Overview** > **Topology**.

   The Topology map for the selected site is displayed.
3. In the topology map, hover over a device or a link to view the pop-up details. For more information, see Pop-Up Details.
4. In the device or the link pop-up, click the **Show Details** link to view the corresponding **Details** pane. For more information, see Details Pane .

Parts of the Topology Tab User Interface

In the topology tab, the icons provides the following functionality:

Figure 361 *Parts of the Topology Tab*

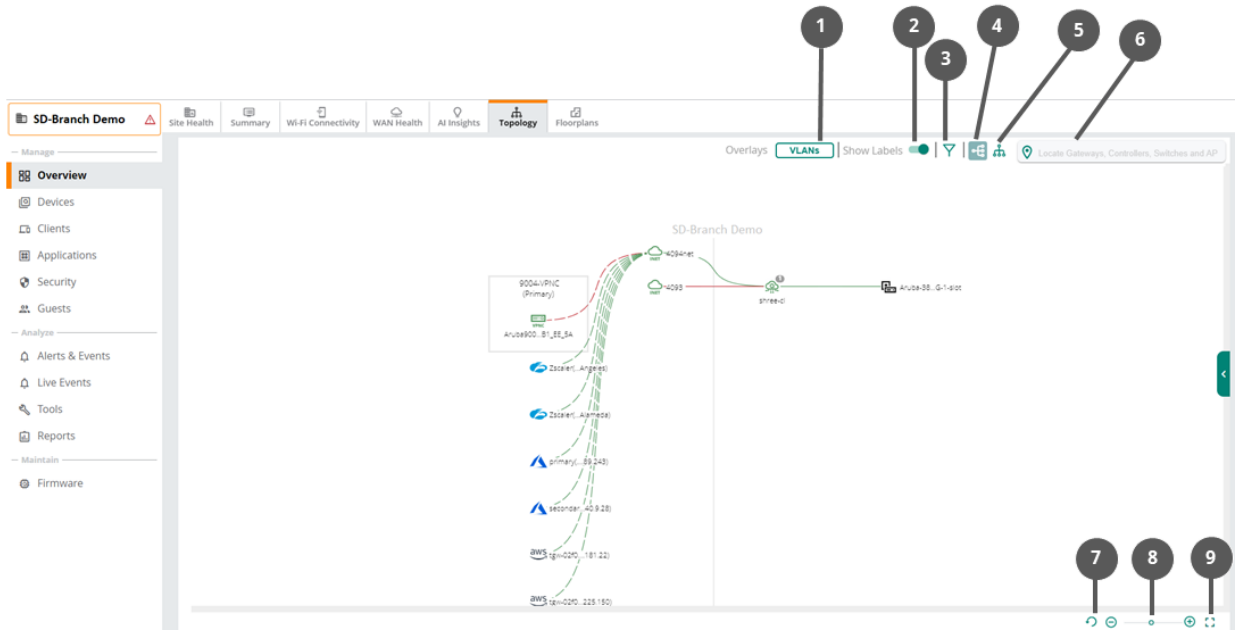


Table 293: *Icon Details*

Callout Number	Description
1	Click the icon to show or hide the **VLANs** pane.
2	Set the toggle icon to show or hide the labels.
3	Click the icon to filter the type of devices to be shown on the map. The following options are available: ■ **Access Points**—Allows you to show or hide the APs from the topology map. ■ **Security Cloud**—Allows you to show or hide the Zscaler and Palo Alto Prisma Access™ Cloud Service from the topology map. ■ **Switch**—Allows you to show or hide the switches from the topology map. ■ **VPNC**—Allows you to show or hide the VPNCs and the virtual gateways from the topology map. ■ **Unmanaged**—Allows you to show or hide the unmanaged devices from the topology map. ■ **Show Devices Without Link**—Allows you to show or hide the devices without link from the topology map.
4	Click the icon to view the topology map in a left to right orientation. The default orientation of the topology map is left to right orientation.
5	Click the icon to view the topology map in a top to down orientation.
6	The search bar allows you to locate a device in the topology map. The search bar field supports exact and partial text search.
7	Click the icon to reset the topology map to the default view.
8	Click the icons to change the zoom level of the topology map. Alternatively, you can drag the slider to set the zoom level of the topology map.
9	Click the icon to view the topology map in full-screen view. In the full-screen view, the pop-up details feature is disabled in the topology map.

When the number of downstream devices connected to a device is less than or equal to 10, the devices are visible in the topology map. When the number of downstream devices connected to a device is more than 10, click the device icon to view the devices in the topology map. A bubble icon on the device represents the number of connected downstream devices.

Table 294: *Icon Types*

Icon	Type
	AP
	Branch Gateway
	Switch

Icon	Type
	Switch Stack
	Unmanaged Device
	Uplink
	VPNC
	Third-party Zscaler VPNC
	Third-party Azure VPNC
	Third-party AWS VPNC

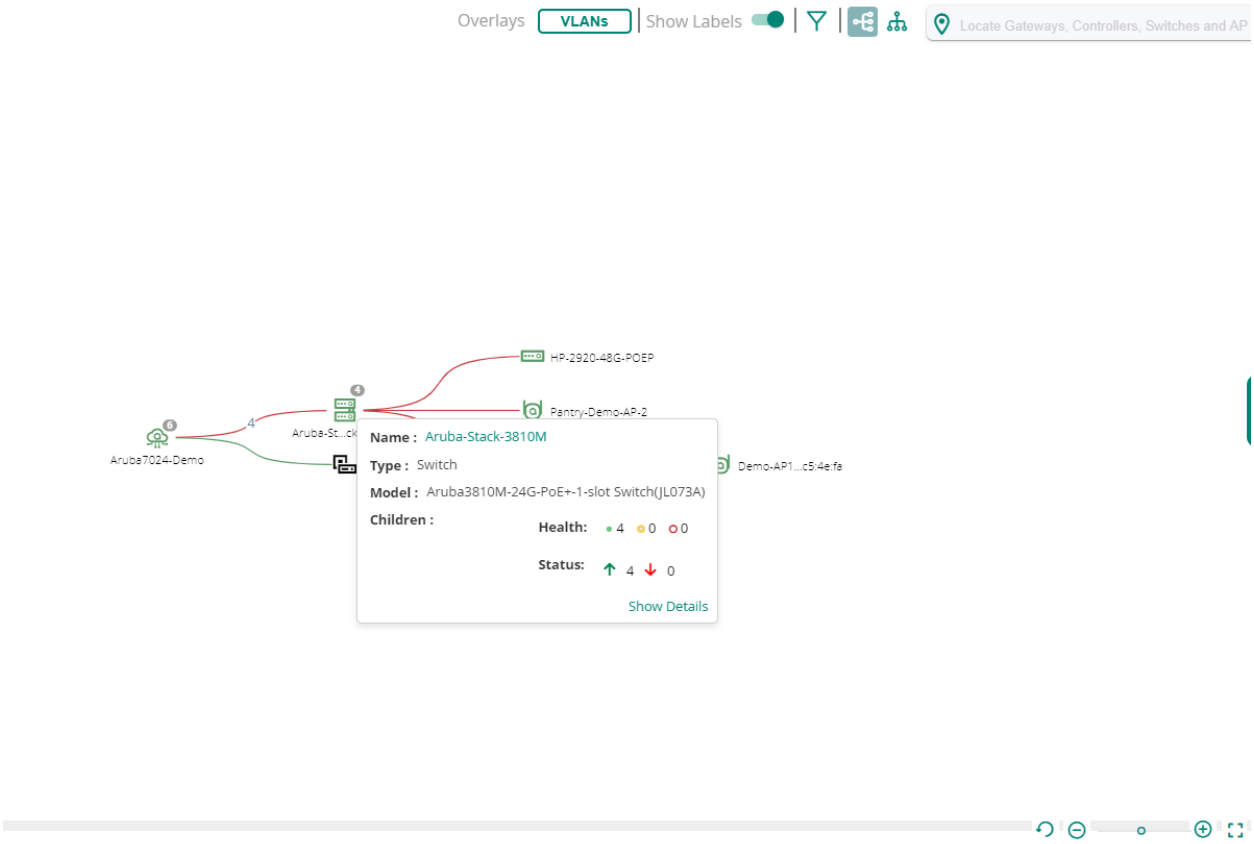
Icon Status

- —Indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
- —Indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%.
- —Indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%.
- —Indicates that the device is online.
- —Indicates that the device is offline.

Pop-Up Details

When you hover over a device or link, a pop-up displays the following details:

Figure 362 *Pop-Up Details*



- Access Point—Displays the following details:
  - **Name**—Hostname of the AP.
  - **Type**—Type of the device.
  - **Model**—Hardware model of the AP.
  - **Health Reason**—The health status of the AP. This parameter is only available when the AP is offline.
  - **Show Details**—Click the link to view the **Details** pane.
- Branch Gateway—Displays the following details:
  - **Name**—Hostname of the Branch Gateway.
  - **Type**—Type of device deployment.
  - **Model**—Hardware model of the device.
  - **Children**—Number of devices connected to the Branch Gateway categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the Branch Gateway based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
    - **Status**—Count of devices connected to the Branch Gateway based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.

- **Show Details**—Click the link to view the **Details** pane.

- VPNC—Displays the following details:
  - **Name**—Hostname of the VPNC.
  - **Type**—Type of device deployment.
  - **Model**—Hardware model of the device.
  - **Show Details**—Click the link to view the **Details** pane.
- Unmanaged—Displays the following details:
  - **Name**—Name of the unmanaged device.
  - **IP Address**—IP address of the unmanaged device.
  - **Show Details**—Click the link to view the **Details** pane.

The value of the **IP Address** parameter is empty if LLDP does not provide the neighbor information.

- Switch—Displays the following details:
  - **Name**—Hostname of the switch.
  - **Type**—Type of the device.
  - **Model**—Hardware model of the switch.
  - **Children**—Number of devices connected to the switch categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the switch based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
    - **Status**—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.
  - **VLANs**—List of VLANs configured on the switch. This field is displayed only when the **VLANs** option is selected under **Overlays**. For more information, see VLAN Overlay Details.
  - **Show Details**—Click the link to view the **Details** pane.
- Switch Stack—Displays the following details:
  - **Name**—Hostname of the switch stack.
  - **Type**—Type of the device.
  - **Model**—Hardware model of the switch.
  - **Children**—Number of devices connected to the switch categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the switch based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.

- **Status**—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.

◦ **VLANs**—List of VLANs configured on the switch. This field is displayed only when the **VLANs** option is selected under **Overlays**. For more information, see VLAN Overlay Details.

◦ **Show Details**—Click the link to view the **Details** pane.

- AOS-CX VSX Switch—Displays the following details:
  - ◦ **Name**—Name of the AOS-CX switch that is configured with VSX. The name is displayed in the **VSX_<Device Name>** format. For example, **VSX_8320-switch-primary**. However, in the map, this name is displayed in the **VSX_<first four characters of device name>...<last eight characters of device name>** format. For example, **VSX_8320...-primary**.
  - ◦ **Type**—Type of the device.
  - ◦ **Model**—Hardware model of the AOS-CX switch.
  - ◦ **VSX Role**—Role of the AOS-CX switch in the VSX configuration. Supported values are **Primary** and **Secondary**.
  - ◦ **Children**—Number of devices connected to the switch categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the switch based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
    - **Status**—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.
  - ◦ **VLANs**—List of VLANs configured on the switch. This field is displayed only when the **VLANs** option is selected under **Overlays**. For more information, see VLAN Overlay Details.
  - ◦ **Show Details**—Click the link to view the **Details** pane.
- Tunnel—Displays the alias map name of the tunnel configured on the Branch Gateway.

  In the topology map, the tunnels are shown as dotted lines. The tunnel in green color indicates that the tunnel is up. The tunnel in red color indicates that the tunnel is down.

  Click the tunnel link to view the **Details** pane.

In case of High Availability, the redundant gateway tunnel details are also displayed in the **Details** tab under **Virtual Tunnels** when you select the tunnel.

- Uplink—Displays the following information about uplinks configured on the Branch Gateway:
  - ◦ **<Name of the Branch Gateway>**—Displays the name of the Branch Gateway.
  - ◦ **Uplink**—Type of the uplink.
  - ◦ **VLAN**—VLAN ID of the uplink.
  - ◦ **Health Reason**—Displays the health status of the uplink. This parameter is only available when the uplink is down. The uplink in green color indicates that the uplink is up. The uplink in red color indicates that the uplink is down.

  Click the uplink to view the **Details** pane.

In case of High Availability, the redundant gateway tunnel details are also displayed in the **Details** tab under **Virtual Tunnels** when you select the uplink.

- Edge—Displays the following information about the link:
  - **<Name of the connected device>**—Name of the device connected with the edge link.
  - **<Interface number>**—Interface number of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Alternative links**—Number of the alternative links.

  The edge in green color indicates that the edge is up. The edge in red color indicates that the edge is down.

  Click the uplink to view the **Details** pane.
- Unmanaged edge—Displays the following information about the link:
  - **<Name of the connected device>**—Name of the device connected with the edge link.
  - **<Port Identifier>**—Port number of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Alternative links**—Number of the alternative links.

  The unmanaged edge in green color indicates that the unmanaged edge is up. The unmanaged edge in red color indicates that the unmanaged edge is down.

  Click the unmanaged edge link to view the **Details** pane.
- ISL edge in AOS-CX VSX toplogy map—Displays the following information about the link:
  - **ISL**—Number of inter-switch link (ISL) present between the AOS-CX switches configured with VSX
  - **Other Links**—Number of other links present between the AOS-CX switches configured with VSX.
  - **<Name of the connected device>**—Name of the device connected with the edge link.
  - **<Interface name>**—Interface name where the switches are connected to the devices.

Active tunnels are green in color and inactive tunnels are red in color. If there are multiple tunnels connecting to a VPNCs, and even if one of those tunnels is down, the tunnel mapping is displayed in red dotted lines.

Details Pane

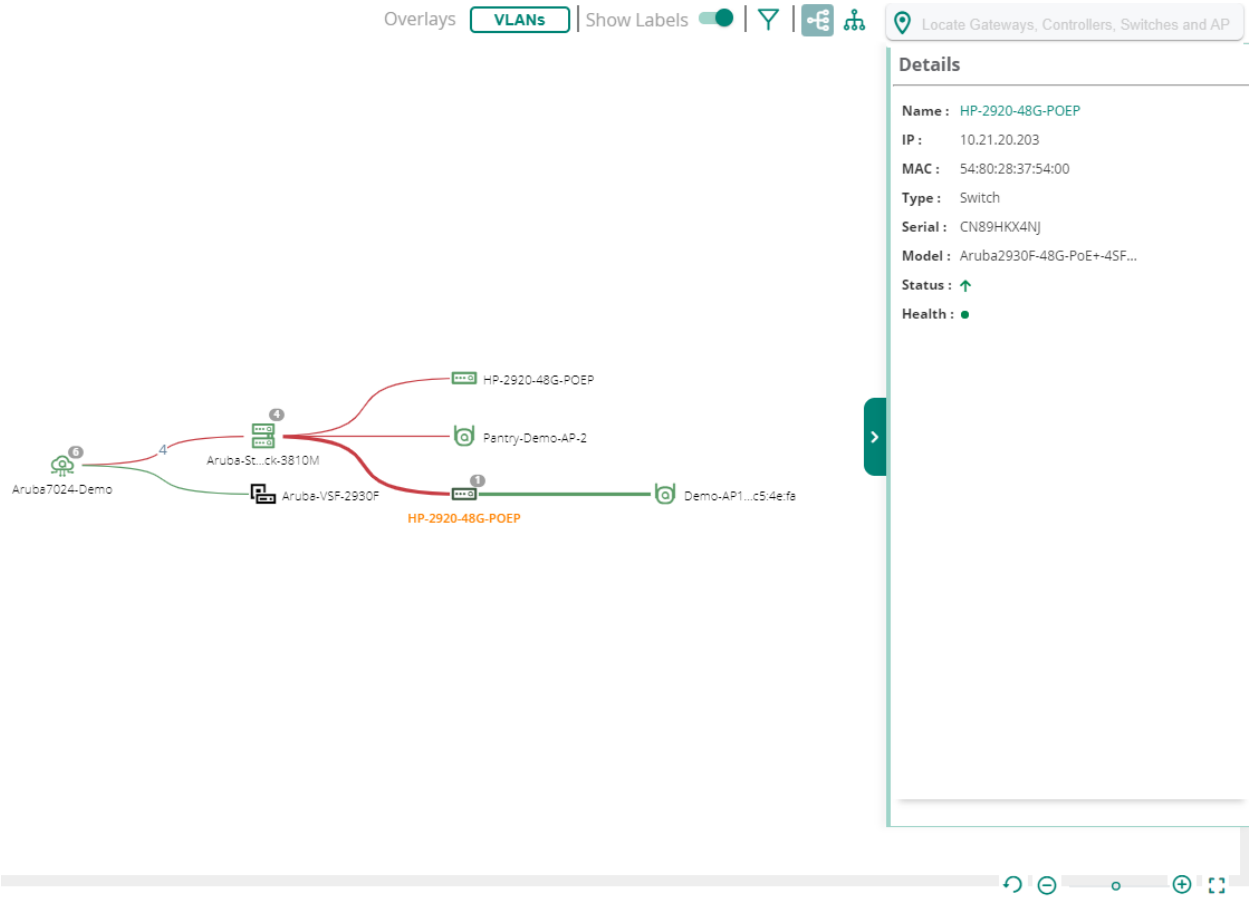
In the topology map, the **Details** pane provides a summary of the devices, uplinks, and tunnel details.

A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.

In the topology map, select a device and then click the **Show Details** link in the pop-up window to view the **Details** pane. To view the **Details** pane for a tunnel, uplink, or edge, click the link.

The **Details** task pane displays the following information:

Figure 363 *Details Pane*



- Access Point—Displays the following details:
  - **Name**—Hostname of the AP. Click the AP name to view the **Access Point Details** page.
  - **IP**—IP address of the AP.
  - **MAC**—MAC address of the AP.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the AP.
  - **Model**—Hardware model of the AP.
  - **Status**—Operational status of the AP.
  - **Health**—Operational health of the AP.
- Branch Gateway—Displays the following details:
  - **Name**—Hostname of the Branch Gateway. Click the Branch Gateway name to view the **Gateway Details** page.
  - **IP**—IP address of the Branch Gateway.
  - **MAC**—MAC address of the device.
  - **Type**—Type of device deployment.
  - **Serial**—Serial number of the Branch Gateway.
  - **Model**—Hardware model of the device.

- **Status**—Operational status of the device.
- **Health**—Operational health of the device.

- VPNC—Displays the following details:
  - **Name**—Hostname of the VPNC. Click the VPNC name to view the **Gateway Details** page.
  - **IP**—IP address of the VPNC.
  - **MAC**—MAC address of the device.
  - **Type**—Type of device deployment.
  - **Serial**—Serial number of the VPNC.
  - **Model**—Hardware model of the device.
  - **Status**—Operational status of the device.
  - **Health**—Operational health of the device.
- Unmanaged—Displays the following details:
  - **Name**—Name of the unmanaged device.
  - **Description**—Description of the unmanaged device.
  - **IP**—IP address of the unmanaged device.
  - **Capabilities**—Displays the capabilities of the unmanaged device.
    - **Supported**—Lists the supported capabilities of the unmanaged device.
    - **Enabled**—Lists the enabled capabilities of the unmanaged device.

The value of the parameters are empty if LLDP does not provide the neighbor information.

- Switch—Displays the following details:
  - **Name**—Hostname of the switch. Click the switch name to view the **Switch Details** page.
  - **IP**—IP address of the switch.
  - **MAC**—MAC address of the switch.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the switch.
  - **Model**—Hardware model of the switch.
  - **Status**—Operational status of the switch.
  - **Health**—Operational health of the switch.
- Switch Stack—Displays the following details:
  - **Name**—Hostname of the switch. Click the switch name to view the **Switch Details** page.
  - **IP**—IP address of the switch.
  - **MAC**—MAC address of the switch.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the switch.
  - **Stack Role**—Role of the switch in the stack.
  - **Model**—Hardware model of the switch.
  - **Status**—Operational status of the switch.
  - **Health**—Operational health of the switch.
  - **Stack Members**—Provides the **Name**, **Role**, and **State** details of the stack member. Click the stack member name to view the **Switch Details** page.

- AOS-CX VSX—Displays the following details:
  - **Name**—Hostname of the AOS-CX switch with VSX configured. Click the switch name to view the **Switch Details** page.
  - **IP**—IP address of the switch.
  - **MAC**—MAC address of the switch.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the switch.
  - **Model**—Hardware model of the switch.
  - **Status**—Operational status of the switch.
  - **Health**—Operational health of the switch.

  The **VSX** section displays the following details:
  - **ISL State**—State of the ISL connection with the peer AOS-CX switch. Following are the supported values:
    - **WAITING_FOR_PEER**—Waiting for connectivity to the peer.
    - **PEER_ESTABLISHED**—Steady state. VSX LAGs are up when the device is in this state.
    - **SPLIT_SYSTEM_PRIMARY**—Lost ISL connectivity to the peer and the device is operating as primary.
    - **SPLIT_SYSTEM_SECONDARY**—Lost ISL connectivity to the peer and the device is operating as secondary.
    - **SYNC_PRIMARY**—ISL connectivity to the peer restored and the device is syncing states to the peer.
    - **SYNC_SECONDARY**—ISL connectivity to the peer restored and he device is learning states from the peer. VSX LAGs are down when the device is in this state.
    - **SYNC_SECONDARY_LINKUP_DELAY**—Device has learned its states from the peer and monitoring for hardware is to be programmed. VSX LAGs are down when the device is in this state.
  - **ISL Port**—ISL port number of the selected AOS-CX switch. If the ISL is a LAG, then this field displays the LAG name.
  - **ISL Mgmt State**—Management state of the ISL. Following are the supported values:
    - **OPERATIONAL**—ISL management is operational.
    - **INTER_SWITCH_LINK_MGMT_INIT**—ISL management is in initialization state.
    - **CONFLICTING_OR_MISSING_DEVICE_ROLES**—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers.
    - **SW_IMAGE_VERSION_MISMATCH_ERROR**—Software version on the primary device does not match with the software version on the secondary device.
    - **INTER_SWITCH_LINK_DOWN**—ISL is down.
    - **INTERNAL_ERROR**—ISL management has internal errors.
  - **Config Sync Enabled**—Configuration synchronization between the VSX switches are enabled or disabled.
  - **Config Sync Status**—Status of the configuration synchronization between the VSX switches. Following are the supported values:
    - **IN-SYNC**—Configuration synchronization is operational and the VSX switches are in sync.
    - **DISABLED**—Configuration synchronization is disabled.

- **SW_IMAGE_VERSION_MISMATCH_ERROR**—Software image version on the primary device does not match with the software image version on the secondary device.
- **CONFLICTING_OR_MISSING_DEVICE_ROLES**—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers.
- **PEER_DB_CONNECTION_ERROR**—Error in connecting to peer database. It involves errors due to ISL or ISL management.
- **CONFIGURATION_SYNC_CONFLICT**—Configuration synchronization is operational, but has conflicts synchronizing the configuration. Conflicts can occur if the configuration on the primary device is marked for sync, but the same configuration on the secondary device is not marked for sync.
- **CONFIGURATION_SYNC_MISSING_REFERENCE**—Configuration synchronization is operational, but has missing references in synchronizing the configuration.

◦ **Role**—Role of the AOS-CX switch in the VSX configuration. Supported values are **Primary** and **Secondary**.
◦ **Peer IP**—IPv4 address of the peer switch.
◦ **Peer Serial**—Serial number of the peer switch.
◦ **Peer MAC**—MAC address of the peer switch.
◦ **Peer Name**—Hostname of the peer switch.
◦ **Last Seen**—Date on which the peer switch was last synced.

- Tunnel—Displays the following information about tunnels configured on the Branch Gateway:
  ◦ **Map Name**—Name of the tunnel interface.
  ◦ **Peer MAC**—MAC address of the peer device with which the tunnel was established.
  ◦ **Local MAC**—MAC address of the Branch Gateway.
  ◦ **Source IP**—Source IP address from where the traffic originates.
  ◦ **Destination IP**—IP address to which the traffic is sent.
  ◦ **Established Time**—Timestamp showing when the tunnel was established.
  ◦ **VLAN**—VLAN ID of the tunnel.
  ◦ **Source Serial**—Source Serial of the tunnel.

  The tunnel in green color indicates that the tunnel is up. The tunnel in red color indicates that the tunnel is down.
- Uplink—Displays the following information about uplinks configured on the Branch Gateway:
  ◦ **Uplink Type**—Type of the uplink.
  ◦ **VLAN**—VLAN ID of the uplink.
  ◦ **Link Status**—Uplink status.
  ◦ **Description**—Description of the uplink.
  ◦ **WAN Status**—WAN status.
  ◦ **IP Address**—IP address of the WAN interface.
  ◦ **Public IP Address**—Public IP address.
  ◦ **Device MAC**—MAC address of the device.
  ◦ **Serial**—Serial number of the device.
  ◦ **Port Number**—Port number of the device.
  ◦ **Tunnels**—Displays a list of tunnels mapped to the uplink. Click the drop-down on each tunnel to view the tunnel details.

The uplink in green color indicates that the uplink is up. The uplink in red color indicates that the uplink is down.

- Edge—Displays the following information about the link:
  - **Interface numbers**—Interface numbers of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Interface**—Interface number of the device.
  - **Serial**—Serial number of the device.
  - **Device Name**—Name of the device.
  - **Port Number**—Port number of the device.

In case of Branch Office Controller (BOC) to Switch link, if a peer Branch Gateway link is configured for redundancy, link details are displayed for the peer Branch Gateway to switch link as well.

- Unmanaged edge—Displays the following information about all the links:
  - **Interface numbers**—Interface numbers of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Interface**—Interface number of the device.
  - **Serial**—Serial number of the device.
  - **Device Name**—Name of the device.
  - **Port Number**—Port number of the device.
  - **Interface**—Interface number of the unmanaged device.
  - **MAC**—MAC address of the unmanaged device.
  - **Device Name**—Name of the unmanaged device.
  - **Port Identifier**—Displays the port ID, port name, or MAC address of the unmanaged device.
- ISL edge in AOS-CX VSX toplogy map—Displays the following information about the ISL edge:
  - **Inter-Switch Link Status**—Status of the ISL connection with the peer.
  - ***<LAG-name>* - ISL** section displays details about all the interfaces that are part of the LAG. This section also displays the details of the devices connected to these interfaces. It displays the following details:
    - **Serial**—Serial number of the individual device.
    - **Device Name**—Name of the individual device.
    - **Port Number**—Port number of the individual device.
  - **Other**—This section displays details about the other links present between the VSX configured AOS-CX switches. It displays the following details:
    - **Serial**—Serial number of the individual device.
    - **Device Name**—Name of the individual device.
    - **Port Number**—Port number of the individual device.

Unreachable Devices

The **Unreachable Devices** pane provides information about the orphan and the offline unmanaged devices. An unmanaged device is considered to be orphan when all its neighboring Aruba devices get deleted and are only displayed in the **Unreachable Devices** list. An unmanaged device is considered to be offline

when all its neighboring Aruba devices are offline and are displayed both in the **Topology** map and in the **Unreachable Devices** list.

When an unmanaged device is either offline or disconnected, they are only displayed in the **Unreachable Devices** list. The devices listed in the **Unreachable Devices** pane are deleted after 15 days.

To view the **Unreachable Devices** pane, click the **Unreachable Devices** button. The **Unreachable Devices** pane displays the following details:

- **Name**—Name of the unmanaged device.
- **Type**—Type of the unreachable device.
- **MAC**—MAC address of the unmanaged device.
- **Last Seen**—The last active time and date of the unmanaged device.

VLAN Overlay Details

The topology map displays information about the VLANs configured on switches running AOS-Switch and AOS-CX software. To view the VLAN information:

1. Select the **VLANs** option under **Overlays**. The **VLANs** pane is displayed and the network elements in the topology map, such as device icons and edge links, are grayed out.

   The **VLANs** pane displays the first 50 VLANs (unique VLAN ID and name pairs) in the ascending order of VLAN IDs. To search for other VLANs, click the search icon.
2. Select a VLAN from the **VLANs** pane. You can also enter a VLAN name or ID in the search box.
3. The topology map displays the following information:
   - The switches that have the selected VLANs configured are highlighted in a color depending on the status of the switch, green for online and red for offline.
   - The edge link connecting two switches is highlighted in blue, if the following conditions are met:
     - The VLAN IDs are present in both the switches and in the ports associated with the edge link between the switches.
     - The VLAN type (tagged or untagged) configured is the same in both the switches.
4. Hover over the switch to view the list of all VLANs (comma separated) configured on the switch.

   The VLAN IDs are also listed as a range if consecutive VLAN IDs are configured. For example, 100-178, 190, 210.
5. Hover over the edge link connecting the two switches. The pop-up displays the following information:
   - Host name of the switch
   - Serial number of the switch
   - VLAN ID
   - Type of VLAN: **tagged**, **untagged**, or **missing**

Monitoring SaaS Express

The **SaaS Express** monitoring dashboards are used for viewing the SaaS-related information. It displays charts with Quality of Experience (QoE) scores for all the SaaS applications that are being monitored or optimized. Branch Gateways measure the network performance in terms of packet loss, latency, jitter, and MOS, and sends that data to Aruba Central. Then, these Key Performance Indicators (KPI) and the Quality of Experience are displayed in Aruba Central. The QoE value is calculated based on the discrete data obtained in every measurement along with their trend. This allows Aruba Central to highlight how one-off events like sudden latency or packet loss spikes could be seen as a drop in performance. The insights gained from the

monitoring dashboards identify applications that are not performing well and help correlate this information with the geographical region, the ISP, and so on to root-cause the potential problem.

To view the performance of the SaaS applications, you must have configured the required SaaS applications in the corresponding Branch Gateway groups. For more information, see Configuring SaaS Express.

You can monitor SaaS Express from the following dashboards:

- Global Dashboard
- Site Dashboard
- Gateway Dashboard

Global Dashboard

To view the SaaS Express monitoring dashboard for all sites in the Aruba Central account, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications** > **SaaS Express**.
   By default, the map view of the Saas Express dashboard is displayed.
3. Click **List** to view details in a tabular format.

The following views are available in the Global dashboard:

- Map View
- List View

Map View

The map displays the sites with Branch Gateways in which SaaS Express is configured. The sites in which the QoE scores of all the SaaS applications are good are displayed in green. If one of them is fair or poor, the site is displayed in yellow or red, respectively. The default QoE scores are displayed at the bottom of the table along with the status color. You can view scores based on the performance of the applications only for the last three hours.

The QoE threshold values can be customized. The default QoE scores are classified as follows.

Table 295: *Status and Color for QoE Score*

Application Status	Color	QoE score
Good	Green	7 to 10
Fair	Orange	3 to 7
Poor	Red	0 to 3

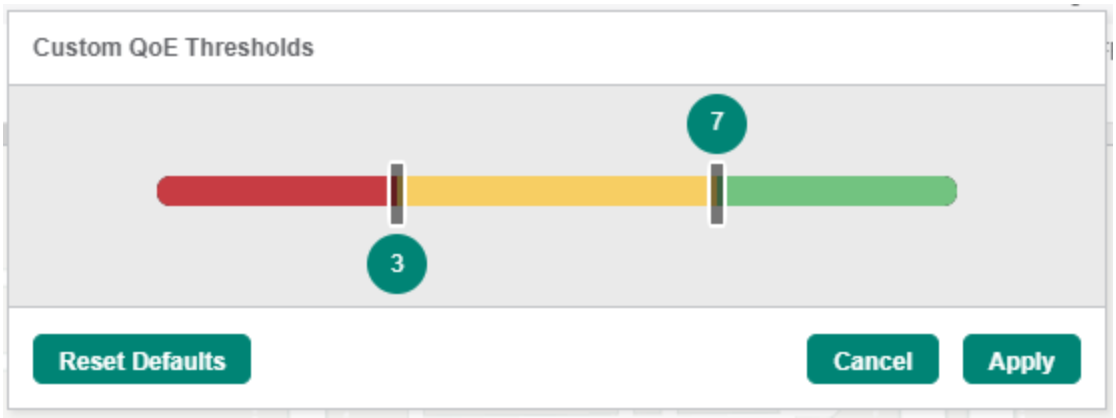
Customize QoE Thresholds

To customize the QoE threshold values:

1. In the **Application Health** section, click the Edit icon .
   The **Custom QoE Thresholds** pane is displayed.
2. Select and drag the bars left or right to increase or decrease the values.

3. Click **Apply**.
   The threshold values are successfully customized and displayed at the bottom of the table.
4. To reset to the default values, click **Reset Defaults**.

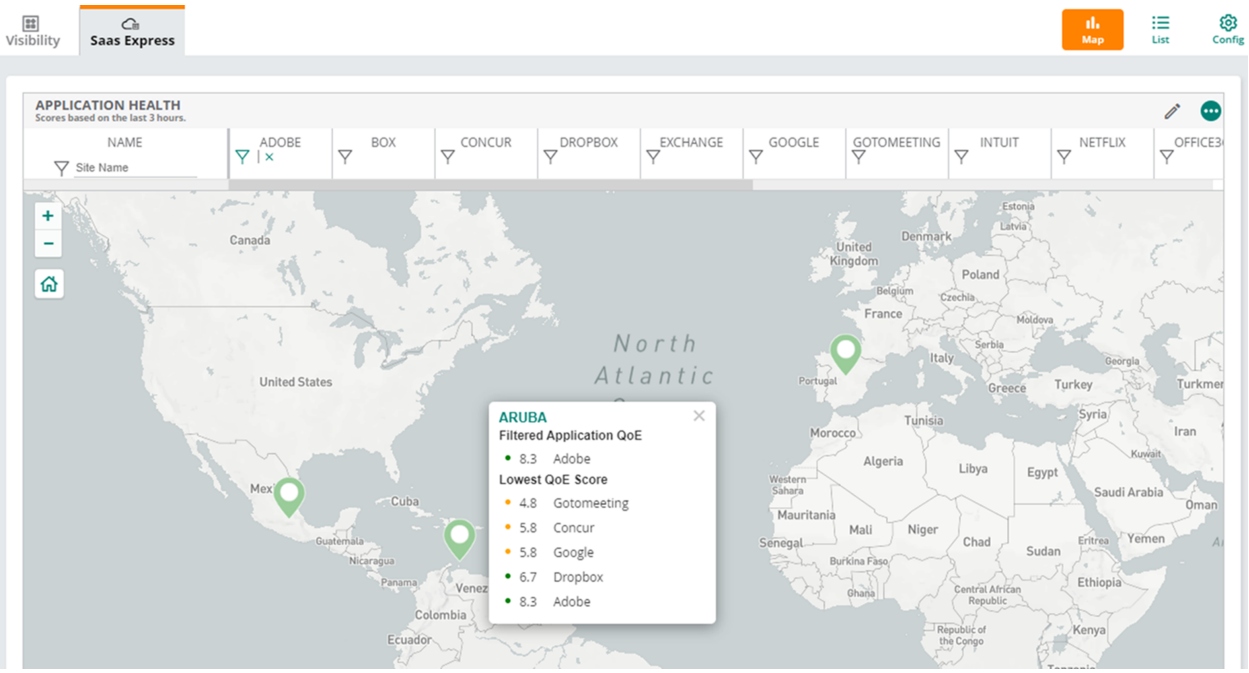
Figure 364 *Custom QoE Thresholds Pane*



The following actions are available in the map view:

- Click the **+** or **-** icons to zoom in or zoom out in the map view.
- Click the Home icon to reset the map view.
- Enter the site name in the **Name** column and click the icon to only view the details of the required site.
- Click the icon in the application name column to view sites where that particular application is running. To clear the selection, click the **x** icon.
- Click the pin (site) to view the site name and five applications with Lowest QoE Score in the pop-up dialog box. Click the site name to navigate to the site dashboard and view the details of all applications. For more information, see Site Dashboard.
- To view the QoE for a particular application on the site, click the icon in that application column. Then, click the pin (site) to view **Filtered Application QoE** in the pop-up dialog box.
- Click the Edit icon to customize the QoE thresholds.
- Click the ellipsis icon to select the required applications to be displayed in the table.

Figure 365 *Map View—SaaS Express Monitoring Dashboard*



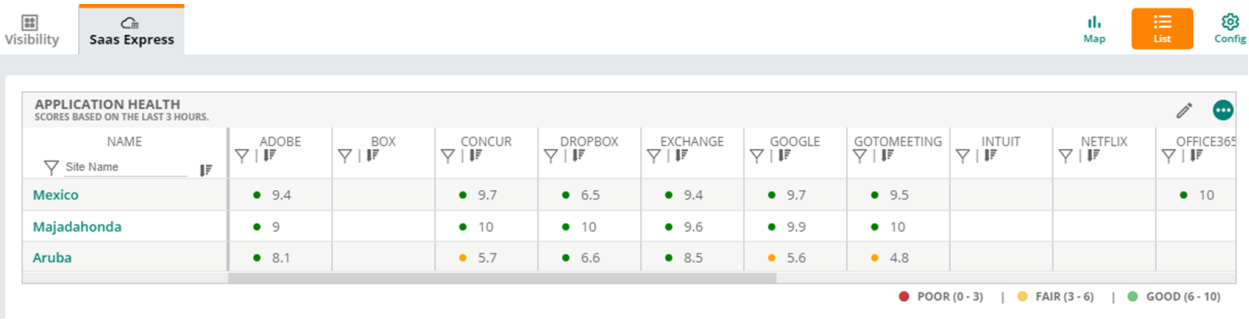
List View

The list view displays the **Application Health** table consisting of the QoE scores of all the sites for all the applications for the last three hours. The default QoE scores are displayed at the bottom of the table along with the status color.

The following actions are available in the list view:

- Enter the site name in the **Name** column and click the icon to only view the details of the required site.
- Click the Filter icon in the application name column and select the **Poor**, **Fair**, or **Good** option to view the corresponding score based on the selection. You can select multiple options.
- Click the and icons in the column to sort the list from **Good** to **Poor** or vice versa.
- Click the Edit icon to customize the QoE thresholds.
- Click the ellipsis icon to select the required applications to be displayed in the table.
- Click the site name in the **Name** column to navigate to the dashboard that displays Site-specific information. For more information, see Site Dashboard.

Figure 366 *List View—SaaS Express Monitoring Dashboard*



Site Dashboard

The details displayed in the site dashboard provide more granular insights into the performance of the SaaS applications.

To view the SaaS Express monitoring dashboard for a specific site, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
2. Under **Manage**, click **Applications** > **SaaS Express**.

   The **Saas Express** monitoring dashboard for that site is displayed.

The following sections are available in the Site dashboard:

- SaaS Express Summary
- SaaS Express Details

By default, the details displayed are for **3 Hours** time range. To change the time, click the **Time Range** filter and select the required option. The available options are:

- **3 Hours**
- **1 Day**
- **1 Week**
- **1 Month**
- **3 Months**

SaaS Express Summary

The **SaaS Express Summary** section displays the following information:

- **Total Apps**—The total number of active applications.
- **Categories Per Exit**—The total number of WAN interfaces for each application category.
- **Avg QoE**—An average of all the three scores: Loss, Latency, and Jitter.
- **Avg Loss**—The average percentage of packet loss during transmission.
- **Avg Latency**—The average time taken to transmit data packets to the destination in milliseconds.
- **Avg Jitter**—The average time delay or jitter in transmitting data packets over the network in milliseconds.

SaaS Express Details

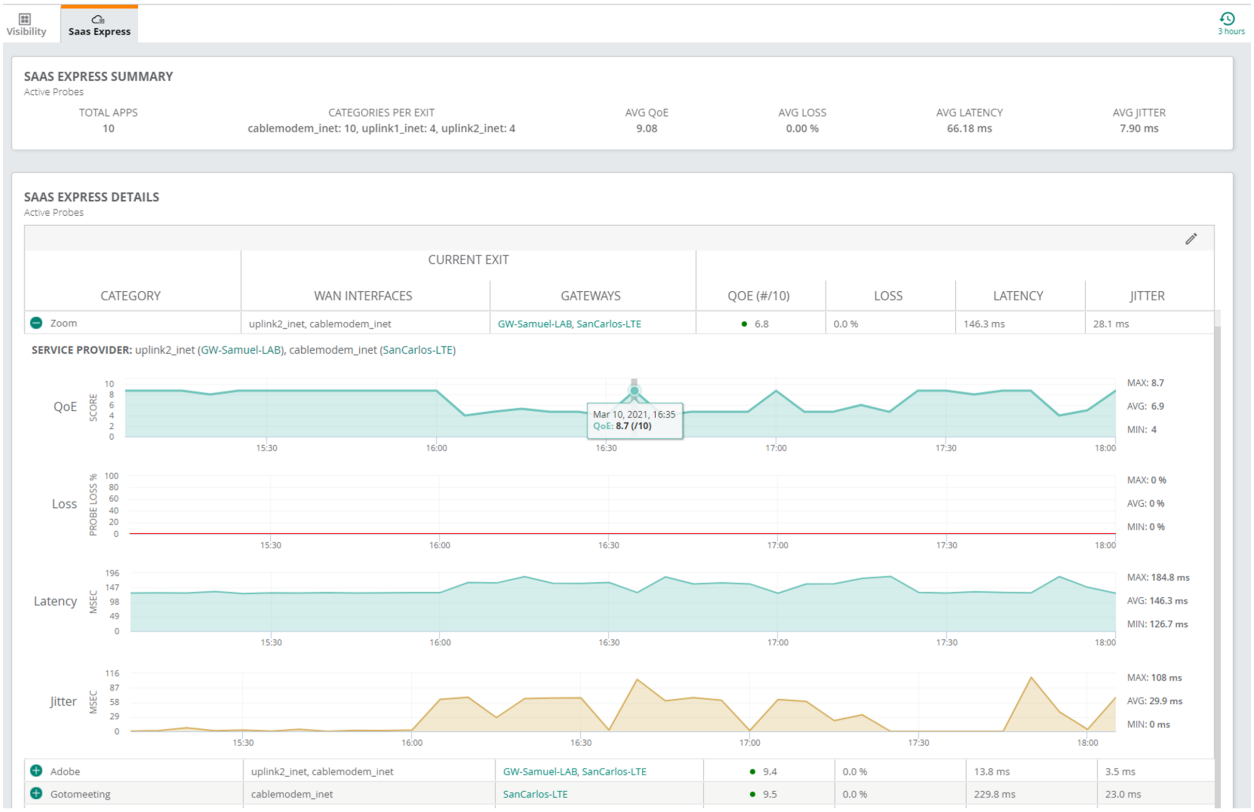
The **SaaS Express Details** table in this section displays the following information for each active SaaS application category:

- **Category**—The name of the SaaS application category.
- **Current Exit**
  - **WAN Interfaces**—The uplink through which the SaaS application traffic traverses.
  - **Gateways**—The Branch Gateway through which the SaaS application traffic traverses.
- **QoE (#/10)**—The average score (out of 10) based on the loss, latency, and jitter values.
- **Loss**—The percentage of packet loss during data transmission.
- **Latency**—The time taken to transmit data packets to the destination that is displayed in milliseconds.
- **Jitter**—The time delay or jitter in transmitting data packets over the network that is displayed in milliseconds.

The following actions are available:

- In the **SaaS Express Details** section, click the Edit icon to customize the QoE thresholds. For information about how to customize, see Customize QoE Thresholds.
- In the **Category** column, click **+** next to the category name to expand the graphical representation of the application performance. To collapse the graph, click **-**.
- Hover over the graph to view the values at a particular time of the day or the day of the week and so on, depending on the time range selected. The maximum, minimum, and average scores for each parameter for the selected time range are displayed next to the QoE, loss, latency, and jitter graph.

Figure 367 *Site View - SaaS Express Monitoring Dashboard*



Gateway Dashboard

The gateway dashboard provides additional information about the SaaS traffic traversing the gateways. The **Measured QoE** values (based on the synthetic probes to the SaaS front -doors) and the **Observed LAN/WAN QoE** values (based on inspecting TCP sessions as they traverse the gateway) can be analyzed. This allows the network administrator to correlate between what is being measured with what is being observed.

To view the SaaS Express monitoring dashboard for a specific gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Select the required gateway that is configured for SaaS Express.

   The dashboard context for the selected gateway is displayed.
4. Under **Manage**, click **Applications** > **SaaS Express**.

   The **Saas Express** monitoring dashboard for that gateway is displayed.

The following sections are available in the Gateway dashboard:

- SaaS Express Summary
- SaaS Express Details

By default, the details displayed are for **3 Hours** time range. To change the time, click the **Time Range** filter and select the required option. The available options are:

- **3 Hours**
- **1 Day**
- **1 Week**
- **1 Month**
- **3 Months**

SaaS Express Summary

The **SaaS Express Summary** section displays the following information:

- **Total Apps**—The total number of active applications.
- **Categories Per Exit**—The total number of WAN interfaces for each application category.
- **Avg QoE**—An average of all the three scores: Loss, Latency, and Jitter.
- **Avg Loss**—The average percentage of packet loss during transmission.
- **Avg Latency**—The average time taken to transmit data packets to the destination in milliseconds.
- **Avg Jitter**—The average time delay or jitter in transmitting data packets over the network in milliseconds.

SaaS Express Details

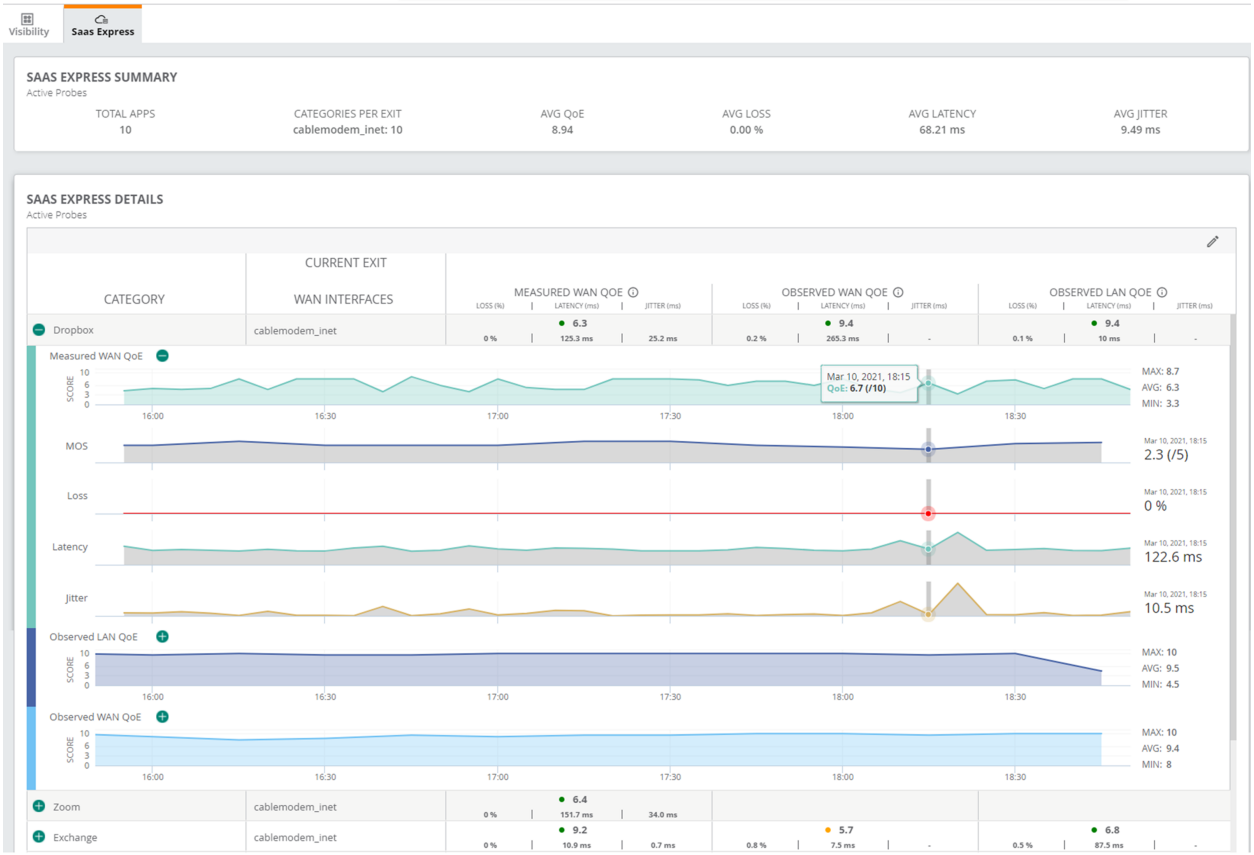
The table in this section displays the following information for each active SaaS application category:

- **Category**—The name of the SaaS application category.
- **Current Exit**
  - **WAN Interfaces**—The uplink through which the SaaS application traffic has traversed.
- **Measured WAN QOE**—The QoE score is based on the active probe and uplink application statistics. The **Loss**, **Latency**, and **Jitter** values are in milliseconds.
- **Observed LAN QOE**—The QoE score is based on analyzing the LAN segment of the communication as downlink SaaS traffic traverses the gateway. The **Loss** and **Round Trip Time (RTT)** values are in milliseconds.
- **Observed WAN QOE**—The QoE score is based on observing the WAN segment of the communication as uplink SaaS traffic traverses the gateway.

The following actions are available:

- In the **SaaS Express Details** section, click the Edit icon to customize the QoE thresholds. For information about how to customize, see Customize QoE Thresholds.
- In the **Category** column, click **+** next to the category name to expand the graphical representation of the application performance. To collapse the graph, click **-**.
  - Hover over the graph to view the values at a particular time of the day or the day of the week and so on, depending on the selected time range. The maximum, minimum, and average scores for each parameter for the selected time range are displayed next to the **Measured WAN QoE**, **Observed LAN QoE**, and **Observed WAN QoE** graphs.
- In the graphical representation, click **+** next to the **Measured** or **Observed QoE** to expand and view the **Mean Opinion Score (MOS)**, **Loss**, **Latency**, and **Jitter** values. To collapse the graph, click **-**.
  - Hover over the graph to view the values at a particular time of the day or the day of the week and so on, depending on the time range selected. The maximum, minimum, and average scores for each parameter for the selected time range are also displayed.

Figure 368 *Gateway—SaaS Express Monitoring Dashboard*



Gateway Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts.

Following are the SD-WAN and Gateway appliance-related alerts that you can configure:

- **SLA DPS Compliance Violations**—Generates an alert when the WAN policy does not meet the compliance criteria.
- **New Gateway Connected**—Generates an alert when a new Branch Gateway is connected.
- **Gateway Disconnected**—Generates an alert when a Branch Gateway is disconnected. When a gateway disconnects because of license expiry, the alert description shows 'Reason: Device unlicensed'.
- **Gateway CPU Utilization**—Generates an alert when the Branch Gateway CPU utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Gateway Memory Utilization**—Generates an alert when the Branch Gateway memory utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **OSPF Session Error**—Generates an alert when an OSPF session fails.
- **BGP Session Error**—Generates an alert when a BGP session fails.
- **Gateway Base License Capacity Limit Exceeded**—Generates an alert when a Gateway with Foundation-Base Capacity subscription exceed the client capacity threshold.
- **Routing Table Limit**—Generates an alert when the routing table size exceeds the 90% of the capacity. This alert is auto-acknowledged when the Routing table size goes below 85% of the capacity.

- **BGP Neighbor Route Limit**—Generates an alert when the number of routes received from a BGP neighbor exceeds the configured limit. This alert is auto-acknowledged when the number of routes from the BGP neighbor goes below the configured limit.
- **Overlay Route Orchestrator Connection**—Generates an alert when the control connection between the Branch Gateway and the Overlay Route Orchestration (ORO) is down. This alert is auto-acknowledged when the control connection is re-established.
- **Gateway Cellular Data Usage**—Generates an alert when the cellular data usage exceeds the threshold value. You must set the **Data Usage alert limit** and **Billing start date** in the **Uplink** configuration page for this alert to generate.

  Note: This alert configuration is only applicable for 9004-LTE gateways that have an integrated LTE modem.
- **WAN Health-Check Failure**—Generates an alert when WAN health check fails.
- **WAN VPN-Peer Unreachable**—Generates an alert when the WAN VPN peer is unreachable.
- **WAN Uplink Status Change**—Generates an alert when the WAN uplink status changes.
- **WAN Uplink Autonegotiation State Change**—Generates an alert when the WAN uplink automatic negotiation status changes.
- **WAN Uplink Input Errors**—Generates an alert when the percentage of WAN uplink input errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink Output Errors**—Generates an alert when the percentage WAN uplink output errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule (s) for this alert.
- **WAN Uplink PHY Errors**—Generates an alert when the percentage WAN uplink PHY errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **DHCP Pool Consumption Alert**—Generates an alert when the percentage DHCP pool consumption exceeds the threshold value. In the **Subnet** field, enter the subnet address to filter the alert based on subnet.
- **IPSec Establishment Failure**—Generates an alert when the IPsec tunnel fails to establish.
- **IPSec SA Down**—Generates an alert when the IPsec SA is down.
- **All IPSec SAs Down**—Generates an alert when all the IPsec SAs are down.
- **CFG-SET Advertisement Failure**—Generates an alert when the CFG-SET advertisement fails.
- **Uplink Flapping**—Generates an alert when the uplink state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Tunnel Flapping**—Generates an alert when the tunnel state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Uplink Speed Flapping**—Generates an alert when the uplink speed changes. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **EST Enrollment Failure**—Generates an alert when the Virtual Gateway fails to enroll with the EST server.
- **VGW VM Down**—Generates an alert when an Aruba Virtual Gateway deployed as a Virtual Machine is down.
- **Gateway Firmware Upgrade Failed**—Generates an alert when there is a firmware upgrade failure.
- **Gateway IDS/IPS Engine Error State**—Generates an alert when the Gateway's IDS/IPS Engine state is either crashed or stopped. A severity of **Critical** indicates that the engine has crashed and **Major** indicates that the engine has stopped.

- **Gateway IDS IPS Engine CPU Utilization**—Generates an alert when the CPU utilization by IDS/IPS engine exceeds the threshold value and duration. You can add additional rule(s) for this alert.
- **Gateway IDS IPS Engine Memory Utilization**—Generates an alert when the memory utilization exceeds the threshold value and duration. You can add additional rule(s) for this alert.
- **Gateway IDS IPS Engine Packer Dropped Detected**—Generates an alert every time when the number of packets dropped exceeds the configured threshold value.
- **Gateway Threat Count**— Generates an alert when the number of threats exceeds the configured limit (Range - 50 to 500 threats) in the given duration. The gateway threat counts are aggregated at the device level.
- **Gateway Threat Count Per Signature**— Generates an alert when the number of threats associated with a specific signature exceeds the configured limit in the given duration. These alerts are aggregated for all the gateways at the customer level.

Currently, Aruba IDPS is supported only on 9004, 9012, and 9004-LTE Branch Gateways that have Security license entitled to them.
Alerts that fall under WAN/ Tunnels/ DPS/ Routing/ Firewall are not applicable to Aruba Unified Network Architecture deployments.

You can configure the following alerts for gateways running ArubaOS 8.0.x:

- **Gateway Emergency Mode**—Generates an alert when a gateway enters the emergency mode, where all the uplinks are down and the backup uplink is activated.
- **VPN Peer Failover**—Generates an alert when all the tunnels from the gateway to the primary VPN controller go down including via backup uplink and establishes a tunnel with the secondary VPN controller.

You can configure and enable these alerts for gateways running other ArubaOS versions also. However, these alerts will not be generated for gateways on versions other than ArubaOS 8.0.x.

Reports

The Aruba Central dashboard enables you to create various types of reports. To create a report, you must have Read/Write or Admin access for Aruba Central.

The Reports feature is available for Foundation license of APs, switches, and gateways.

Viewing the Reports Page

To view the **Reports** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.

The **Reports** page has the following sections:

- **Browse**—Allows you to browse through the generated reports.
- **Manage**—Allows you to manage the scheduled reports.
- **Create**—Allows you to create and schedule a report.

This section includes the following topics:

Report Categories

The following list provides information about the types of report under each category of the report. For information about how to configure the Context, Transport Type, Report Order, Top N Count, Classify On, Report Subtype, Report Period, Recurrence, and Report Information for a report, see Report Configuration Options

- **Clients**
  - **Client Inventory**—The Client Inventory report provides information about the total number of clients and the type of connected networks that assists the administrators in planning for scalability and to evaluate the deviations from the baseline. You can select the context of the report from the available options:
    - **Groups**
    - **Labels**
    - **Sites**
  - **Client Session**—The Client Session report monitors the sessions of all the users in the network and provides insights related to usage analysis and connectivity patterns. In the Central 2.5.3 release, the report also projects the WLAN user experience to assist the user in measuring the efficiency of the deployed networks. You can select the context of the report from the available options:
    - **Groups**
    - **Labels**
    - **Sites**
  - **Client Usage**—The Client Usage report displays the client usage and client connectivity details to assist the administrator in planning the expansion of the network and the application requirements. You can select the context of the report from the available options:
    - **Groups**
    - **Labels**
    - **Sites**
  - **Guest**—Displays the guests and guest session details for all the SSIDs for a specific time period. The Guest report provides visibility for all the users associated to the cloud guest network that assists the user in conducting campaigns and also provides analytics of the guest users in the network.

Guest report does not support location based filtering for any selected device group, site, or label to ensure end user privacy protection.

- **Summary**—Displays the details about the wireless and wired clients, and the usage details of the wireless and wired clients over a time period of the last one year (except the current date). The Summary report assists the user in measuring the Key Performance Indicator (KPI) trends for the last one year that aids the user in planning for scalability.
  In the **Summary** report, you can choose to generate a report from **Trends** such as **Unique clients per day**, **Clients per SSID**, **Unique client sessions per day**, **Average client sessions per day**, **Average clients per day**, and **Usage over time**. The **Average clients per day** is the number of concurrent users at a given time (updated every five minutes). **Unique clients per day** is the total number of clients that were seen for that day. For example, consider a scenario where four clients were connected in a day, and after every hour, one client disconnected and another was connected. Then, the count for **Average clients per day** was four and **Unique clients per day** was 27 (3+24 =27).
  You can further chose to generate a report form **Top N Widgets** such as **Top clients by usage**, **Top OS by usage**, **Top APs by usage**, **Bottom APs by usage**, **Top sites by WLAN usage**, and **Bottom sites by WLAN usage**. The **Top sites by WLAN usage** and **Bottom sites by WLAN usage** options are only available under **Top N widgets** section, when you select **All** in the **Groups** context level. You can choose **Top 5**, **Top 10**, **Top 25**, or **Top 50** from the **Show Results** drop-down list to view the data for top 5, top 10, top 25, or top 50 widgets. You can select the context of the report from the available options:
  - **Groups**
  - **Label**
  - **Site**

The **Summary** report is supported from Aruba Central 2.5.2 onwards and the data is available only after an upgrade to version 2.5.2 or later. Data prior to the 2.5.2 upgrade is not available in the report.

- **Infrastructure**
  - **Capacity Planning**—The Capacity Planning report provides information about the subscription utilization and most used devices in the network that assists the administrator to add more devices in a specific location to enhance the scalability and to increase the uplink capacity of the switching infrastructure. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
  - **Configuration & Audit**—Displays the configuration and audit logs for all the device management, configurations, and user management events triggered in Aruba Central. The Configuration & Audit report aids the user in tracking the configuration changes in the network that assists in tracking the deviations from the IT polices. The context available for this report is only **Groups**.
  - **Infra Inventory**—Displays the inventory and subscription information for the devices that are online or offline during a specific time period. The Infra Inventory report aids the user in maintaining a record of the infrastructure devices and validate the firmware versions compliance. You can select the context of the report from the available options:

- **Groups**
- **Label**
- **Site**

- **Network**—Displays the summary details of the network that aids the user in measuring the availability of every device in the network and projects compliance to the defined Network SLAs. You can select the context of the report from the available options:
  - **Groups**
  - **Label**
  - **Site**
- **New Infra Inventory**— The New Infra Inventory report provides detail of the infrastructure devices added in a time period that assists the administrator in validating the network deployment progress against the deployment schedule. You can select the context of the report from the available options:
  - **Groups**
  - **Label**
  - **Site**
- **Resource Utilization**—Displays the details of the infrastructure devices that exceeded the configured thresholds on a daily, weekly, and monthly basis in the report. The Resource Utilization report provides information about the devices with high CPU and memory utilization that assists the administrator in evaluating the deviations against the device utilization baselines. You can select the context of the report from the available options:
  - **Groups**
  - **Label**
  - **Site**
- **RF Health**—The RF Health report provides detail of the radios of an access point with poor health indicators and assists the administrator in evaluating the deviation from the network baselines. You can select the context of the report from the available options:
  - **Groups**
  - **Label**
  - **Site**
- **Switch Capacity Planning**—The Switch Capacity Panning report provides an user with insights on the used and unused ports usage along with power consumed by clients that helps the user plan for scalability. You can select the context of the report from the available options:
  - **Groups**
  - **Label**
  - **Site**

The data for this report is generated only after you upgrade to Aruba Central version 2.5.2. You can view or generate the report for 1, 7, 30, and 90 days after upgrading to Aruba Central version 2.5.2.

- **WAN Availability**—The report displays the WAN overlay and underlay availability information. You can select the transport type for the report from the available options:
  - **Overlay**
  - **Underlay**

- **WAN Inventory**—Displays a list of Branch Gateways onboarded. The report is segregated by ArubaOS software version.
- **WAN Compliance**—Displays the worst performing or best performing links according to the SLA compliance violations.
- **WAN Transport Health**—Displays the top N links with probed values. You can select the transport type for the report from the available options:
  - **Overlay**
  - **Underlay**
- **WAN Utilization**—Displays WAN bandwidth utilization information for Underlay, Overlay, and overall network. You can select the transport type for the report from the available options:
  - **Overlay**
  - **Underlay**
- **WAN Web Content Classification**—The WAN Web Content Classification report provides information regarding the URLs, IP reputations, and geo-locations that aids an user in implementing policy enforcements. You can select the transport type for the report from the available options:
  - **Internet**
  - **VPN**

- **Security Compliance**
  - **PCI Compliance**—Displays the PCI Compliance result with the number of violations and the PCI DSSv3.2 for an Instant AP. The PCI compliance report automatically executes some of the test cases of the PCI DSS test requirements and projects compliance results that reduces the manual efforts in validating the test cases. The context available for this report is only **Groups**.
  - **RAPIDS**—Displays the details of all the rogue devices in the network that assists the administrator about the possible threat and provides essential information needed to locate and manage the threat. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
  - **Security Compliance**—Displays the details of the rogue APs and wireless intrusions detected in the network that assists the administrator in validating the compliance to the security guidelines. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
- **Applications**
  - **AppRF**—Displays the application usage report for a specific device group in the network. The AppRF report provides information about the application usage patterns and the web usage patterns in the network that assists the administrators in evaluating the deviations from the data usage patterns. The context available for this report is only **Groups**.

Important Points to Note

- When you select **Custom range** under **Report Period**, the **Every day**, **Every week**, and **Every month** options are not available under **Recurrence**.

- For the **Client Session** report, the **Show Detailed Report** option is available only for a selected site. Selecting this option restricts the **Report Period** to **Last Day** and **Custom Range** only. Selecting custom range enables you to select a one day time range from the particular day till the last seven days only.
- In the **Infra Inventory** report, select the **Offline** option in the **Device Inventory** section to generate the report with details of the devices that are offline. The PDF displays the distribution of inactive devices by the device type and CSV displays the list with additional information.
- In the **Configuration and Audit** report with local overrides details, the count for device override is available only for the **Groups** context. To include local overrides column in the **Configuration and Audit** report, select the **Show Override** option in the **Audit Report** section.
- When a new switch connects to Aruba Central, the **Last Used at** and **Unused Since (Days)** columns value is displayed as **NA** for all the ports that are down in the .csv file, that is created for the Switch Ports in the **Switch Capacity Planning** report. When a port continues to be in a down state, the **Last Used at** and **Unused Since (Days)** columns value will be displayed as **NA** for the time period of the generated report.

Previewing a Report

Aruba Central allows you to preview a type of report prior to generating the report. The preview of the report displays dummy values.

To preview the report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The Reports page is displayed in the **Summary** view.
3. Click **Create**.

   The **Reports** page is displayed in the **List** view.
4. Hover over a report and then click **Preview** to preview the report.

The report preview provides the following details:

- **Report Name**—Name of the report.
- **Report Type**—Type of the report.
- **Date Run**—Time when the report was last run.
  - **Group/Device**—The group or device for which the report was run.

In the preview of the report, the **PDF**, **CSV**, and **Email to** icons are dummy icons.

For more information about the reports under each category, see Report Categories.

Report Configuration Options

Aruba Central allows you to create various types of reports based on your network requirements. For information about each type of report, see Report Categories.

The types of report categories supported by Aruba Central are:

- **Clients**
- **Infrastructure**
- **Security Compliance**
- **Applications**

Sections in Reports

Context

Allows you to select the context for which you want to create the report. Select one of the available options from the following:

- **Groups**—Allows you to generate the report for the devices attached to a group.
  - **Filter By**—Select either **Roles** or **SSIDs** to filter the devices within the selected group(s) based on their roles or SSIDs.
  - **Roles**—Select a device from the list of roles for which you want to generate the report.
  - **SSIDs**—Select a device from the list of SSIDs for which you want to generate the report.
  - **Trends**—Select a trend or multiple trends from the list for which you want to generate the report. Select **All** to generate the report for all the available trends in the list. Allows you to generate the report to view the data for one year for trends such as **Unique clients per day**, **Clients per SSID**, **Unique client sessions per day**, **Average client sessions per day**, **Average clients per day**, and **Usage over time**.
  - **Top N Widgets**—Select a widget or multiple widgets from the list for which you want to generate the report. Select **All** to generate the report for all the available widgets in the list. Allows you to generate the report to view the data for one year for widgets such as **Top clients by usage**, **Top OS by usage**, **Top APs by usage**, **Bottom APs by usage**, **Top sites by WLAN usage**, and **Bottom sites by WLAN usage**.
  - **Audit Report**—Select **Show Overrides** to include the override data of the devices within the group in the **Configuration & Audit** report.
  - **Device Inventory**—Select **Offline** to include the details of the offline devices within the group in the **Infra Inventory** report.
  - **Threshold**—Select the **Same as AP threshold** check-box to set the same threshold as the AP. Allows you to set the percentage of the CPU and the memory thresholds for APs, switches, and gateways within the group.
  - **Criteria**—Select **Used/Unused Ports** and/or **PoE** to include the data regarding the used ports, unused ports, and/or PoE usage in the **Switch Capacity Planning** report. When you select **Used/Unused Ports**, the **Switch Port Summary** report is generated. When you select **PoE**, the **Switch PoE Usage Summary** report is generated. The individual port details are available only in the .csv export of the **Switch Port Summary** report.
  - **Subnet/SSID List**—Select **Subnet/SSID List** to generate the report based on the CDE SSIDs or CDE subnets.
  - **CDE SSIDs**—Select an SSID from the list for which you want to generate the report.
  - **CDE Subnets**—Select a subnet from the list for which you want to generate the report.
- **Label**—Allows you to generate the report for the devices attached to a label.
  - **Label**—Select a label or multiple labels from the list for which you want to generate the report. Select **All** to generate the report for all the available labels in the list. The search bar allows you to filter a label from the list.

- **Site**—Allows you to generate the report for the devices attached to a site.
  - **Site**—Select a site or multiple sites from the list for which you want to generate the report. Select **All** to generate the report for all the available sites in the list. The search bar allows you to filter a site from the list.
  - **Detailed Report**—Select **Show Detailed Report** to include the client session details for each client within the site in the **Client Session** report.

Transport Type

Select one of the available options from the following:

- **Overlay**—Select **Overlay** you to include the WAN overlay availability information in the report.
- **Underlay**—Select **Underlay** to include the WAN underlay availability information in the report.
- **Internet**—Select **Internet** to include details of WebCC over the internet in the report.
- **VPN**—Select **VPN** to include details of WebCC over the VPN tunnel in the report.

Report Order

Select either **Best Performing** or **Worst Performing** to include the details of the best or worst performing WAN interfaces in the report.

Top N Count

Enter the range in the **Top N** for the number of results you want the include in the report. The Top N range should be between 1 to 250.

Classify On

Select either **web category** or **web reputation** to include data about the total usage of each device based on the web reputation or web category in the report.

Report Subtype

Select either **summary report** or **blocked urls report** to include the summary or blocked urls details in the report. A blocked URLs report will contain blocked URL Information along with the number of attempted session count.

Report Period

Specify the time period for which you want to create the report. Select one of the available options from the following:

- **Last day**—Select **Last day** to generate the report for the last day.
- **Last 7 days**—Select **Last 7 days** to generate the report for the last 7 days.
- **Last 30 days**—Select **Last 30 days** to generate the report for the last 30 days.
- **Last year**—Select **Last year** to generate the Summary report for the last year.
- **Custom range**—Select **Custom range** to generate the report for a time period within the last 90 days. When you select **Custom range**, the **Date Range** option is displayed. In the **Date Range** window, select a time period within the last 90 days for which you want to create the report.

The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

Recurrence

Select **Recurrence** to schedule the report. Select one of the available options from the following:

- **One time (Now)**—Select **One time (Now)** to schedule the report generation once for the current time.
- **One time (Later)**—Select **One time (Later)** to schedule the report generation once for a later time. When you select **One time (Later)**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the date for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every day**—Select **Every day** to schedule the report generation for every day. When you select **Every day**, the **Run Time** option is displayed. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every week**—Select **Every week** to schedule the report generation for every week. When you select **Every week**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the day for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every month**—Select **Every month** to schedule the report generation for every month. When you select **Every week**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the date from the **Day** drop-down list for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.

Report Information

Allows you to add a title, an email address, and specify the format of report to receive the email. Enter the following information:

- **Report title**—Enter the title of the report.
- **Email to**—Enter an email address to receive the report over an email.
- **Email Format**—Select **PDF** and/or **CSV** to specify the format of the report to receive the email.

Creating a Report

Aruba Central allows you to generate a report for devices associated with a group, multi-group, label, or a site.

Although your page view is set to a specific group, site, or label, you can create reports for a different group, site, or a label. However, if your page view is set to an Instant Access Point (IAP) cluster or switch, you can schedule a report only for that IAP cluster or switch.

To create a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Create**.

   The **Reports** page is displayed.
4. Select the type of report you want to create and then click **Next**.

5. Based on the type of report you select, a few options are displayed. Select one of the available options to set the context of the report. For example, for the **Client Inventory** report, select one of the available options under **Context**, which is either **Groups**, **Labels**, or **Sites**.
   - **Groups**—Select **Groups** to generate reports for the devices attached to a group.
   - **Labels**—Select **Labels** to generate reports for the devices attached to a label.
   - **Sites**—Select **Sites** to generate reports for the devices attached to a site.

   Based on the selected context, further options are displayed to create a report with more details. For more information, see Report Configuration Options.
6. Click **Next**.

   The **Report Period** option is displayed.
7. Under **Report Period**, select one of the available options to create a report for the last day, last 7 days, last 30 days, last year, or for a custom range.

The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

8. Click **Next**.

   The **Recurrence** option is displayed.
9. Under **Recurrence**, select one of the available options to schedule a report for the current time, later time, every day, every week, or every month.
10. Under **Report Information**, enter the title of the report and an email address.
11. Select **PDF** and/or **CSV** to specify the format of the report to receive the email.
12. Click **Generate**.

    The report gets generated and is displayed under the **Scheduled Reports** table. The report gets emailed as an attachment to the email address provided.

Editing a Report

Aruba Central allows you to edit a report for devices associated with a group, multi-group, label, or a site.

To edit a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The Reports page is displayed in the **Summary** view.
3. Click **Manage**.

   The **Scheduled Reports** table is displayed in the **Config** view.
4. In the **Scheduled Reports** table, select a report and then click the edit icon.

   The report that you want to edit is auto-selected in the **Reports** page.
5. Click **Next**.
6. Based on the type of report you select, a few options are displayed. Select one of the available options to set the context of the report. For example, for the **Client Inventory** report, select one of the available options under **Context**, which is either **Groups**, **Labels**, or **Sites**.

- **Groups**—Select **Groups** to generate reports for the devices attached to a group.
- **Labels**—Select **Labels** to generate reports for the devices attached to a label.
- **Sites**—Select **Sites** to generate reports for the devices attached to a site.

Based on the selected context, further options are displayed to create a report with more details. For more information, see Report Configuration Options.

7. Click **Next**.

   The **Report Period** option is displayed.
8. Under **Report Period**, select one of the available options to create a report for the last day, last 7 days, last 30 days, last year, or for a custom range.

The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

9. Click **Next**.

   The **Recurrence** option is displayed.
10. Under **Recurrence**, select one of the available options to re-schedule a report for the current time, for a later time, every day, every week, or every month.
11. Under **Report Information**, edit the title of the report and an email address.
12. Select **PDF** and/or **CSV** to specify the format of the report to receive the email.
13. Click **Generate**.

    The report gets generated and is displayed under the **Scheduled Reports** table. The report gets emailed as an attachment to the email address provided.

Viewing the Generated Report

To view a generated report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The Reports page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.
4. In the **Generated Reports** table, click a report name listed under **Title**.

   The report details are displayed.

The **Generated Reports** table provides the following information:

- **Title**—Name of the report. Click ▽ to filter the report based on the name of the report.
- **Date Run**—Time when the report was last run.
- **Group/Device**—The group or device for which the report was run.
- **Label/Site**—The label or site for which the report was run.
- **Type**—Type of report. Click ▽ to filter the report based on the type of the report. Click › to select a type of report from the drop-down list.
- **Created By**—Email address of the user who created the report.

Viewing the Scheduled Report

To view a scheduled report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Manage**.

   The **Scheduled Reports** table is displayed in the **Config** view.
4. In the **Scheduled Reports** table, click a report name listed under **Title**.

   The report details are displayed.

The **Scheduled Reports** table provides the following information:

- **Title**—Name of the report. Click to filter the report based on the name of the report.
- **Next Run**—Time when the report will run in the future.
- **Group/Device**—The group or device for which the report was run.
- **Label/Site**—The label or site for which the report was run.
- **Recurrence**—Time period of the scheduled report.
- **Type**—Type of report. Click to filter the report based on the type of the report. Click to select a type of report from the drop-down list.
- **Created By**—Email address of the user who created the report.
- **Status**—Status of the report. Click to filter the report based on the status of the report. Click to select a status of report from the drop-down list.

Downloading a Report

To download a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.
4. In the **Generated Reports** table, hover over the report you want to download.
5. Click the **PDF** or the **CSV** icon to download the report to the local system.
6. Optionally, click the **Email to** icon to generate an email attachment of the report.

Deleting a Report

To delete a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.
4. In the **Generated Reports** table, hover over the report that you want to delete.
5. Click the **Delete** icon.

   The **Delete Report** pop-up window is displayed.
6. Click **Yes** to delete the report.

   The selected report is deleted.

Deleting Multiple Reports

To bulk delete multiple reports, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** Reports page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.
4. To bulk delete, select multiple reports by clicking the rows. Alternatively, press and hold the **Ctrl** key and select the reports.

   The number of selected reports is displayed in a pop-up window.
5. In the pop-up window, click the icon.

   The **Delete Report** pop-up window is displayed.
6. Click **Yes** to bulk delete the selected reports.

   The selected reports are deleted.

Chapter 29
Maintenance

The **Maintenance** application allows you to upgrade firmware and troubleshoot devices. See the following topics for more information:

- Updating Software Images on Aruba Gateways
- Troubleshooting Devices

Troubleshooting Devices

The **Troubleshooting** menu in the **Maintenance** module allows your network administrators to run troubleshooting or diagnostics commands on the devices managed from Aruba Central. When a troubleshooting operation is initiated, Aruba Central establishes a session with the devices, retrieves the output of the commands, and displays the output in the UI.

Aruba Central supports running troubleshooting operations on one or several devices. You can select up to 10 devices for a troubleshooting operation. If the user access is restricted to certain groups within a network, Aruba Central allows running troubleshooting commands only for the devices provisioned in the allowed groups.

For more information on troubleshooting, see *Troubleshooting Devices* in the *Aruba Central Help Center*.

Gateway Diagnostic Tests

Aruba Central provides troubleshooting utilities to test SD-WAN overlay network connections. Users experiencing device connectivity issues at the branch site at a specific location, can select the device and specify an IP address to test the network connectivity. SD-WAN diagnostic tests allow users to view the routing path and forwarding rules that are used to forward or drop packets in an SD-WAN orchestrated network.

Diagnostic tests identify the routing or forwarding issues in the overlay network path, if any. Following are two types of diagnostic tests:

- **Control plane** test
- **Data plane** test

SD-WAN diagnostic tests do not trace underlay routing network paths.

The minimum firmware version required for performing SD-WAN diagnostic tests is ArubaOS 8.5.0.0-2.1.0.0.

This section includes the following topics:

- Control Plane
- Data Plane
- Node-Specific Error Messages
- Asymmetric Routing

- Routing Loop
- Error Notifications

Control Plane

The control plane builds and maintains the network topology and makes decisions on the traffic flow in an SD-WAN network. Control plane tracing is based on the active routing table entries.

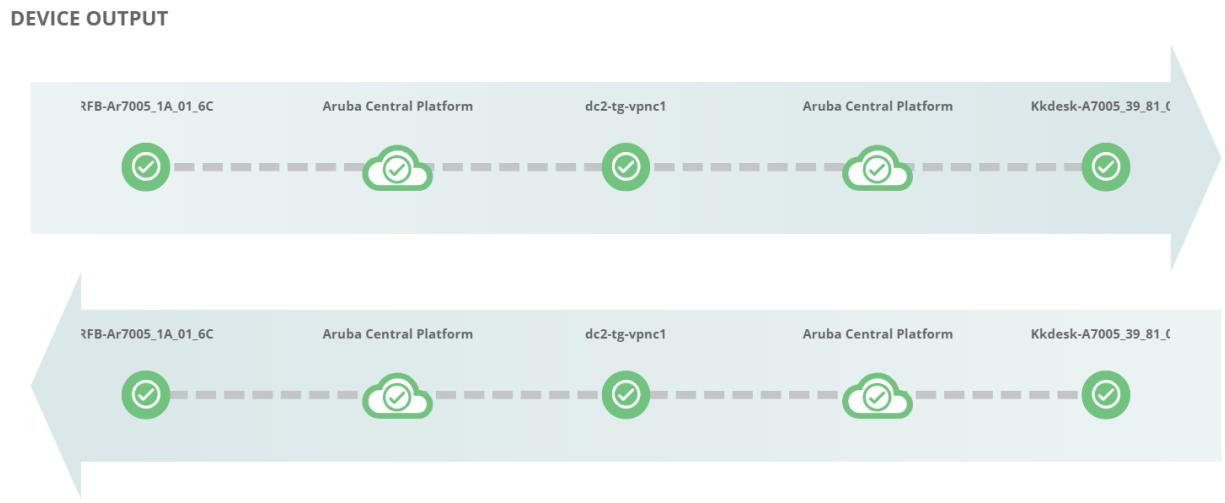
In the **Control plane** test, the diagnostic framework traces all the nodes and the forward route details in the orchestrated path from the selected gateway to the destination IP. It also traces all the nodes and the forward route detail in the reverse path, from the last gateway in the overlay path to the source IP. The last gateway in the path tracing output is the gateway in which the packet gets routed through the underlay routes, but not through the tunnels.

To perform a **Control plane** test, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.The dashboard context for the selected filter is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Diagnostics**.
5. From the **Diagnostic Type** drop-down list, select **Control plane**.
6. From the **Sources** drop-down list, select the source.
7. In the **Source IP Address** field, enter the IP address for which you want to perform the test.
8. In the **Destination IP Address** field, enter the IP address for which you want to perform the test.
9. Click **Run**.

The output is displayed in the **Device Output** section.

Figure 369 *Control Plane—Device Output*



Control Plane—Node Details

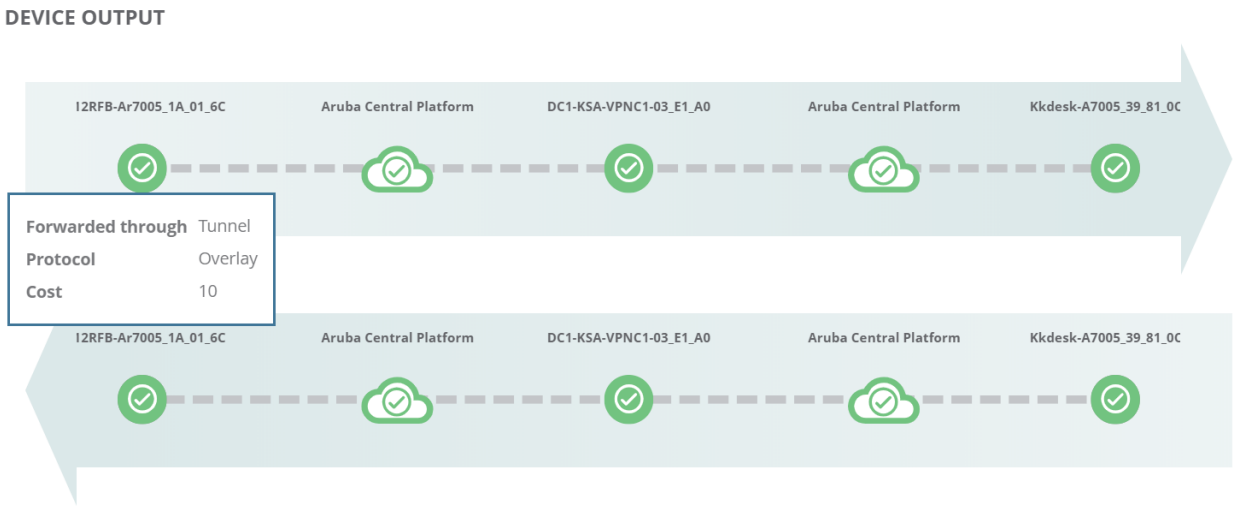
When you click on a node, a pop-up displays information that allows the user to analyze the data at every node in the forward and reverse path.

Gateway and VPNC—Node Details

When you click a Gateway node or a VPNC node in a forward or reverse path, the pop-up displays the following information:

- **Forwarded through**—Displays the name of the network path.
- **Protocol**—Displays the type of protocol.
- **Cost**—Displays the metric value of the path cost.

Figure 370 *Gateway and VPNC—Node Details*

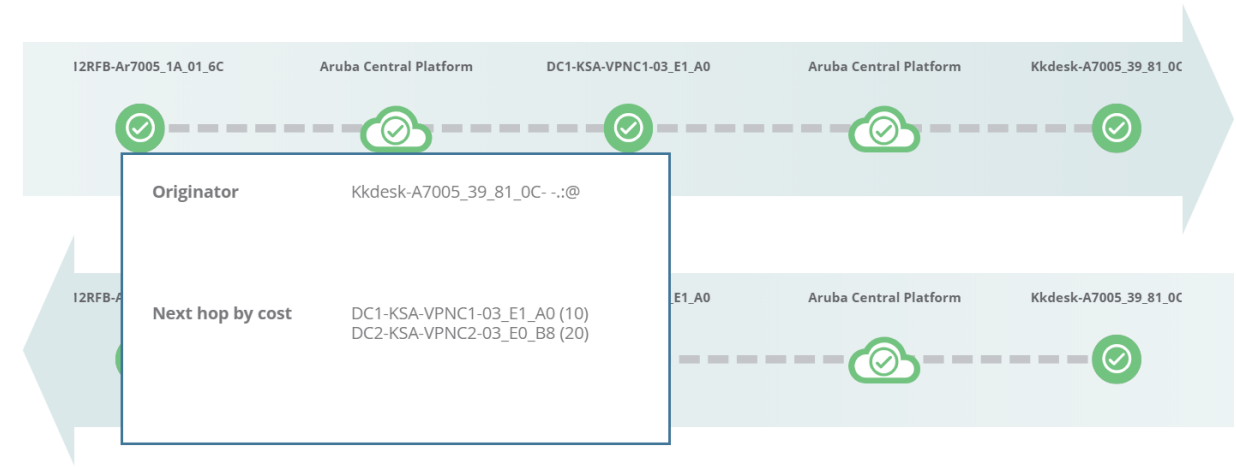


Aruba Central Platform—Node Details

When you click an Aruba Central Platform node in a forward or reverse path, the pop-up displays the following information:

- **Originator**—Displays the name of the devices which originated the particular route prefix in the overlay topology. It is the destination IP for the forward path and the source IP for the reverse path.
- **Next hop by cost**—Displays the list of next hops in an order of increasing value of cost.

Figure 371 *Aruba Central Platform—Node Details*



Data Plane

The data plane is responsible for forwarding the packets based on the decisions from the control plane in an SD-WAN network. Data plane tracing is based on the current datapath session table entries. Data path sessions are created when traffic flows through the gateways. When the data traffic flow stops, data path sessions are cleared after the age-out interval of the session. The test output is valid when you execute the test within the age-out interval of the data path session, and there are data path session entries in the gateway matching your input for the diagnostics test.

For most effective data plane test results, live traffic flow must be available matching your input for the diagnostics test.

In the **Data plane** test, the diagnostic framework traces all the nodes and the datapath session status for the selected flow in the overlay path from the selected gateway to the destination IP or port. It also traces all the nodes and the datapath session status for the reverse traffic from the last gateway in the overlay path to the source IP. The last gateway in the data plane tracing output is the gateway in which the packet gets routed through the underlay routes or gets dropped because of the configured firewall rules, but not through the tunnels.

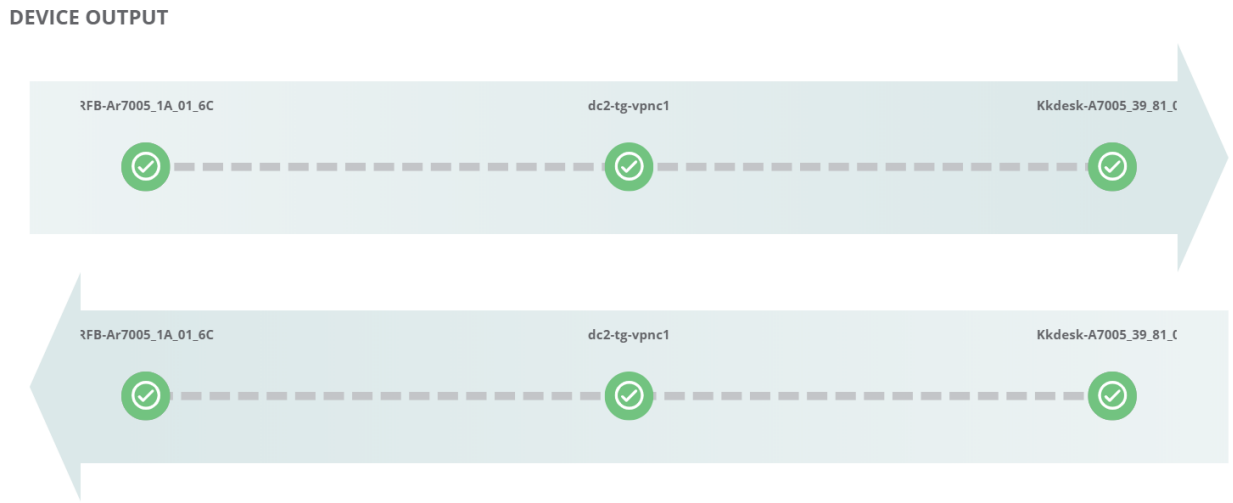
To perform a **Data plane** test, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Diagnostics**.
5. From the **Diagnostic Type** drop-down list, select **Data plane**.
6. From the **Protocol** drop-down list, select the protocol. The protocols supported are **ICMP**, **IGMP**, **IPv4_ENCAP**, **TCP**, **UDP**, **IPv6_ENCAP**, **RSVP**, **GRE**, **IPSEC_ESP**, **IPSEC_AH**, and **L2TP**.
7. From the **Sources** drop-down list, select the source.
8. In the **Source IP Address** field, enter the IP address for which you want to perform the test.
9. In the **Port** field, enter the port number.
10. In the **Destination IP Address** field, enter the IP address for which you want to perform the test.
11. In the **Port** field, enter the port number.
12. Click **Run**.

The output is displayed in the **Device Output** section.

In the **Data plane** test, the **Port** fields are optional. When you select the **ICMP** protocol, the **Port** fields are disabled.

Figure 372 *Data Plane—Device Output*



Data Plane—Node Details

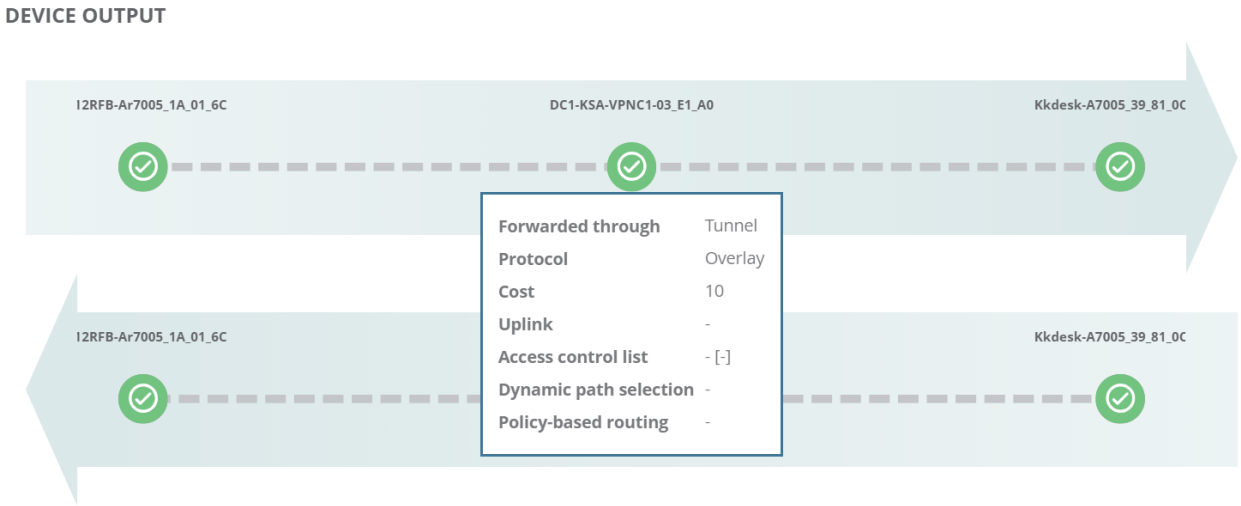
When you click on a node, a pop-up displays information that allows the user to analyze the data at every node in the forward and reverse path.

Gateway and VPNC—Node Details

When you click a Gateway node or a VPNC node in a forward or reverse path, the pop-up displays the following information:

- **Forwarded through**—Displays the name of the network path.
- **Protocol**—Displays the type of protocol.
- **Cost**—Displays the metric value of the path cost.
- **Uplink**—Displays the name of the uplink.
- **Access control list**—Displays the firewall ACL/ACE rules applied for the session.
- **Dynamic path selection**—Displays the SD-WAN DPS policy applied for the session.
- **Policy-based routing**—Displays the PBR policy applied for the session.
- **Error description**—Displays the error message associated with a specific error.

Figure 373 *Gateway and VPNC—Node Details*



Node-Specific Error Messages

In the diagnostic tests, when an error occurs, the **Error description** parameter appears in the pop-up of that specific node. The icon for that specific node changes to an error icon.

The following are few error messages:

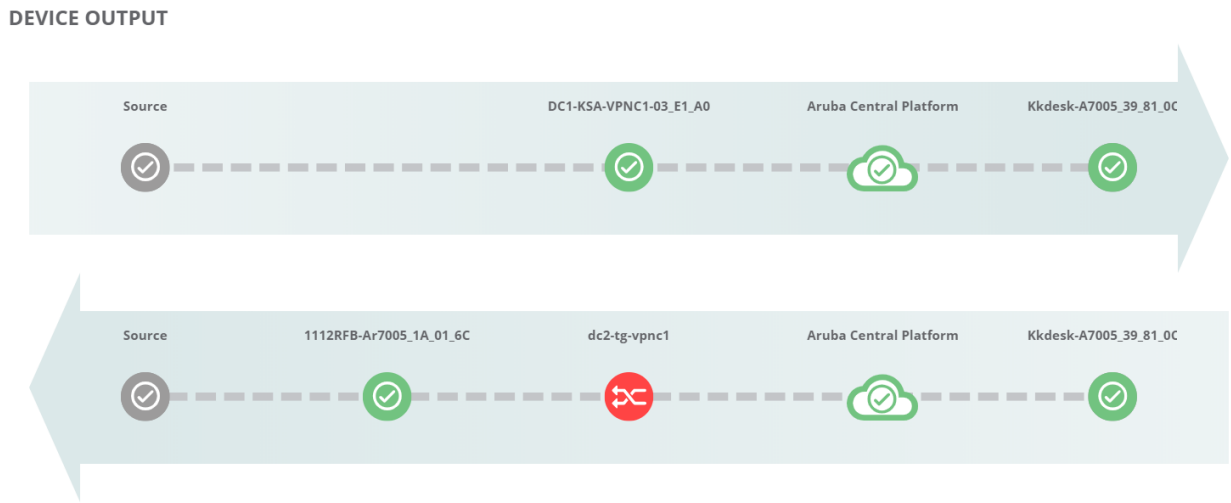
- **Session not found**—Error message states that the device does not have any session entry for the specified parameters, such as source IP, destination IP, protocol, source port, or destination port, and the packet flow did not reach the device.
- **ACL denied**—Error message states that the session has hit a firewall ACL/ACE deny rule and the packets are dropped by the device.
- **Reverse packet not seen**—Error message states that the device has forwarded the packets to the next hop in the forward direction but is yet to receive any packets from that next hop device.
- **Connection test stopped here due to incompatible device firmware**—Error message states that the device firmware is incompatible to run the diagnostic tests.

Asymmetric Routing

Asymmetric routing occurs when the forward traffic traverses from a source to a destination in one path but the reverse traffic follows a different path from the destination to source. For example, forward traffic from Branch B1 traverses via VPNC A and the reverse traffic traverses via VPNC A to reach Branch B1. Asymmetric path is when the reverse traffic traverses via VPNC B to reach Branch B1.

The diagnostic tests detect asymmetric routing in a control plane path and data plane path.

Figure 374 *Asymmetric Routing*



Routing Loop

Routing Loop is a network failure in which the traffic is continuously routed back and forth between two hops rather than reaching the destination host.

The diagnostic tests detect routing loop issues in a control plane path and data plane path.

Error Notifications

The following are a few error notifications:

- **Diagnostics test has timed out**—Error message states that the diagnostic test is not completed within the expected delay of 60 seconds. The reason for the time out can be one of the following:
  - The back-end is still querying a gateway.
  - The device fails to answer for a reason.
  - Occurs even after partial path data is collected and displayed.
- **Diagnostics test request cannot be fulfilled**—Error message states that the diagnostic test request is not fulfilled. The reason for the failure of the request can be because invalid parameters are entered in the diagnostic test request or while querying for the diagnostic test result.
- **Diagnostics test is unavailable**—Error message states that the test cannot be completed and indicates that the back-end or the source gateway is down.
- **Diagnostics test has failed**—Default error message to indicate errors other than mentioned above.

Figure 375 *Error Message*

Updating Software Images on Aruba Gateways

Aruba Central supports various versions of SD-WAN software images on the Aruba Gateways provisioned in your account. Using the Aruba Central management interface, you can also update software images on Gateways. The **Firmware** page in the Aruba Central also shows the recommended software versions for each device.

Feature Availability Across Multiple Software Versions

Aruba Central supports provisioning Gateways running different versions of SD-WAN software images. Although some features introduced in later software versions can be configured at the group level, the devices running lower software versions do not inherit these configuration changes.

To alert users about the feature availability, Aruba Central shows per-field caution indicators when you try to configure a feature on a device that is running an older software version. The caution text also displays the minimum software version that supports the feature.

If a software version of a device does not support any particular feature or function, Aruba Central does not allow you to enable, disable, or modify values for that feature on the device.

To view the feature availability indicator for a group that includes a device with a lower software version, complete the following steps:

1. After selecting the group from the filter, navigate to **Devices**.
2. Click the **Config** icon to open the Branch Gateway group configuration page.
3. In the **Advanced mode**, go to **VPN** > **DPD** to view the feature availability indicator for a group that includes a device with a lower software version.

Upgrading Software

Aruba recommends that you upgrade your devices periodically to the recommended software version. Aruba Central also allows you to schedule a compliance check and thus ensure that compatibility between devices provisioned in a group.

For information on how to upgrade software images on Aruba Gateways, see the *Managing Software Upgrades* topic in *Aruba Central Help Center*.

Chapter 30
APIs

Aruba Central supports an Application Programming Interface (APIs) to allow the administrator users to create and manage APIs. It supports the following types of APIs:

- A polling-based API—The Representational State Transfer (REST)-based APIs support HTTP GET operations by providing a specific URL for each query. The output for these operations are returned in the JSON format.
- Push or Event APIs—The Push API gives web applications the ability to receive messages pushed to them from a server.

  The API Gateway feature in Aruba Central offers the following benefits:
- Provides an API management gateway to create, publish, mange the life cycle of APIs
- Provides a gateway that can run on public and private cloud as containers
- Displays the API usage pattern
- Provides a developer portal to develop applications using the APIs

For more information on API Gateway, supported APIs, and the OAuth token generation procedure, see API Gateway in *Aruba Central Help Center*.

Chapter 31
Updating Software Images on Aruba Gateways

Aruba Central supports various versions of SD-WAN software images on the Aruba Gateways provisioned in your account. Using the Aruba Central management interface, you can also update software images on Gateways. The **Firmware** page in the Aruba Central also shows the recommended software versions for each device.

Feature Availability Across Multiple Software Versions

Aruba Central supports provisioning Gateways running different versions of SD-WAN software images. Although some features introduced in later software versions can be configured at the group level, the devices running lower software versions do not inherit these configuration changes.

To alert users about the feature availability, Aruba Central shows per-field caution indicators when you try to configure a feature on a device that is running an older software version. The caution text also displays the minimum software version that supports the feature.

If a software version of a device does not support any particular feature or function, Aruba Central does not allow you to enable, disable, or modify values for that feature on the device.

To view the feature availability indicator for a group that includes a device with a lower software version, complete the following steps:

1. After selecting the group from the filter, navigate to **Devices**.
2. Click the **Config** icon to open the Branch Gateway group configuration page.
3. In the **Advanced mode**, go to **VPN** > **DPD** to view the feature availability indicator for a group that includes a device with a lower software version.

Upgrading Software

Aruba recommends that you upgrade your devices periodically to the recommended software version. Aruba Central also allows you to schedule a compliance check and thus ensure that compatibility between devices provisioned in a group.

For information on how to upgrade software images on Aruba Gateways, see the *Managing Software Upgrades* topic in *Aruba Central Help Center*.

Chapter 32
Deploying Aruba Virtual Gateways

The Aruba SD-Branch solution supports deploying a hardware VPNC as headend gateway in the customer's data center or a virtualized instance of a headend gateway in customer's public cloud infrastructure. The virtualized instance of Aruba Gateway is referred to as Virtual Gateway.

Virtual Gateways allow customers to bring their public cloud infrastructure to the SD-WAN fabric and facilitate connectivity between branches and the public cloud.

The inclusion of Virtual Gateways in the Aruba SD-WAN architecture offers the following benefits:

- Ability to directly connect a branch to cloud instances and thereby improving access to the instances hosted on a public cloud infrastructure.
- Resilient connectivity from the cloud by utilizing multiple transport links; for example, the link between an Internet Gateway and Virtual Gateway.
- Centralized control and policy management across branch, data center and cloud end-points.

To enable Virtual Gateway support on your SD-Branch, please contact your Aruba Sales Specialist.

Features Supported by Virtual Gateway

With Virtual Gateway, users can extend their SD-WAN overlay services to the public cloud infrastructure. Virtual Gateways function as VPNCs in the SD-WAN architecture. Virtual Gateways can terminate tunnels from Branch Gateway, Instant APs (micro SD-Branches with Instant APs) and VIA clients. Like the on-premises VPNCs, Virtual Gateways support routing, security, and tunneling features.

Virtual Gateway Redundancy

Aruba supports deploying Virtual Gateways for high availability (HA). The Virtual Gateways can be deployed in the HA mode and also can be deployed in multiple availability zones.

Software Image for Virtual Gateways

The software image required for creating Virtual Gateway instances are available as an AMI. To obtain the AMI for a Virtual Gateway, contact your Aruba Sales Specialist.

This section includes the following topics:

Deploying Aruba Virtual Gateways in AWS

Virtual Gateways simplify branch network deployments for organizations intending to migrate their infrastructure to cloud providers such as Amazon.

Aruba supports instantiating Virtual Gateways on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) virtualized environment. Network administrators can deploy an AWS EC2 instance with enhanced networking option that uses single root I/O virtualization (SR-IOV)-enabled Ethernet Network Interface Card (NIC).

The AWS EC2 instance is created from OS images in Amazon Machine Image (AMI) format. The ArubaOS VMC image is used for creating and registering the Virtual Gateway AMI. To obtain the AMI for Virtual Gateway, contact your Aruba sales representative.

Aruba Central supports deploying and managing Virtual Gateways hosted on the Amazon AWS VPCs using one of the following methods:

- Managed mode—In the managed mode, Aruba Central allows administrators to deploy Virtual Gateways using the orchestrator application in Aruba Central. The Virtual Gateway orchestrator in Aruba Central imports VPCs from an AWS account, deploys, connects, and allows you to manage Virtual Gateways from Aruba Central. For step-by-step instructions on deploying Virtual Gateways in the managed mode, see Deploying Aruba Virtual Gateways in AWS (Managed Mode).
- Unmanaged mode—In the unmanaged mode, Virtual Gateways must be manually deployed and launched from the cloud provider console. Aruba Central allows you to generate user data for such deployments and manage Virtual Gateways from Aruba Central. For step-by-step instructions on deploying Virtual Gateway in unmanaged mode, see Deploying Aruba Virtual Gateways in AWS (Unmanaged Mode).

Virtual Gateway Sizing

The Aruba Virtual Gateway requires the use of a supported AWS instance with a minimum of 500 Mbps of throughput and can support up to 1600 IPSec tunnels. This table lists out the supported AWS instances for each Aruba Model/SKU:

Aruba Model/SKU Name	Throughput	Supported AWS Instance	vCPU	Flash Memory (GB)	Tunnels
VGW-500MB	500 Mbps	c4.xlarge	4	15	1600
		c4.2xlarge	8	30	
		c4.4xlarge	16	60	
VGW-2GB	2 Gbps	c4.2xlarge	8	30	4096
		c4.4xlarge	16	60	
VGW-4GB	4 Gbps	c4.4xlarge	16	60	8192

If a higher number of tunnels are required, please contact your Aruba Sales Specialist.

Deployment Procedure

See the following topics for step-by-step instructions on how to deploy an Aruba Virtual Gateway in AWS VPC:

- Deploying Aruba Virtual Gateways in AWS (Managed Mode)
- Deploying Aruba Virtual Gateways in AWS (Unmanaged Mode)

Additional References

For a detailed description of SD-WAN integration with AWS and Virtual Gateway deployment in AWS, see the Aruba SD-WAN Integration with Public Cloud (AWS) Technical Note.

Deploying Aruba Virtual Gateways in AWS (Managed Mode)

Aruba Central supports deploying Virtual Gateways in managed and unmanaged modes. For managed-mode deployments, Aruba Central supports the orchestration service for automating Virtual Gateway deployments. The orchestrator application in Aruba Central enables IT administrators bring up, configure, and monitor Virtual Gateways from the Aruba Central management interface.

The orchestrator application performs the following key functions:

- Instantiation of Virtual Gateways—The orchestrator service allows you to integrate an Aruba Central account with a cloud provider account. This integration enables Aruba Central to automatically discover VPCs across multiple regions and their subnets, deploy, and connect Virtual Gateways from Aruba Central.

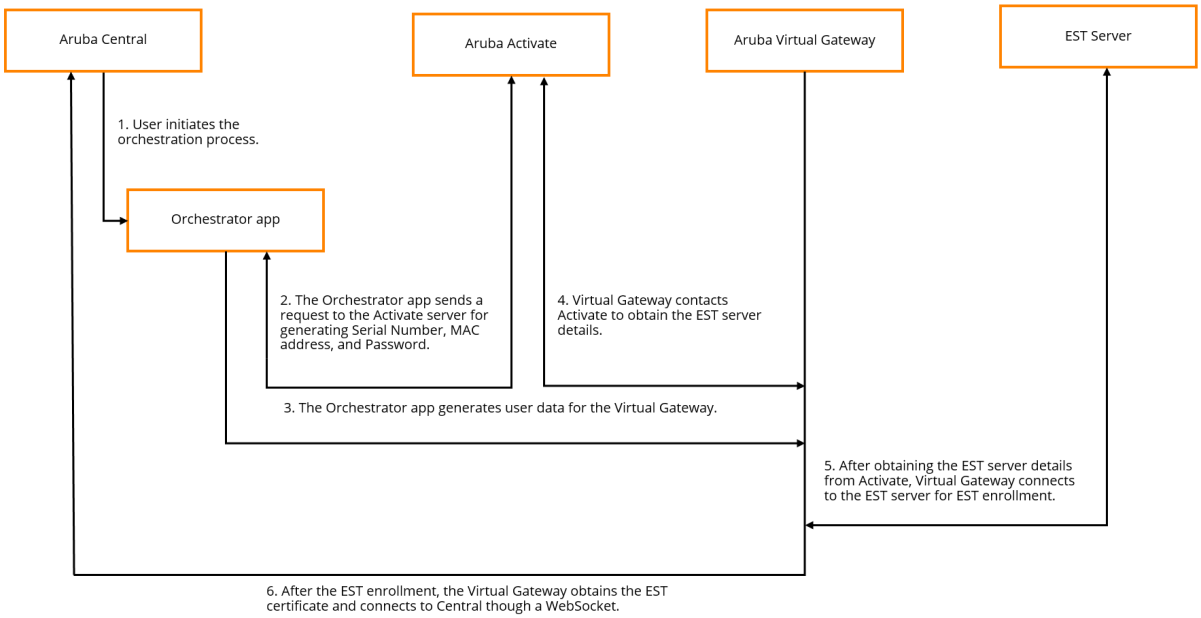
  The orchestrator application also generates an 8-digit serial number for Virtual Gateway before instantiation and creates elastic network interface with a static MAC address that is mapped to Gigabit Ethernet0/0/0. It also creates an Elastic IP (static public IP) and attaches it to the network interface.

- Device Registration—The orchestrator app registers Virtual Gateways in the customer's inventory in Activate database and allowlists the devices for management service from Aruba Central.
- Certificate Enrollment—The orchestrator app generates user data for Virtual Gateways, using which the Virtual Gateways obtain EST certificate to connect to Aruba Central using a WebSocket.

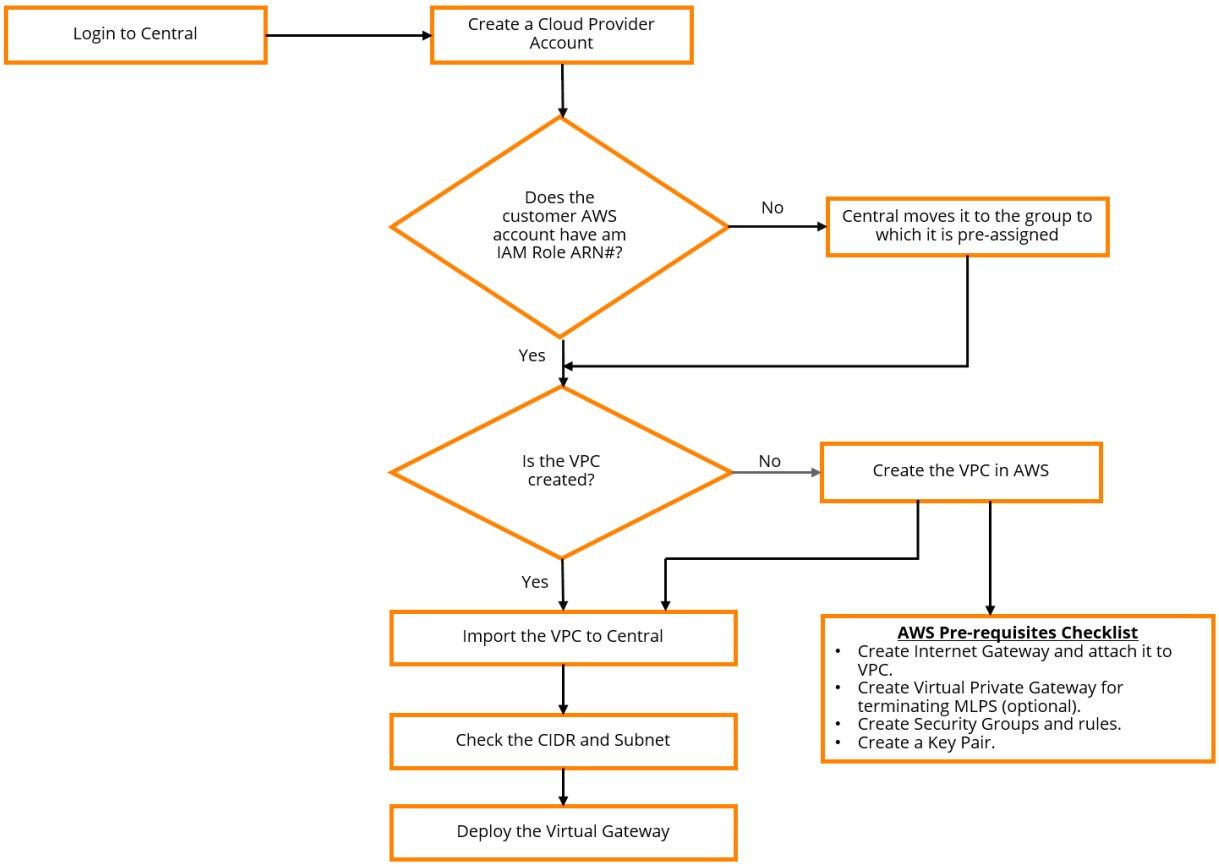
Orchestration Workflow

The following figure illustrates the orchestration workflow for Virtual Gateways:

Figure 376 *Orchestration Workflow*



The following flowchart illustrates the steps required for instantiating Virtual Gateway using the orchestrator app.



Setting up a Virtual Gateway Instance using the Orchestration Service

It is recommended that the resources used in these configurations are not reused or shared.

To instantiate Virtual Gateways using the orchestrator application, complete the following steps:

- Creating a VPC
- Configuring an Internet Gateway for the VPC
- Creating a Security Group
- Configuring a Key Pair
- Creating a Cloud Provider Account in Aruba Central
- Creating a Role ARN
- Deploying Virtual Gateways from Aruba Central
- Verifying the Aruba VGW deployment on AWS

Creating a VPC

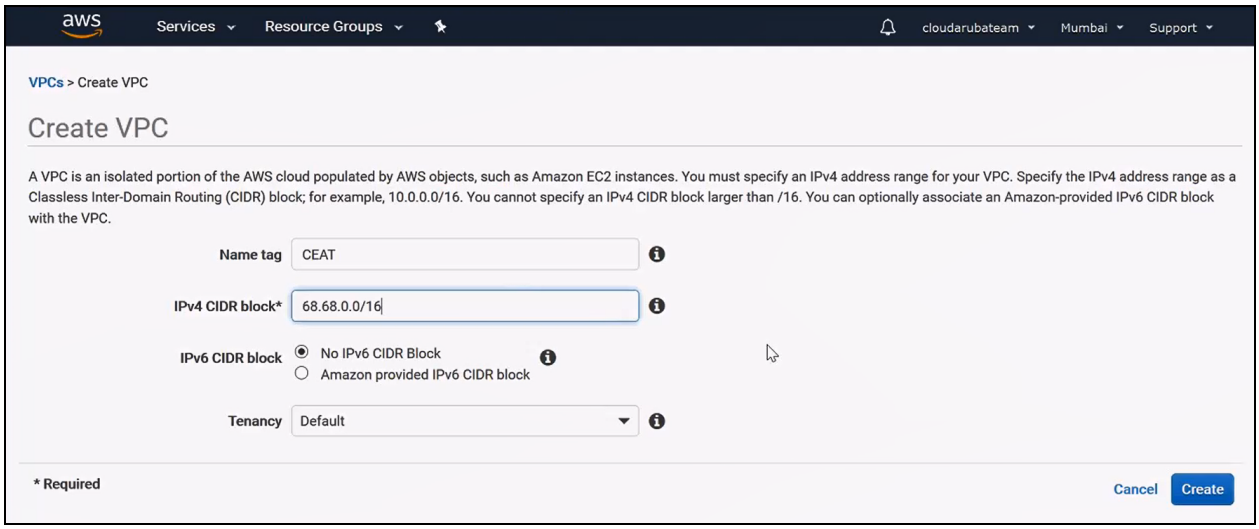
A VPC is a dedicated virtual data center in AWS. You can launch your AWS resources, such as AWS EC2 instances, into your VPC. The VPCs also provide granular cloud security by allowing you to provision a logically isolated section of AWS with your own IP addresses.

NOTE

A single VPC supports a single Virtual Gateway deployment. Ensure that the VPC is not shared between different accounts.

To create a VPC, complete the following steps:

1. Log in to AWS console.
2. Select the region in which you want to deploy the VPC.
3. Go to the AWS VPC Dashboard and create a VPC. You can also create a VPC using the **VPC Wizard**.
4. Enter a name for the VPC.
5. Specify an IPv4 CIDR block.
6. Click **Create**.

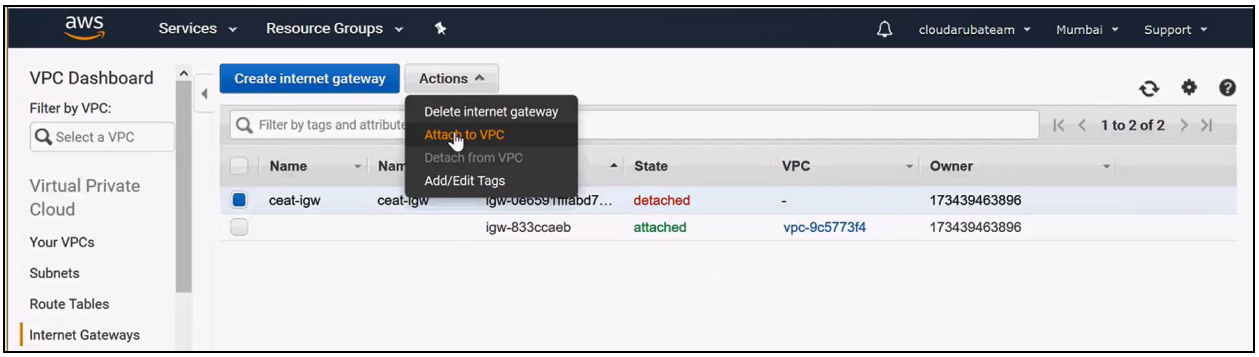


Configuring an Internet Gateway for the VPC

To create an Internet Gateway, complete the following steps:

1. On the AWS VPC console, click **Internet Gateway**.
2. Click **Create Internet Gateway** and create an Internet Gateway.

3. To attach the Internet Gateway to the VPC, click **Actions** > **Attach to VPC**. The Internet Gateway allows communication between the instances in your VPC and the Internet.



NOTE

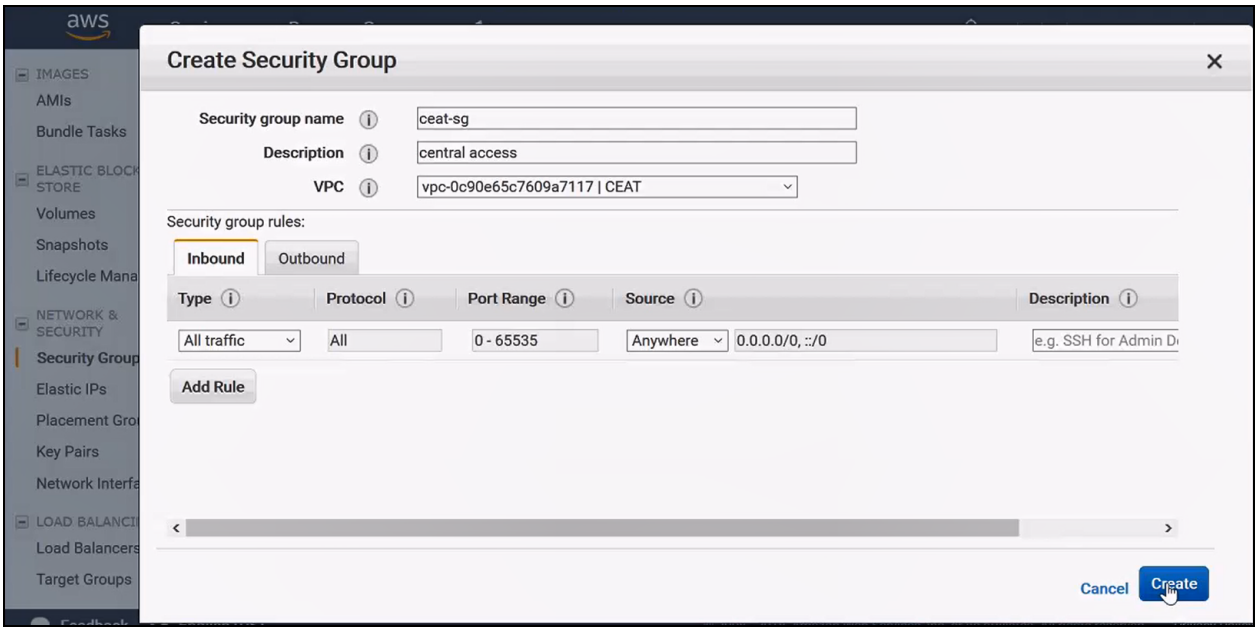
To terminate MPLS connections, you can also create Virtual Private Gateway and attach it to the VPC.

Creating a Security Group

A security group controls traffic for instances to which it is associated. Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.

To create a security group, complete the following steps:

1. Go to the AWS EC2 Console.
2. Select the region in which the VPC is deployed.
3. In the AWS Dashboard, select the EC2 tab and click on **Security Groups** under **NETWORKING & SECURITY**.
4. Enter a name for the group.
5. Select the VPC.
6. Add inbound and outbound rules. Ensure that the UDP 4500, TCP 443 and other ports required for device communication over a network firewall are open.
7. Click **Create**.

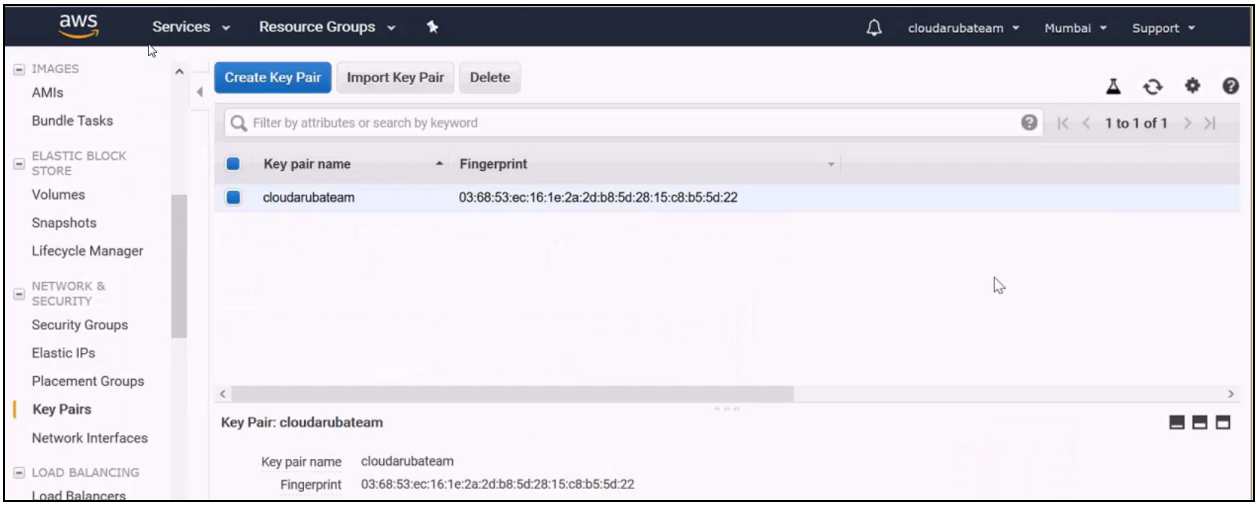


Configuring a Key Pair

By default, the Linux instances do not have a password set. To secure your login information for your instance, you can create a key pair. You can also use the key for logging in to the Virtual Gateway instance using SSH.

To configure a key pair, complete the following steps:

1. In the AWS Dashboard, select the EC2 tab and click on **Key Pairs** under **NETWORKING & SECURITY**.
2. Import an existing key pair or create a new one.



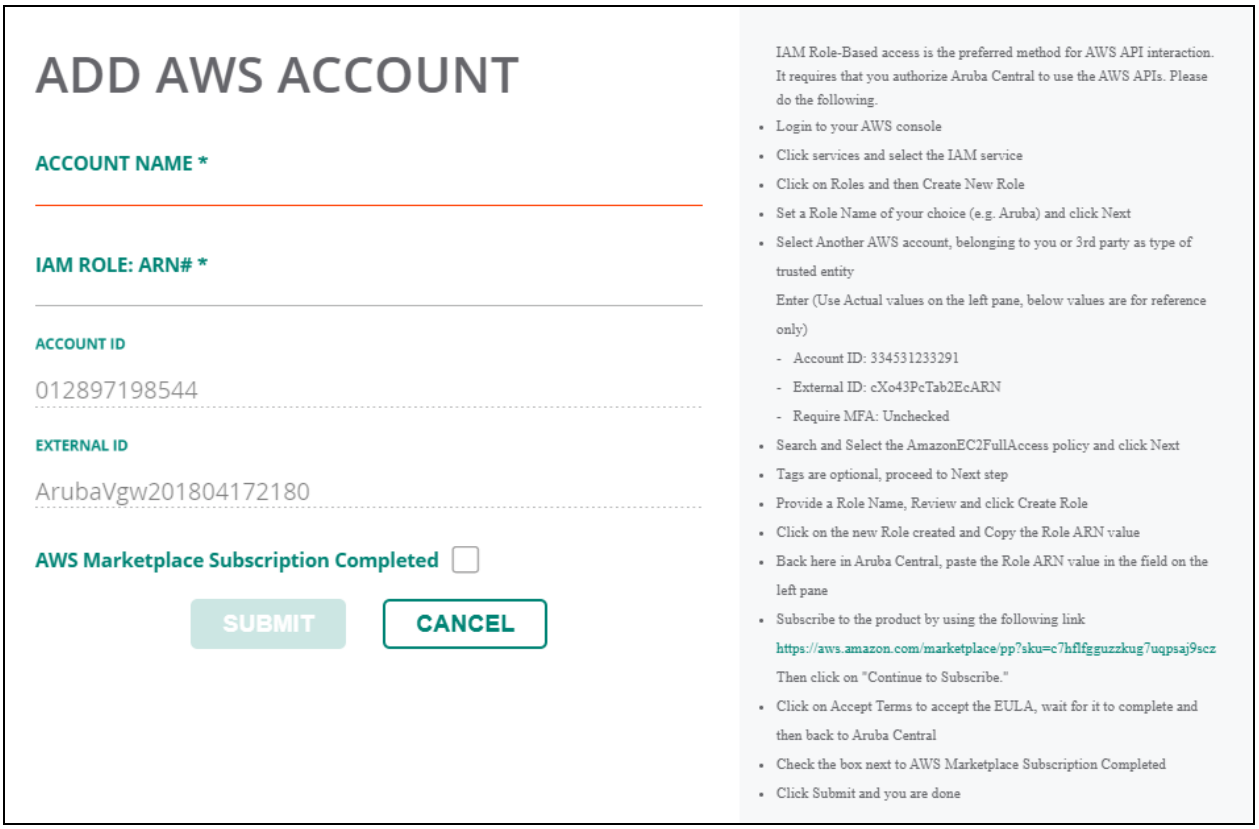
Creating a Cloud Provider Account in Aruba Central

To deploy Virtual Gateway instances in a customer's VPC, you must create a cloud provider account in Aruba Central and map it to the IAM Role ARN of the customer's AWS account in which the VPC is deployed.

1. Log in to Aruba Central.
2. In the **Network Operations** app, set the filter to **Global**.
3. Go to **Manage** > **Network Services** > **Virtual Gateways** > **Orchestrated**, to view the summary page for orchestrated Virtual Gateways with following columns:
   - **Cloud Provider**—Displays the name of the Cloud Provider.
   - **Account**—Displays the account name of the deployed Virtual Gateway.
   - **Region**—Displays the name of the location where the Virtual Gateway is deployed.
   - **VGW Serial**—Displays the serial number of the Virtual Gateway.
   - **VGW Public IP**—Displays the public IP address of the Virtual Gateway.
   - **High Availability**—Displays the High Availability mode (Active or Passive) of the Virtual Gateway.
   - **Orchestration**—Displays the status of the Virtual Gateway orchestration.
   - **VM Status**—Displays the status (Up, Down, or Stopped) of the Virtual Machine.
   - **VGW Status**—Displays the status of the deployed Virtual Gateway.
4. Click the **Config** icon. The configuration page is displayed.
5. To add an account, click **Accounts**, and select **AWS** from the available options and click **Add Account**.
6. In the **Add AWS Account** pop-up window, enter an **Account Name** and your **IAM Role ARN#**.
7. Retain the details that are populated in the **Account ID** and **External ID** fields.

8. **AWS Marketplace Subscription Completed**—Enable this option after subscribing to AWS Marketplace Subscription in AWS console.

   Aruba Virtual Gateway is available in the AWS Marketplace as a limited or private listing to host images. Clicking on the listing deploys the hosted image using Virtual Gateway orchestration.

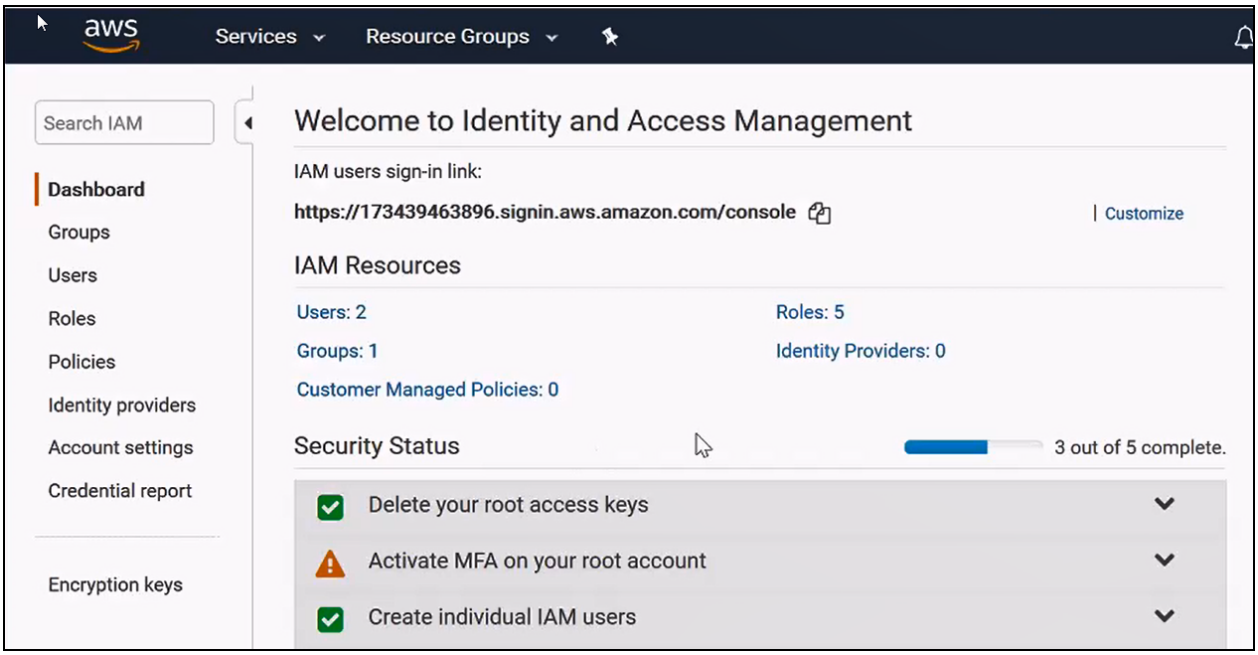


9. Click **Submit**. The account is added to list of accounts on the **Accounts** page.
10. Verify the status of the account. If the status column for the account is shown **Access Verified**, proceed to deploy the Virtual Gateway instance.

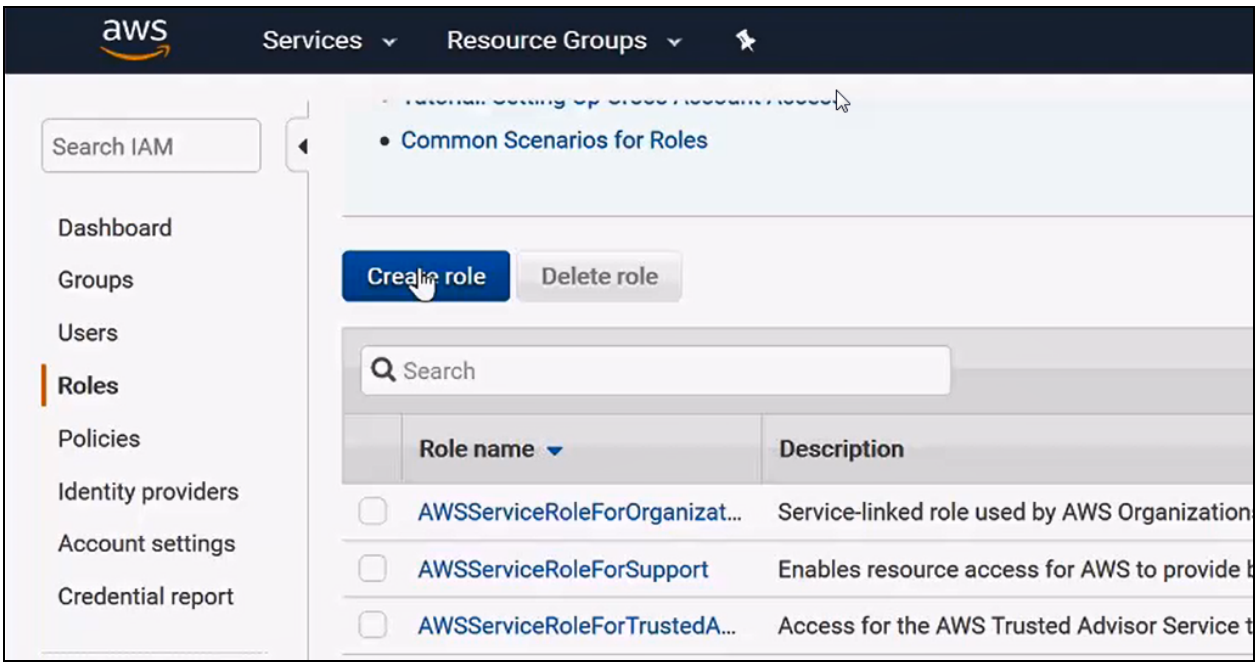
Creating a Role ARN

Ensure that you have the **IAM Role ARN** of the customer's AWS account for which you want to deploy the Virtual Gateway. If the **IAM Role** is not created, complete the following steps:

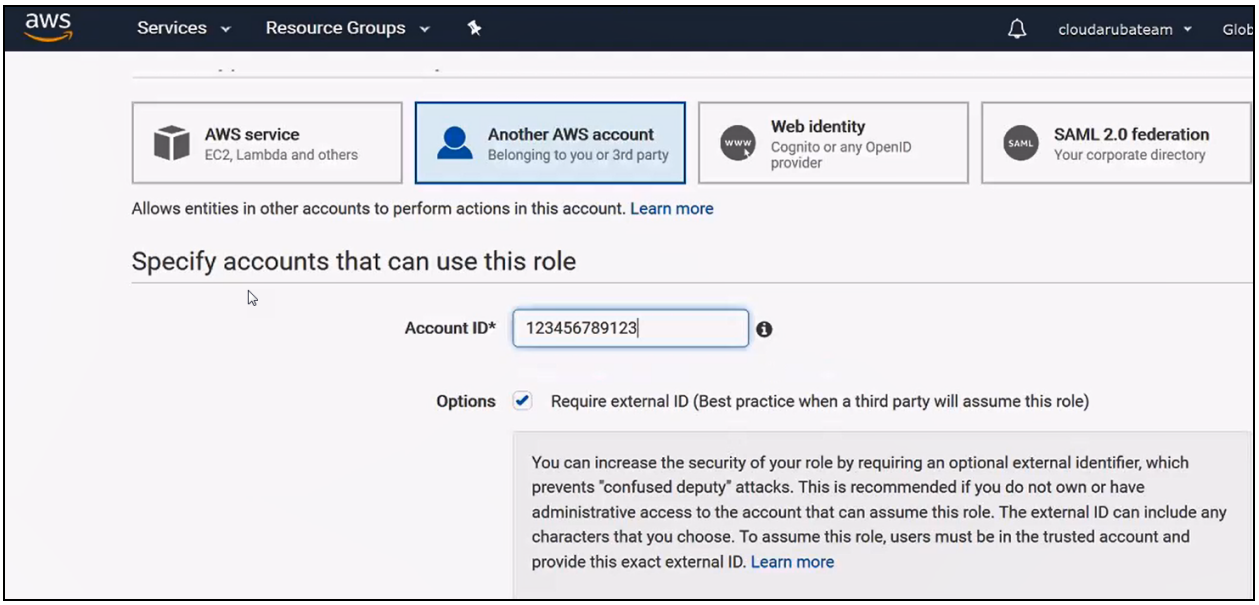
1. Log in the AWS account in which the VPC instance must be deployed.
2. Click **Services**.
3. Select the IAM service.



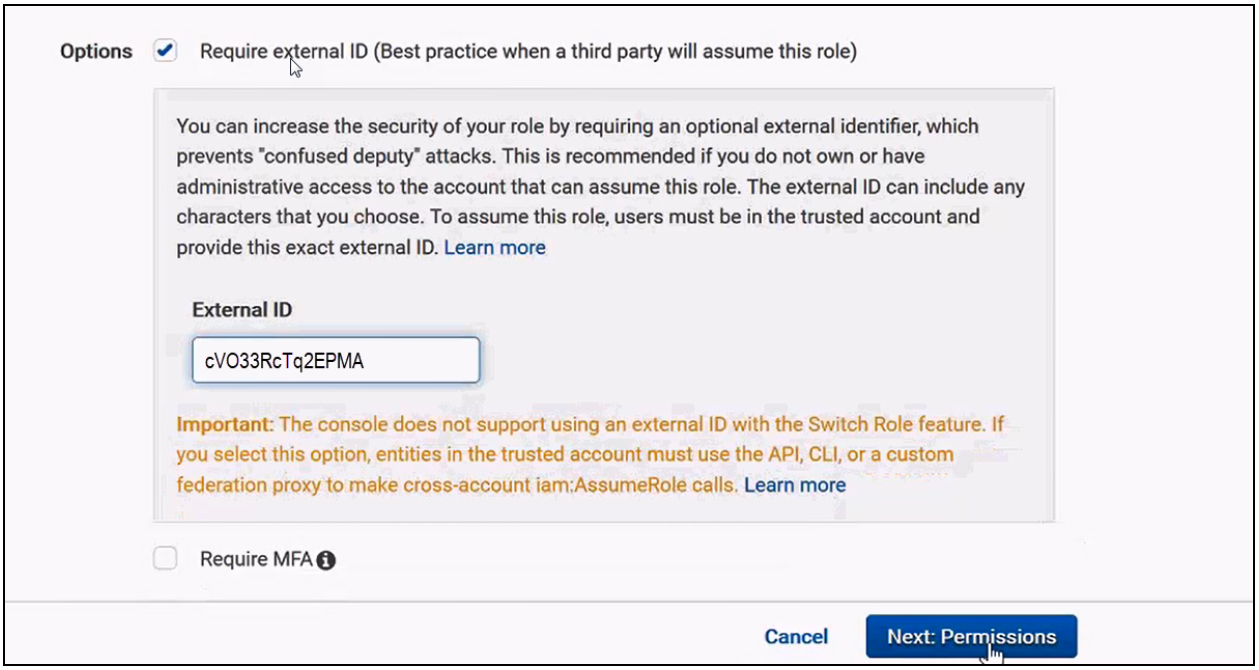
4. To create a new role, click **Roles** > **Create a New Role**.



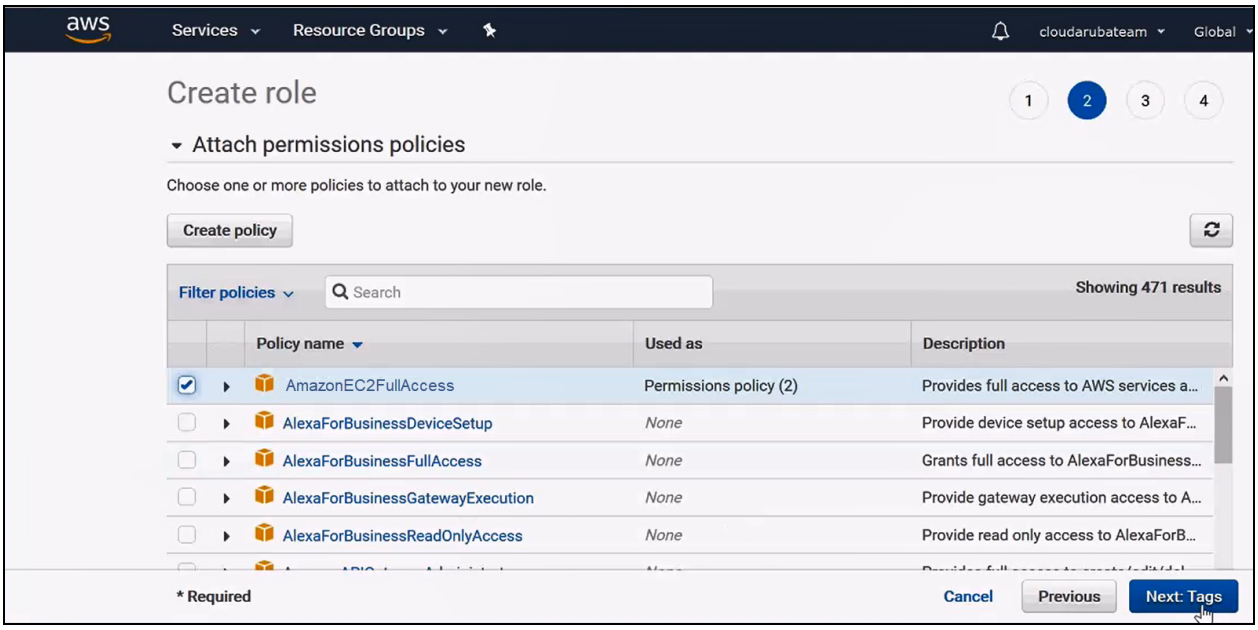
5. Enter a name for the role.
6. Click **Next**.
7. Select **Another AWS Account Belonging to you or a 3rd party**.
8. Enter your **Account ID**.
9. Select the **Require External ID** check box.



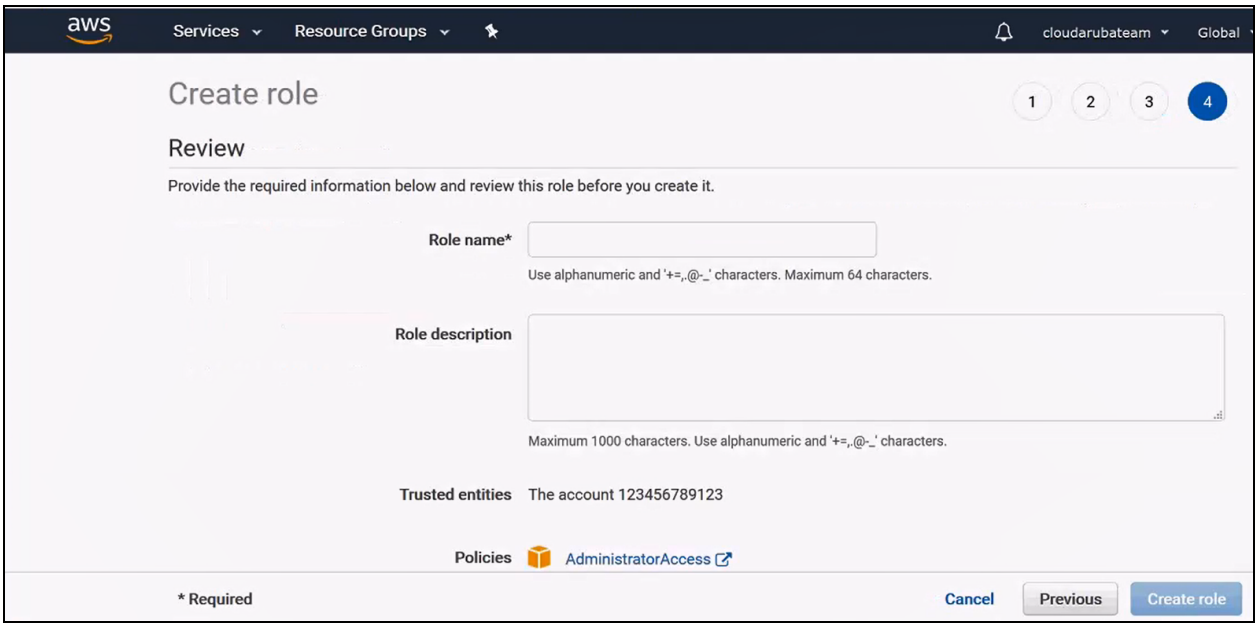
10. Enter the **External ID**. The External ID is created in Aruba while creating the Cloud Provider Account for more information, see the Adding AWS Account image in the Creating a Cloud Provider Account section.



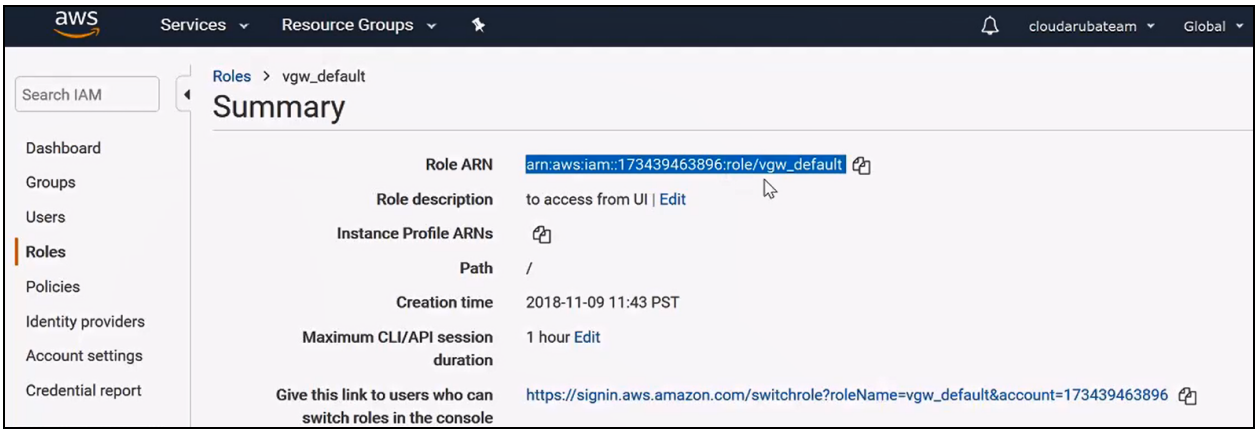
11. Click **Next: Permissions**.
12. Set the permission policy.



13. Click **Next: Tags**.
14. Add a role name and description, in the **Review** screen and click **Create role**.



15. Note the **Role ARN** on the **Role** summary page.



Deploying Virtual Gateways from Aruba Central

NOTE

Before Deploying the Virtual Gateway, ensure that the VPC, Internet Gateway, Security Group, and Key Pair are configured on the AWS.

To deploy a Virtual Gateway instance, complete the following steps:

1. Select the **Deployment** tab.
2. Select the account and the deployment region, and then click **Import VPC**. The orchestrator app imports VPCs and displays the subnets allocated to the VPC.

NOTE

Virtual Gateway deployment from Aruba Central triggers a series of events that may have dependency on AWS. This may result in a delay in displaying the output. For example, a deployment may take up to three or more minutes before the updated status is displayed on the **Deploy Virtual Gateway** page.

3. Click **Deploy Virtual Gateway**. The **Create Virtual Gateway** pop-up window opens.
    a. **Virtual Gateway Subnet**—Enter the subnet range for the VGW. The default subnet is automatically set to the last available /24 subnet and the **Virtual Gateway instance type**.
    b. **Virtual Gateway Size**—Enter the Aruba SKU details for the size of the VGW instance. For more information see, Virtual Gateway Sizing in the Deploying Aruba Virtual Gateways in AWS section.
    c. **AWS Instance Type**Choose the corresponding AWS instance size. For more information see, Virtual Gateway Sizing in the Deploying Aruba Virtual Gateways in AWS section.
    d. **Marketplace Image**—Choose this option to select the ArubaOS image to be installed in Azure Marketplace. When this option is enabled, **Select Image** is automatically updated with the ArubaOS image to be installed in AWS Marketplace.
    e. **Private Image**—Choose this option to select a private ArubaOS image.
    f. **Select Image**—Displays the ArubaOS image to be installed.
    g. **Key-Name**—Choose the Key-pair that will be associated with this VGW.
    h. **Security Group**Choose the **Security Group** that will manage this VGW.
    i. **Edge VPC**—Choose this option to enable or disable Edge VPC. When Edge VPC is enabled, the Virtual Gateways are deployed in an active-active high availability mode. All the Branch Gateways are connected to both Virtual Gateways. The Virtual Gateways in-turn connect to the VPCs through the AWS VPC which is responsible for interconnecting all the VPCs.

When Edge VPC is enabled, Connect/Disconnect Subnet option for VPC will be disabled.

j. **Virtual Gateway High Availability**—Select either to enable or disable High Availability for the VGW.

k. **Deploy Multi-Availability Zone**—Select either to enable or disable Multi-Availability zone deployment for the VGW.

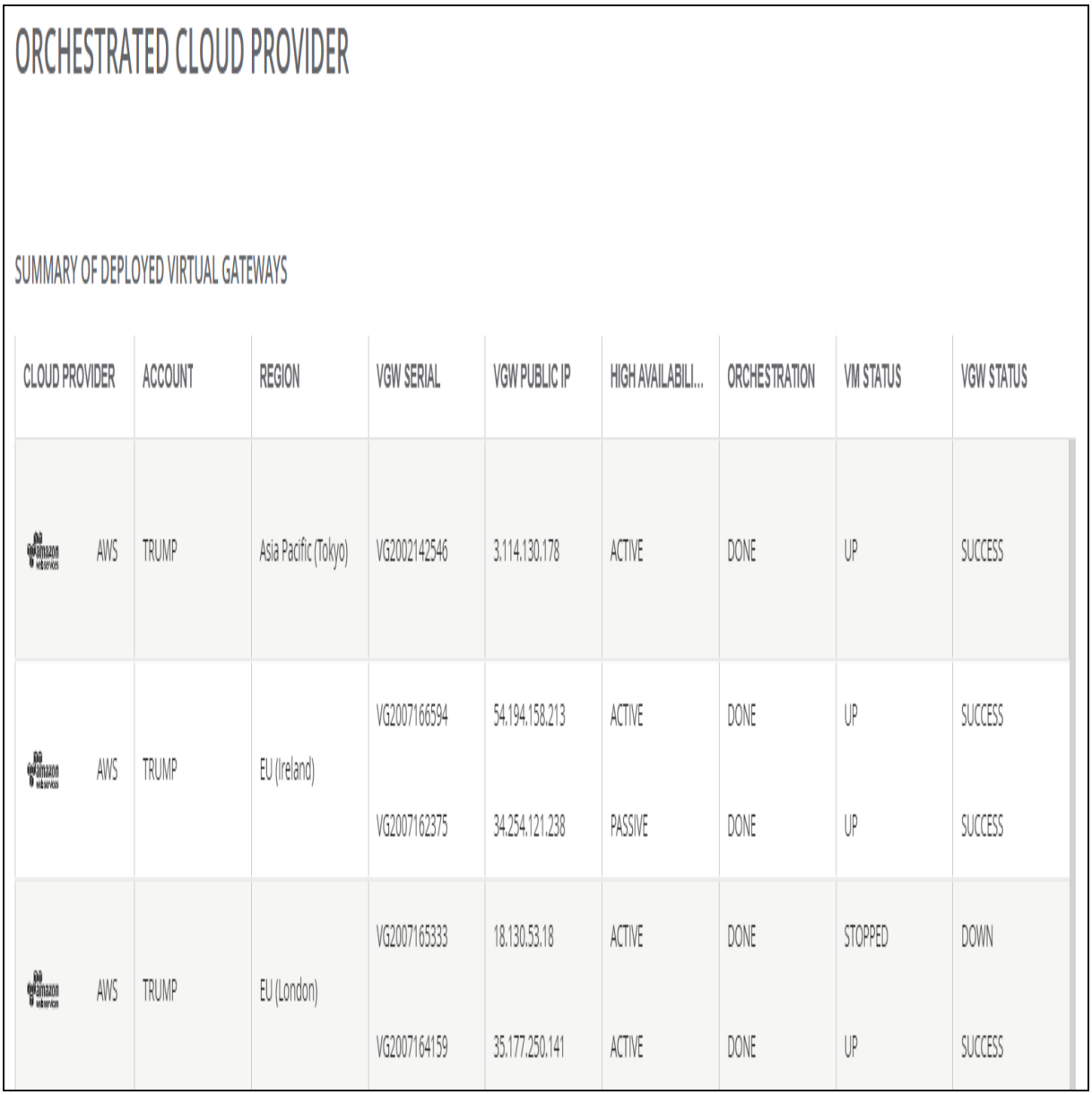
When Edge-VPC is enabled, this configuration option is disabled by default.

Figure 377 *Creating a virtual gateway*

4. Click **Deploy Virtual Gateway**. After the deployment is completed, **Virtual Gateway Deployed** message is displayed.

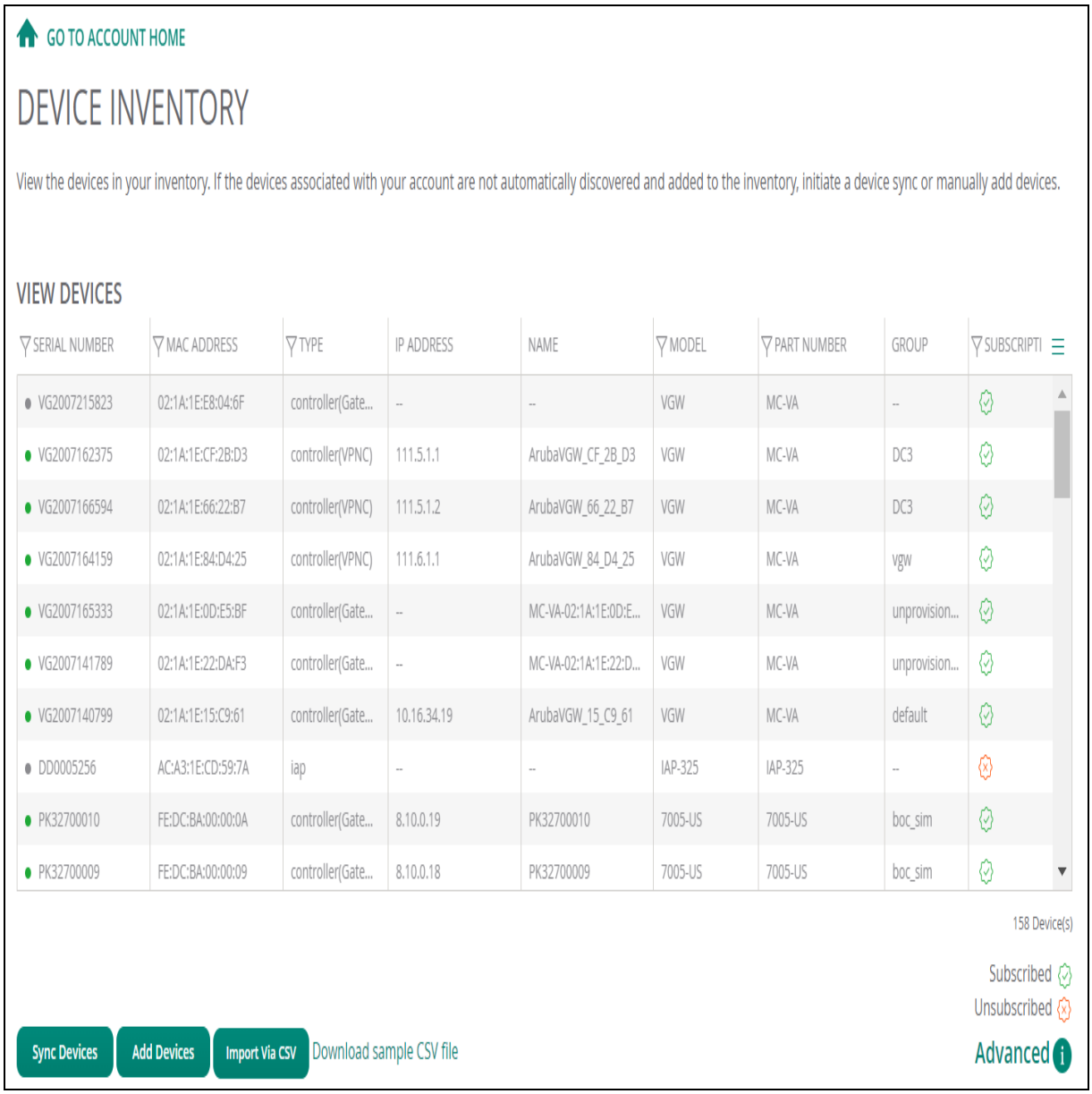
   A summary of the deployment is also displayed on the **Summary** tab of the **Orchestrated Cloud Provider** page. Hovering the cursor over any of the columns displays additional information about the field.

Figure 378 *Summary of deployed virtual gateways*



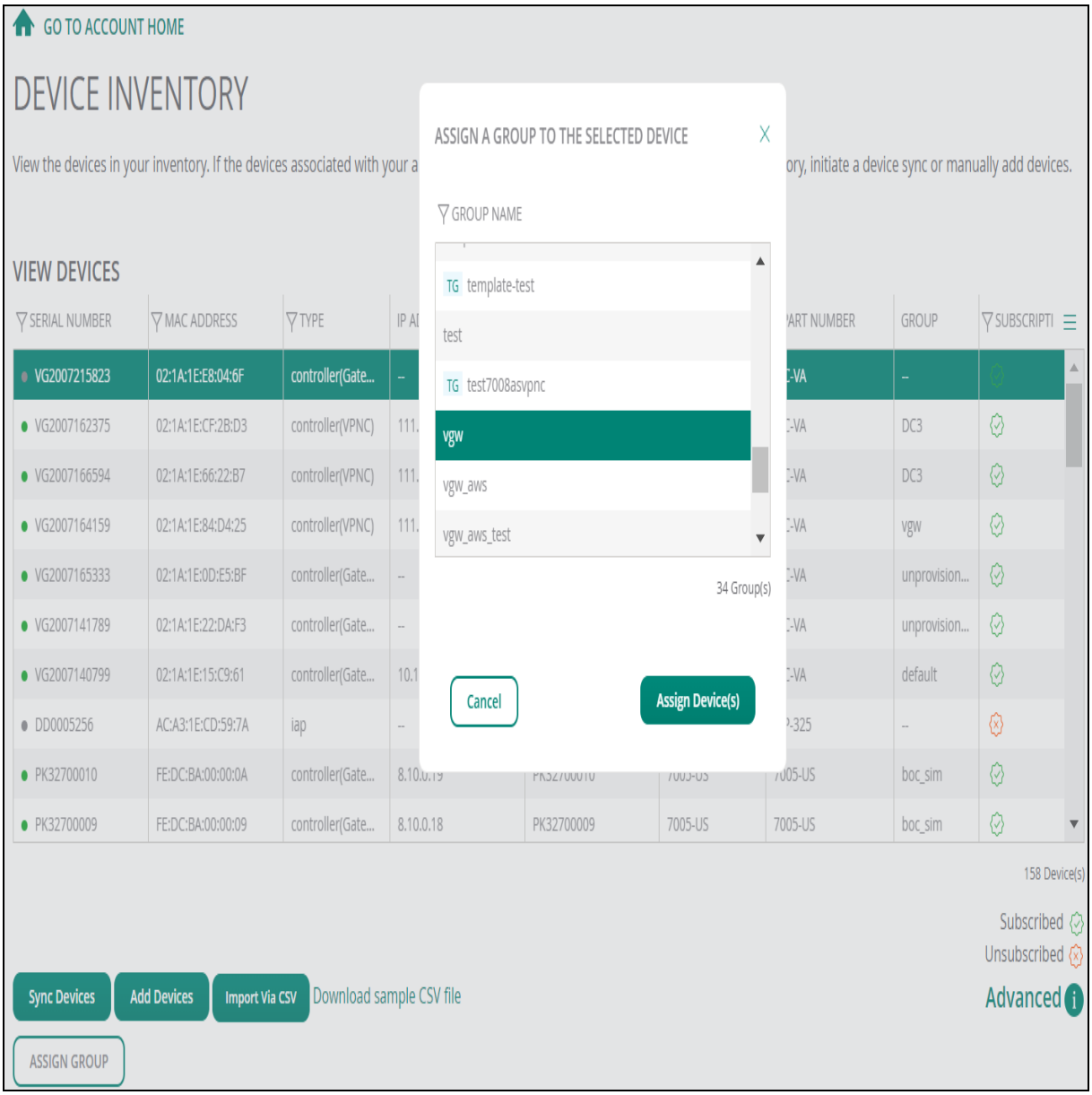
The **Device Inventory** page displays the devices that are in the inventory.

Figure 379 *Viewing devices in Device Inventory*



5. Assign the Virtual Gateway to a valid VPNC group. Adding the deployment to the group ensures that the Virtual Gateway acquires the controllers IP address.

Figure 380 *Assigning Virtual Gateway to a Group*



6. To associate the subnet with the user route table on AWS, on the **Deployment** tab in Aruba Central, click **Connect/Disconnect Subnet**.

Verifying the Aruba VGW deployment on AWS

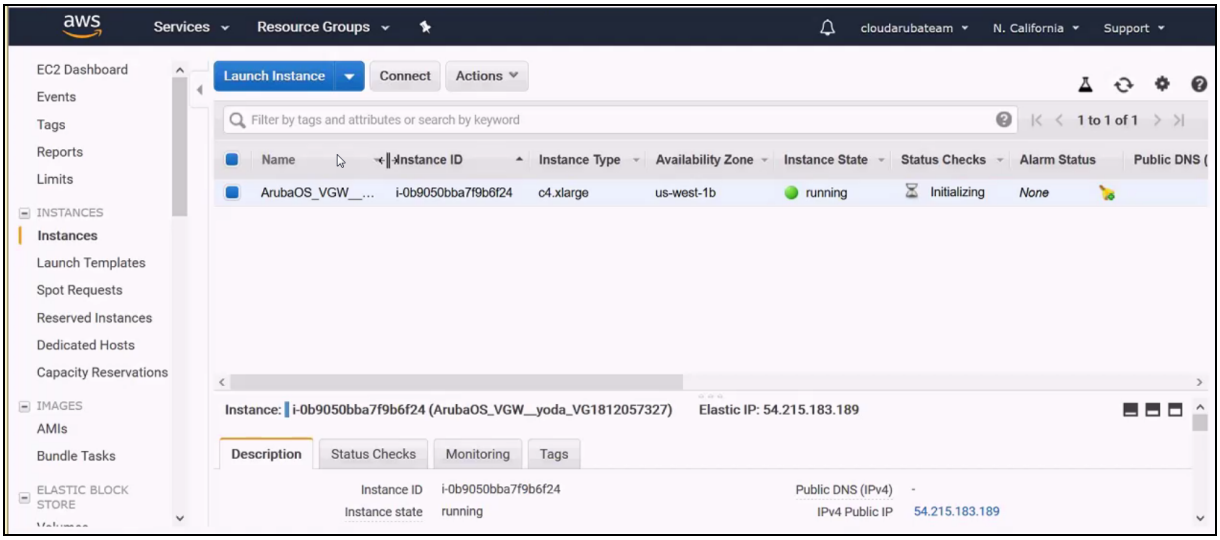
NOTE

The information that is available in this section is meant for debugging purposes only. Aruba does not recommended making any changes as that may disrupt the configuration.

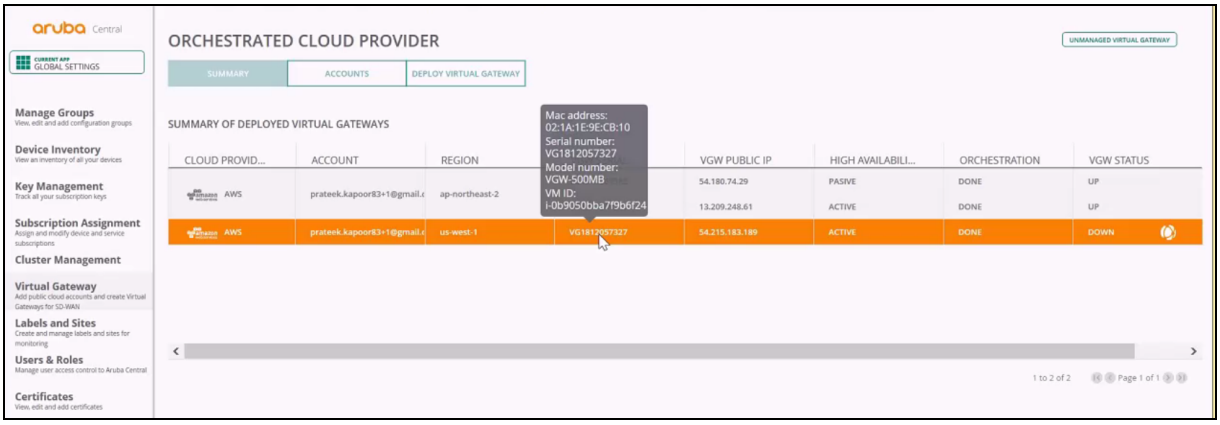
To verify Aruba VGW deployment on AWS, complete the following steps:

1. In the AWS EC2 dashboard, click **Instances** section. After the Virtual Gateway is deployed successfully from Aruba Central, AWS creates an instance.

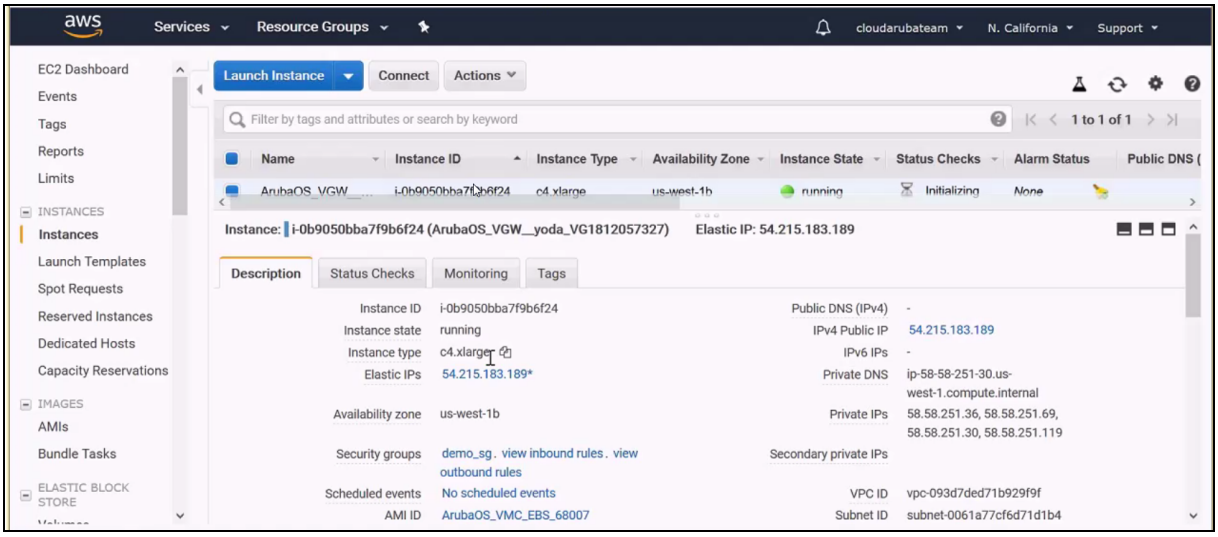
2. Select the **Instance**.



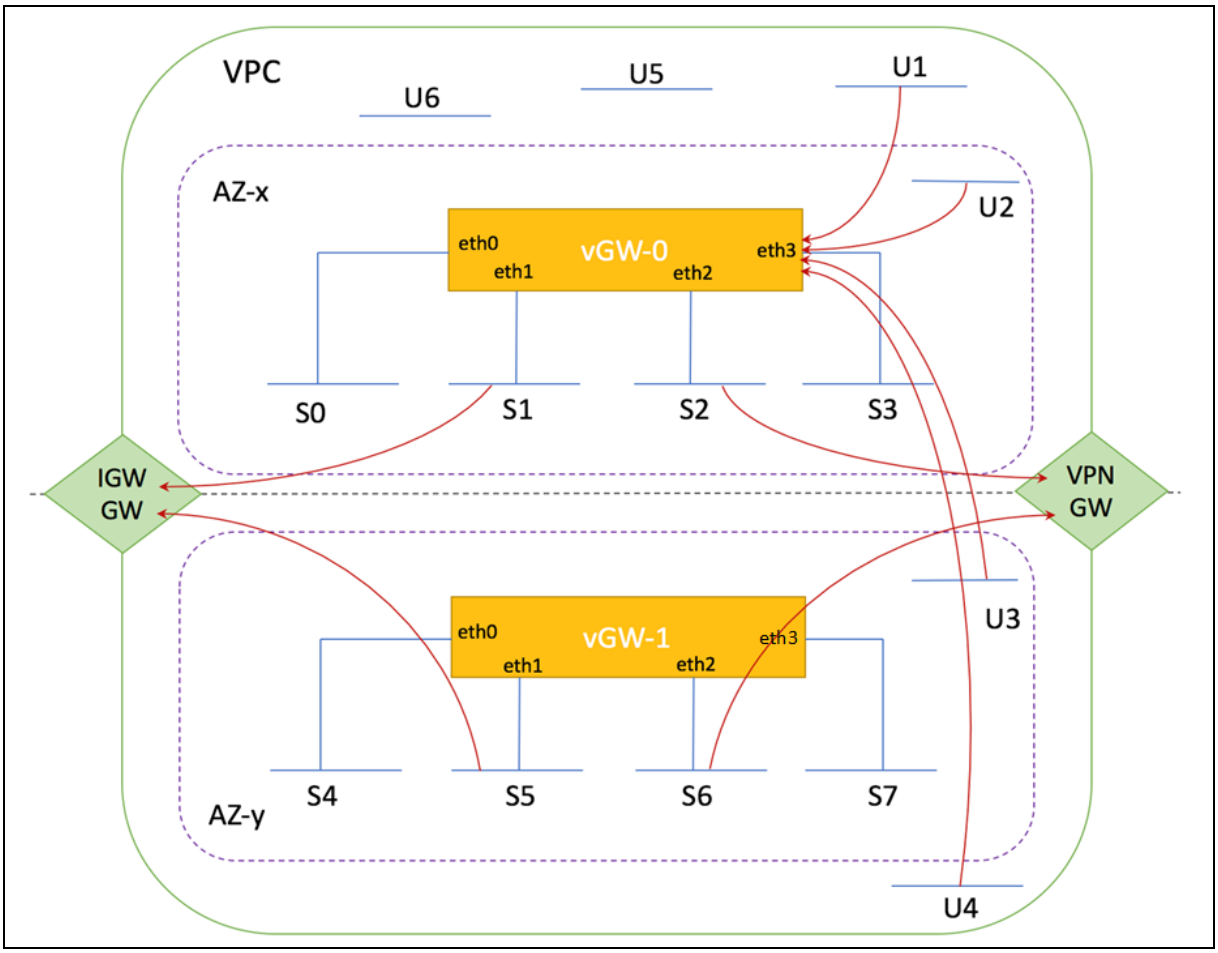
3. Verify the **Status Checks** and ensure that the instance status is displayed as **2/2 checks**. During this process, the **VGW Status** in Central displays as **Down.**
4. Verify the status of Virtual Gateway deployment on the **Virtual Gateway** > **Orchestrated Cloud Provider** > **Summary** page in Aruba Central Orchestrated Cloud Provider, displays the information and status of each Virtual Gateway. Placing the mouse cursor over each item displays additional information.



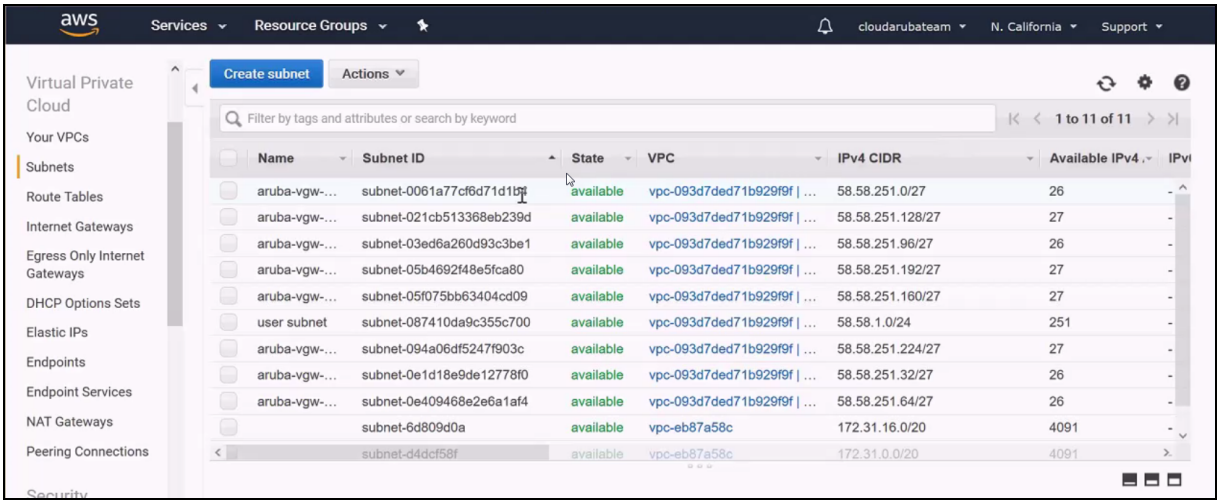
5. Go to the EC2 instance in the AWS console. Verify the **Instance ID**, **Instance Type**, along with displaying the **Elastic IPs**, **Private DNS**, and **Private IPs**. A deployment can support up to two Virtual Gateways. Each Virtual Gateway instance supports up to four interfaces. Each interface must be mapped to a subnet.



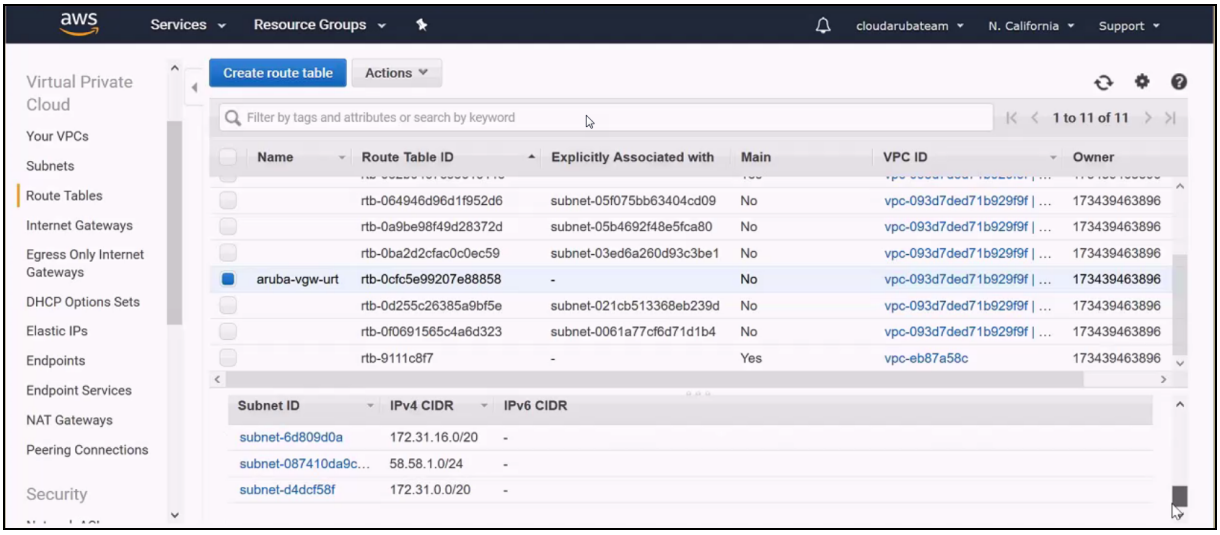
The following figure shows a sample mapping of the network interfaces:



6. In the **Virtual Private Cloud** section of AWS, click **Subnets** to view the subnets.



7. In the **Virtual Private Cloud** section of AWS, click on **Route Tables** and verify the **aruba-vgw-urt** user route table created as part of the orchestration. This route table enables the Virtual Gateway instance to connect the connect the user subnet from Aruba Central to AWS.



After a successful deployment, the Virtual Gateway instances launch and connect to Aruba Central with the latest AMI.

Deploying Aruba Virtual Gateways in AWS (Unmanaged Mode)

Aruba Central supports deploying Virtual Gateways in the unmanaged mode. In the unmanaged mode, administrators deploy the Virtual Gateway instance using the AWS console. After deploying the Virtual Gateway instance in AWS, administrators can generate user data from Aruba Central to allow Virtual Gateway to connect to Aruba Central as a managed device.

To deploy Virtual Gateways in the unmanaged mode in AWS, complete the following steps:

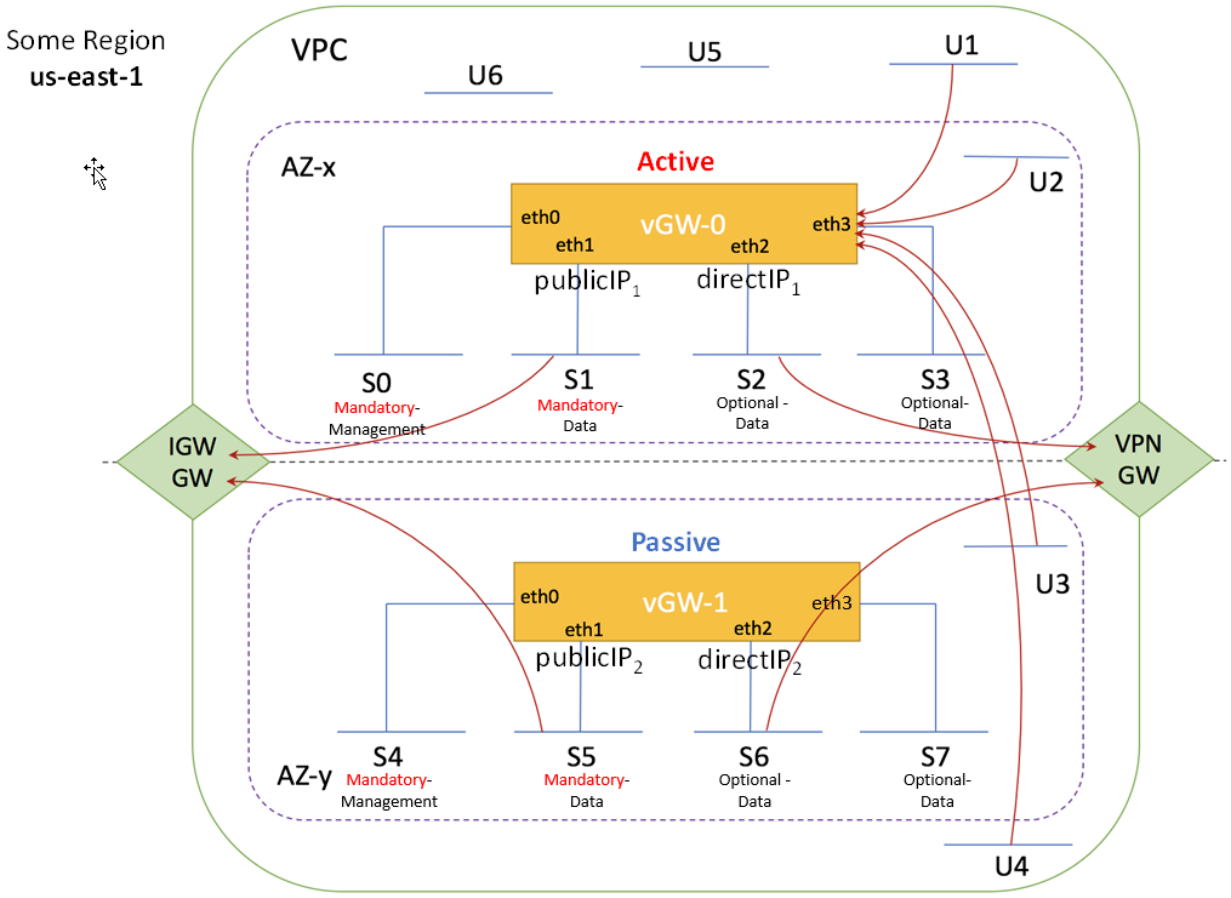
- Creating a VPC for Virtual Gateway Instance on AWS
- Creating a Security Group
- Creating a Network Interface
- Launching a Virtual Gateway Instance

- Generating User Data in Aruba Central
- Uploading the User Data to the Virtual Gateway Instance in AWS Instance
- Verifying the Instantiation Status

Creating a VPC for Virtual Gateway Instance on AWS

To set up a Virtual Gateway instance in AWS, log in to your AWS account and complete the following steps:

1. Log in to your AWS account.
2. Select a region for the VPC.
3. Click **Launch VPC Wizard**. The **VPC Wizard** opens.
4. Enter a name for the VPC.
5. Configure subnets. The Virtual Gateway deployment requires two subnets; one each for management and data traffic. The following figure illustrates the recommended subnet configuration for Virtual Gateway deployments.



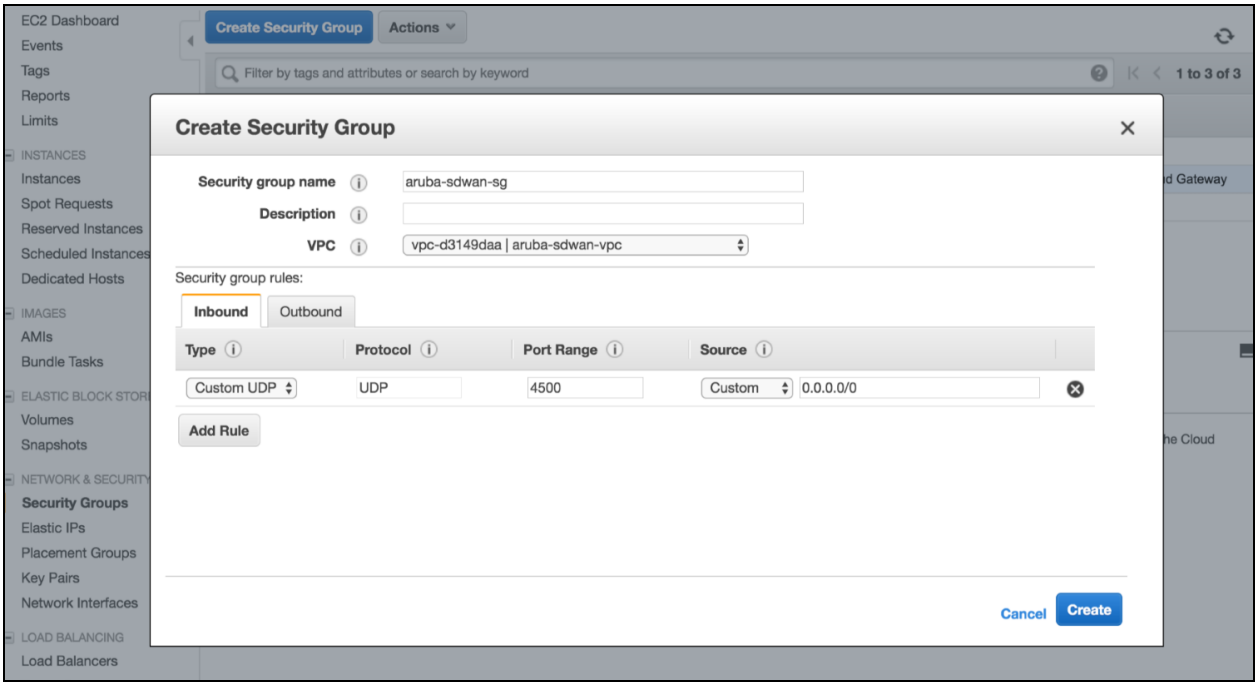
6. Click **Create VPC**.
7. Create an Internet Gateway and attach it to the VPC.

Creating a Security Group

Security groups allow you to control both incoming traffic and outgoing traffic from the Virtual Gateway instance. For example, you can add a rule to a security group for connecting to your instance from your IP address using SSH.

To create a security group, complete the following steps:

1. Select the region in which your VPC is created.
2. In the AWS Dashboard, select the EC2 tab and click on **Security Groups** under **NETWORKING & SECURITY**.
3. Enter a name for the group.
4. Click **Security Groups**.
5. Specify a group name.
6. Select the VPC.
7. Add inbound and outbound rules. Ensure that the UDP port 4500 and other ports required for device communication over a network firewall are open.

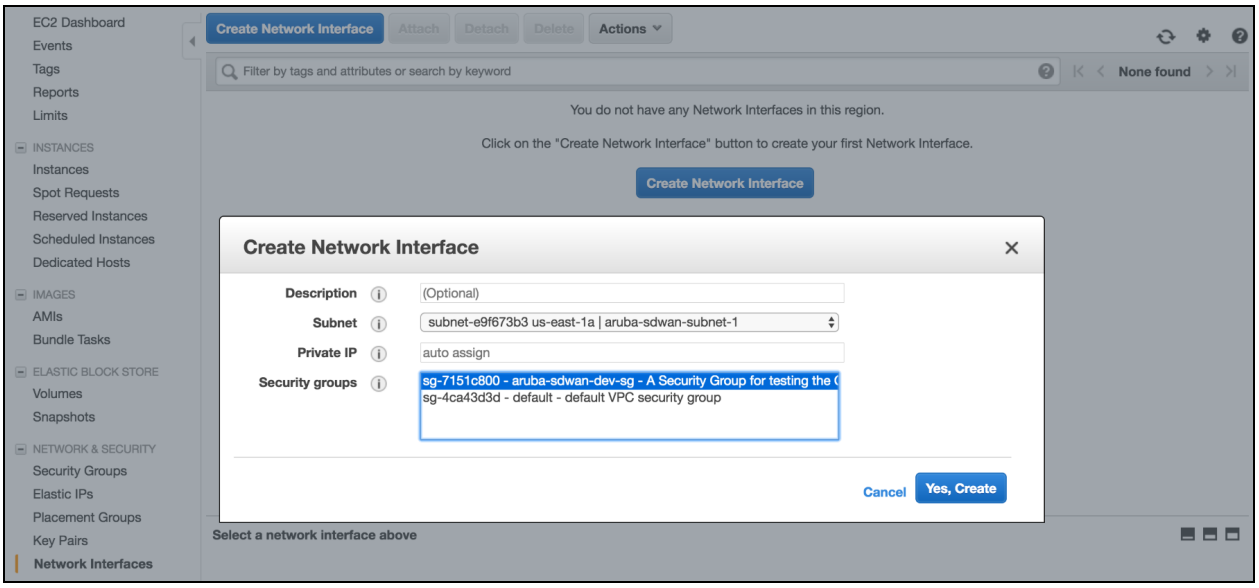


8. Click **Create**.

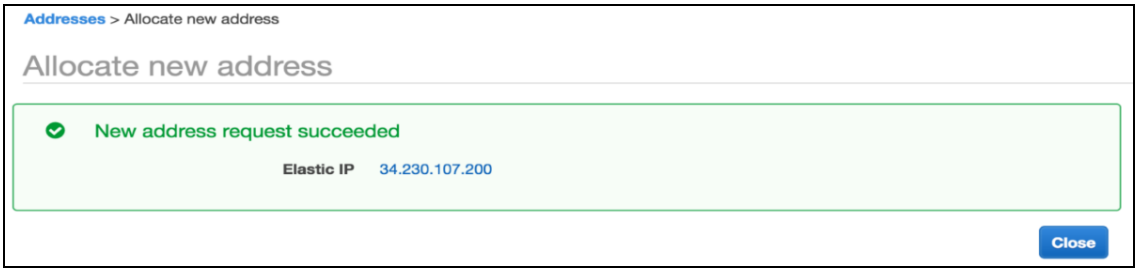
Creating a Network Interface

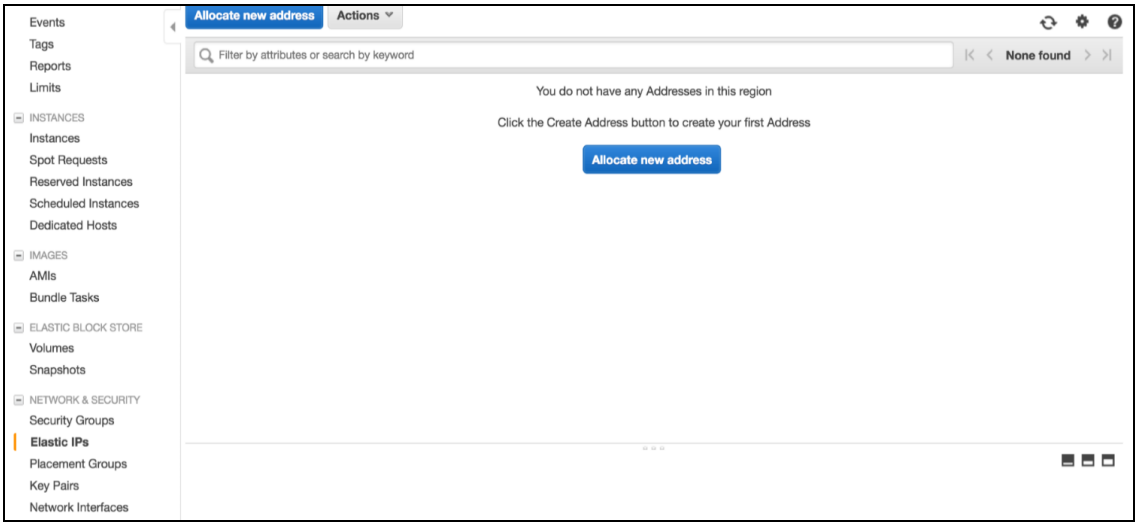
To create a network interface, complete the following steps:

1. Go to Amazon EC2 console and click **Network Interfaces**.
2. Click **Create Network Interface**.
3. Select the subnet.
4. Select the security group you just created.
5. Click **Yes, Create**.



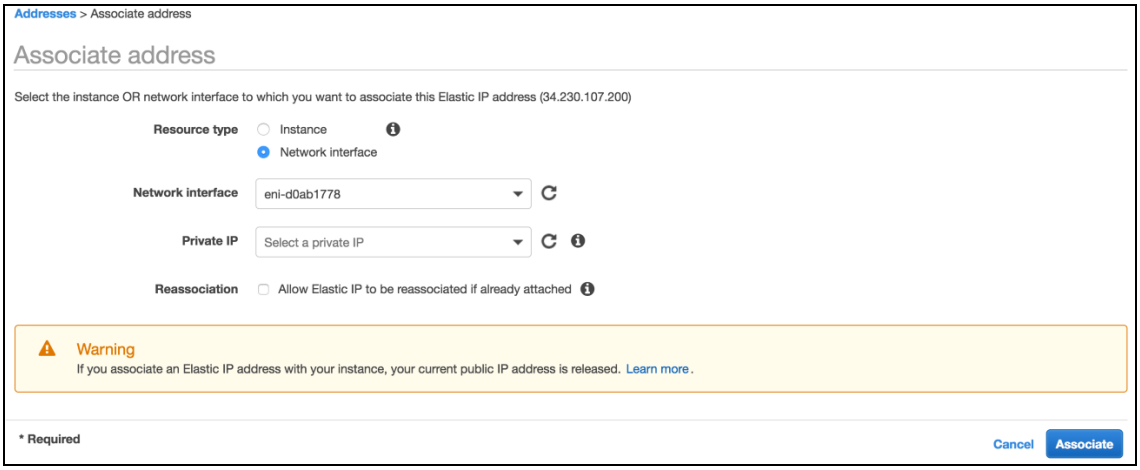
6. Associate an elastic IP address with your instance. By default, an instance in a nondefault VPC is not assigned a public IP address. An elastic IP address must be allocated to your account, and then associated with your instance. To allocate an elastic IP address:
    a. Go to Amazon VPC console and click **Elastic IPs**.
    b. Select **Allocate New Address**.



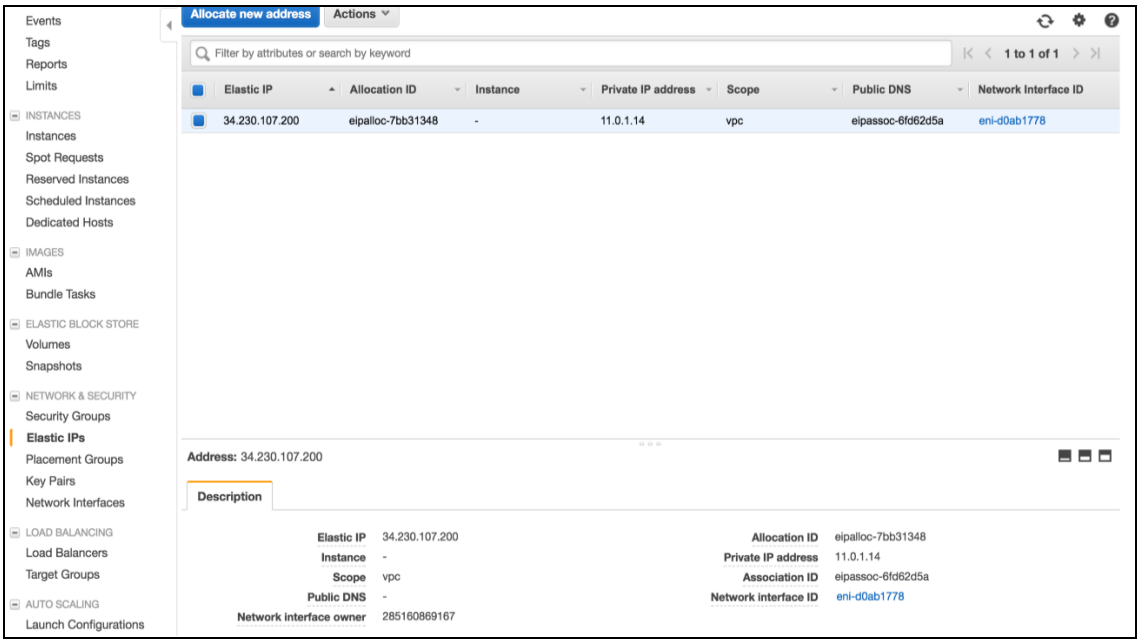


    c. Click **Close**.
    d. Select the elastic IP address from the list, and then click **Actions** > **Associate Address**.

e. Select the network interface.



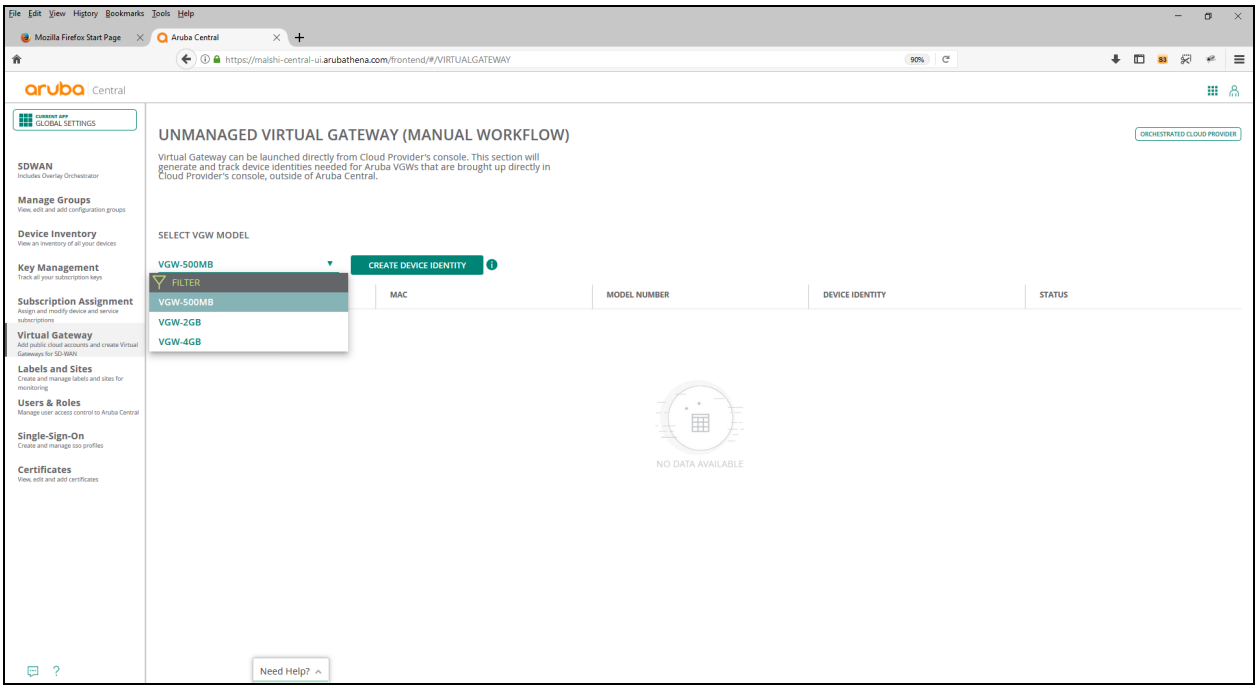
f. Click **Associate**.



Launching a Virtual Gateway Instance

To launch a Virtual Gateway instance, complete the following steps:

1. Open the AWS EC2 console.
2. Select the region in which you have deployed your VPC.
3. Click **Launch Instance**. When you launch an instance, you must select an AMI. An AMI contains the software image or information required to create a new instance. To obtain the AMI image for instance, contact Aruba Customer Support.
4. On the **Choose an Amazon Machine Image (AMI)** page, select the AMI.
5. Click **Choose Instance Type** and select the hardware configuration and size of the instance to use. For more information see, Virtual Gateway Sizing in the Deploying Aruba Virtual Gateways in AWS section.



6. Click **Configure Instance Details**. Ensure that the subnets and network interfaces are configured.
7. Click **Add Storage** and add the storage details. Aruba recommends that you add at least 8GB EBS storage.
8. Click **Add Tags** and add tags if required.
9. Click **Configure Security Group** and ensure that a security group is created and attached to the VPC.
10. Click **Review**.
11. Review the configuration and click **Launch**. The system prompts you to select an existing key pair or create a new key pair. By default, the Linux instances do not have a password set. To secure your login information for your instance, you can create a key pair.
12. Create new key pair if required.
13. Click **Launch**. The instance is launched and available for use.

Generating User Data in Aruba Central

For Aruba Central to manage a Virtual Gateway that is deployed manually and directly in a customer's VPC, generate device identity for the device in Aruba Central.

To generate device identity for the Virtual Gateway instance, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways**, click the **Config** icon. The configuration page is displayed.
3. Click **Unmanaged**.
4. Select the Virtual Gateway model.
5. Click **Create Device Identity**.
6. Click **Yes** to confirm identity creation. Aruba Central displays the newly created VGW with the following fields:
    a. **Serial #**—Displays the serial number of the Virtual Gateway.
    b. **MAC**—Displays the sMAC address of the Virtual Gateway.

c. **Model Number**—Displays the model number of the Virtual Gateway.
d. **Device Identity**—Displays the device identity of the Virtual Gateway.
e. **Status**—Displays the status as User Generated for the created device identity of the Virtual Gateway.

7. Click the three vertical dots icon next to the Status to view the **Account Options**.
8. Click **Download txt**. The user data includes the following information:
   - Aruba Central URL
   - Serial Number
   - User name and password for the Virtual Gateway

Virtual Gateways use these credentials to connect to Activate and EST server for EST enrollment.

- MAC Address of Virtual Gateway
- Part Number of the Virtual Gateway instance
- Deployment mode
- Network interfaces configured on a Virtual Gateway. For example, eth0, eth1, eth2 and eth3
- Activate URL

Uploading the User Data to the Virtual Gateway Instance in AWS Instance

To upload user data to the Virtual Gateway instance, complete the following steps:

1. Log in to the AWS EC2 console.
2. Select the Virtual Gateway instance for which you want to upload the user data.
3. Click **Actions** > **Instance Settings** > **View/Change User Data**.
4. Copy the user data downloaded from Aruba Central and paste it in the **User Data** field.
5. Click **Save**.
6. To start the instance, click **Actions** > **Instance State**, and then click **Start**.
7. Wait for the instantiation to complete.

Verifying the Instantiation Status

To verify the instantiation status, and check the status of the Virtual Gateway instance in the Summary dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways** > **Manual**, to view the summary page for manually orchestrated Virtual Gateways with following columns:
   - **Tenant**—Displays the name of the tenant network.
   - **Serial Number**—Displays the serial number of the Virtual Gateway.
   - **MAC Address**—Displays the MAC address of the Virtual Gateway.
   - **Model Number**—Displays the model number of the Virtual Gateway.
   - **IP Address**—Displays the IP address of the Virtual Gateway.
   - **Name**—Displays the name of the Virtual Gateway.
   - **Device Identity**—Displays the device identity of the Virtual Gateway.
   - **Status**—Displays the Enrollment over Secure Transport (EST) status of the Virtual Gateway.

3. Check if the Virtual Gateway instance is displayed in the device inventory.
4. Check if Virtual Gateway instance is connected to Aruba Central.

Deploying Aruba Virtual Gateways in Microsoft Azure

Virtual Gateways simplify branch network deployments for organizations intending to migrate their infrastructure to cloud providers such as Microsoft Azure.

The SD-Branch integration with a private cloud infrastructure hosted in Microsoft Azure allows you to set up a secure connection between the Aruba Branch Gateways and the Virtual Network (VNET) environments in Microsoft Azure.

Aruba Branch Gateway supports standard IPsec tunnels, and establishes direct communication with the Azure VPN Gateway.

Aruba Central supports deploying and managing Virtual Gateways hosted on the Microsoft Azure VNETs using one of the following methods:

- Managed mode—In the managed mode, Aruba Central allows administrators to deploy Virtual Gateways using the orchestrator application in Aruba Central. The Virtual Gateway orchestrator in Aruba Central imports VNETs from a Microsoft Azure account, deploys, connects, and allows you to manage Virtual Gateways from Aruba Central. For step-by-step instructions on deploying Virtual Gateways in the managed mode, see Deploying Aruba Virtual Gateway in Microsoft Azure (Managed Mode).
- Unmanaged mode—In the unmanaged mode, Virtual Gateways must be manually deployed and launched from the cloud provider console. Aruba Central allows you to generate user data for such deployments and manage Virtual Gateways from Aruba Central. For step-by-step instructions on deploying Virtual Gateway in unmanaged mode, see Deploying Aruba Virtual Gateway in Microsoft Azure (Unmanaged Mode).

Virtual Gateway Sizing

The Aruba Virtual Gateway requires the use of a supported Azure instance with a minimum of 500 Mbps of throughput and can support up to 1600 IPSec tunnels. This table lists out the supported Azure instances for each Aruba Model/SKU:

Aruba Model/SKU Name	Throughput	Supported Azure Instance	vCPU	Flash Memory (GB)	Tunnels
VGW-500MB	500 Mbps	Standard_DS3_v2	4	15	1600
		Standard_F8s_v2	8	30	
		Standard_F16s_ v2	16	60	
VGW-2GB	2 Gbps	Standard_F8s_v2	8	30	4096
		Standard_F16s_ v2	16	60	
VGW-4GB	4 Gbps	Standard_F16s_ v2	16	60	8192

NOTE

If a higher number of tunnels are required, please contact your Aruba Sales Specialist.

Deployment Procedure

See the following topics for step-by-step instructions on how to deploy an Aruba Virtual Gateway in Microsoft Azure VNET:

- Deploying Aruba Virtual Gateway in Microsoft Azure (Managed Mode)
- Deploying Aruba Virtual Gateway in Microsoft Azure (Unmanaged Mode)

Additional References

For a detailed description of SD-WAN integration with Microsoft Azure and Virtual Gateway deployment in Microsoft Azure, see the Aruba SD-WAN Integration with Microsoft Azure Public Cloud Technical Note.

Deploying Aruba Virtual Gateway in Microsoft Azure (Managed Mode)

Aruba Central supports deploying Virtual Gateways in Microsoft Azure using the orchestrated mode. For orchestrated-mode deployments, Aruba Central supports the orchestration service for automating Virtual Gateway deployments. The orchestrator application in Aruba Central enables IT administrators bring up, configure, and monitor Virtual Gateways from the Aruba Central management interface.

Deployment Procedure

Before deploying Aruba Virtual Gateway deployment in Azure VNET, ensure that you have the following resources and account privileges:

- A valid subscription and administrator credentials to access your Azure account.
- A valid subscription and account credentials to deploy Virtual Gateways.
- Virtual Gateway VHD image.

NOTE

You can configure an Aruba Virtual Gateway in Microsoft Azure using either the Azure Cloud Shell or the Azure graphical user interface (UI). The configuration steps described in this document are based on the UI workflows.

To deploy a Virtual Gateway in Microsoft Azure, complete the following steps:

1. Registering a New Application in Azure
2. Creating a Client Secret
3. Adding the Application Permissions
4. Setting up Access control and Role Assignments
5. Viewing the Application IDs
6. Creating a Resource Group
7. Creating a Storage Account
8. Creating a VNET
9. Uploading the Aruba Virtual Gateway Software Image
10. Adding a Cloud Provider Account in Aruba Central

11. Deploying the Virtual Gateway
12. Verifying the Deployment Status

Additional References

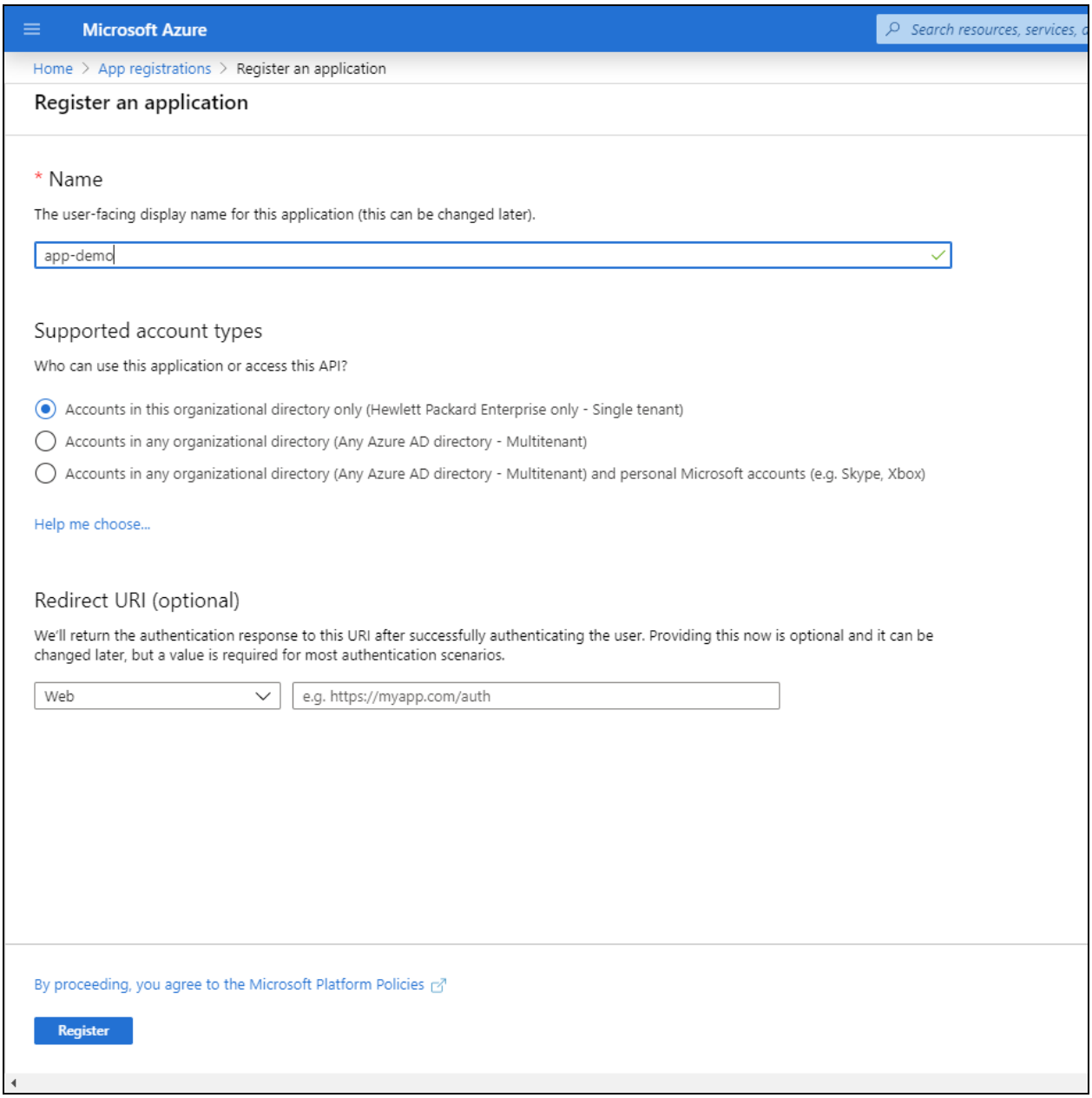
For more information about SD-WAN integration with Microsoft Azure and Virtual Gateway deployment in Microsoft Azure, see the Aruba SD-WAN Integration with Microsoft Azure Public Cloud Technical Note.

Registering a New Application in Azure

Enterprise software-as-a-service (SaaS) providers develop commercial cloud services applications that can be integrated with the Microsoft identity platform to provide secure sign-in and authorization for their services. To register a new application Azure, complete the following steps:

1. Log in to the Azure portal. On the Home screen, select **App registration** from the Azure services listed.
2. In the App registrations page, click **+ New registration** to initiate the registration process.
3. In the **Register an application** page, enter these details:
   - **Name**—Enter an account name for easy identification. This is a mandatory field.
   - **Supported account types**—Select the profile or entity that can access this application. By default **Accounts in this organizational directory only (Hewlett Packard Enterprise only - Single tenant)** is selected.
   - **Redirect URI (optional)**—After successfully authenticating the user, a response is sent to this URI. This information is optional and can be updated at a later time.

Figure 381 *Registering an app*



4. Click **Register** to complete the registration. The new application page loads in a few seconds.

Creating a Client Secret

To ensure that the application communication is secure, complete the following steps and create a client secret:

NOTE

When the Client secret key expires, the orchestration page displays an access denied message. To create a new client secret key, complete the following steps.

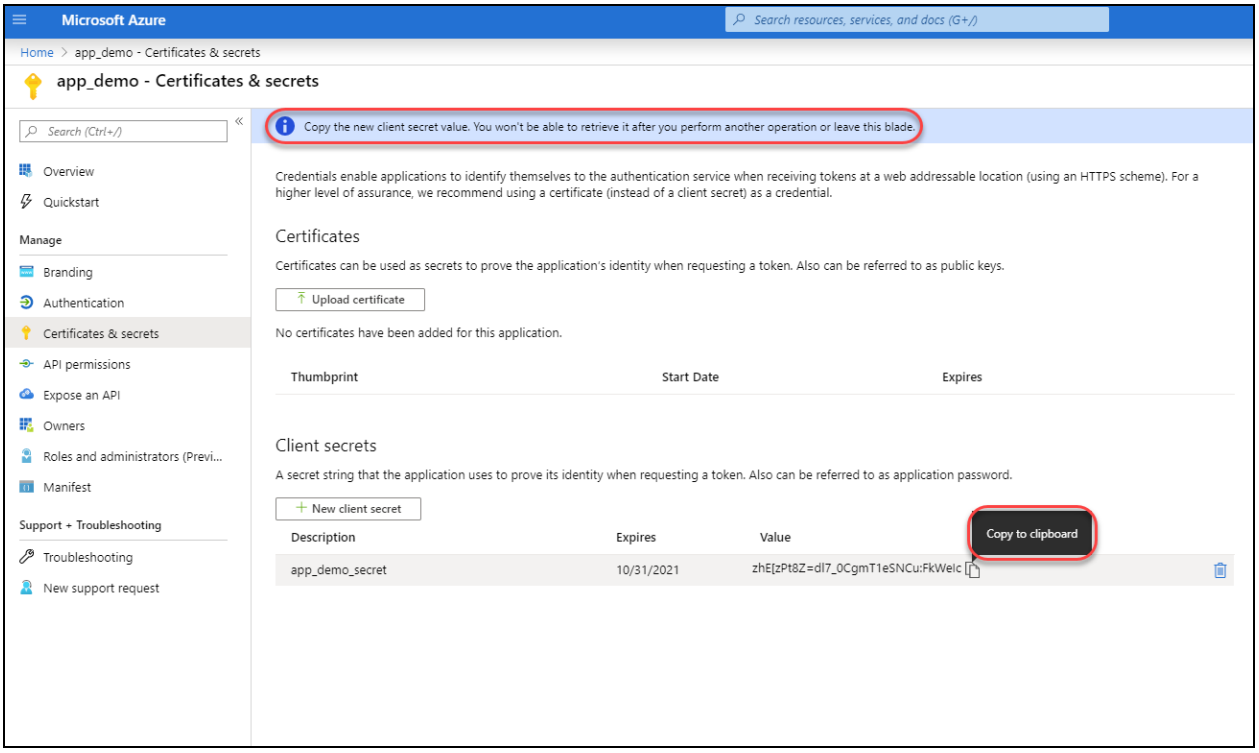
1. On the left navigation pane, click **Certificates & secrets** to configure the client secret.
2. Click the **+ New client secret**, to open the Add a client secret pane.

3. In the Add a client secret pane, enter a description of the secret and the duration of the secret validity and click **Add**.
4. In the **Certificate & secrets** page, the new secret will be displayed along with the **Value**.

NOTE

Copy the **Client secrets Value** as this will be value will be hashed out after approximately ten minutes.

Figure 382 *Setting up a Client secret*

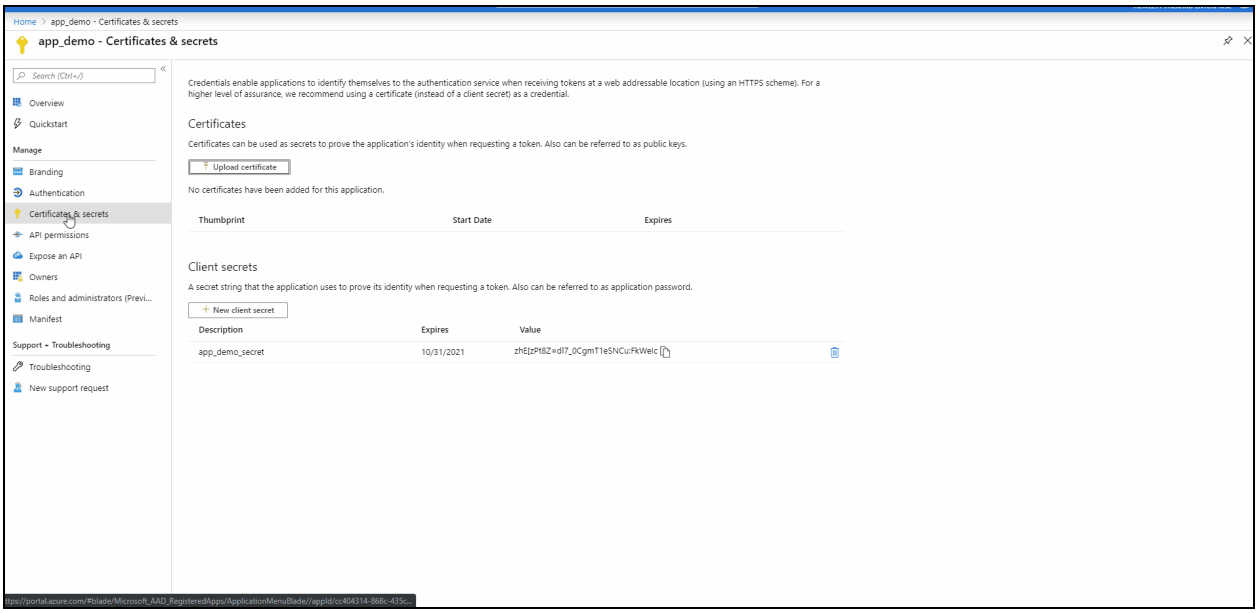


Adding the Application Permissions

To set the permissions for access and control of the application, complete the following steps:

1. To set the application permissions, on the left side navigation pane click **API permissions**.
2. In the **API permissions** pane, click **+Add a permission** to open the **Request API permission** pane.
3. In the **Request API permission** pane, select **Azure Service Management** API from the **Microsoft APIs** tab.
4. **Delegated permission** is selected by default, select **user_impersonation** and click **Add permissions**.
5. The **Azure Service Management** api with **user_impersonation** permission is now added to the list of permitted APIs.

Figure 383 *Adding the Application permissions*



Setting up Access control and Role Assignments

Once the application is set up, a role needs to be assigned to the application. To assign a role to the application, complete the following steps:

1. In the search box on the home screen search for **Subscriptions**, and select subscriptions from the displayed service options.
2. In the **Subscriptions** page, select the subscription that you are working with.
3. Select **Access control (IAM)** from the left side navigation to open the access control pane.
4. In the access control pane, select the **Role assignments** tab, and click the **+Add** and choose **Add role assignment**.
5. In the Add role assignment set the following details:
   - **Role**—Select the Role to be assigned to the app. In this configuration, set the role as a **Contributor**. Changes to the roles and associated assignments can only be made by an administrator.
   - **Assign access to**—Assign the access level for the role.
   - **Select**—Set the application, user, or device that inherits the above properties. If required, search using the registered name or email address as keywords.
   - Choose the user or application from the displayed options.
6. Click **Save** to save and exit.

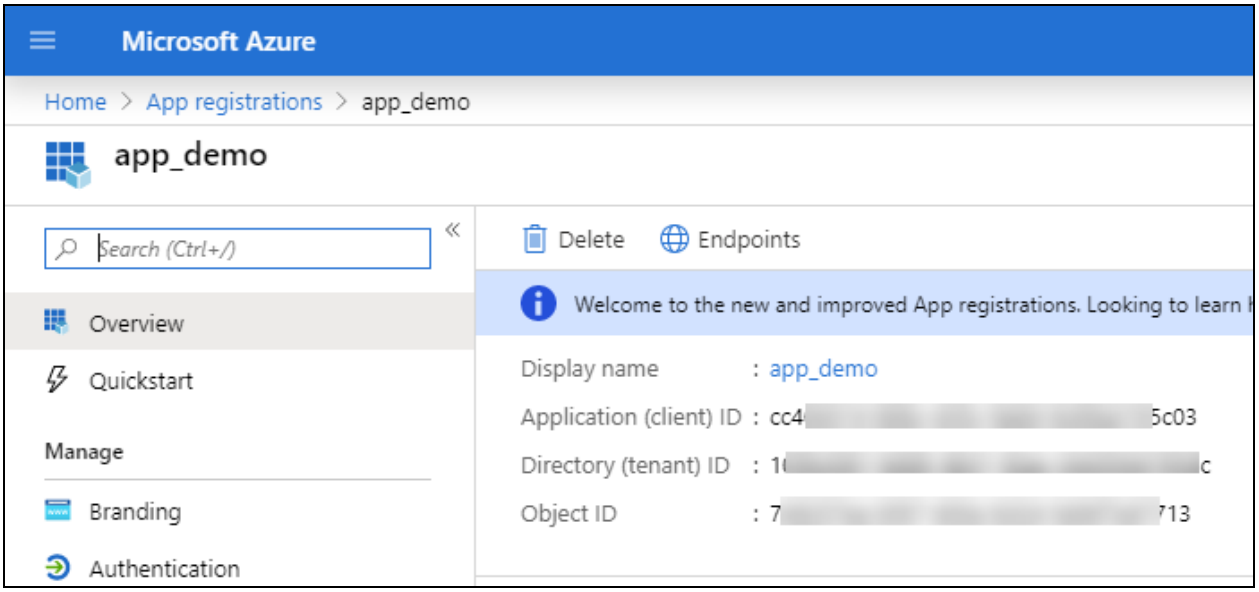
Viewing the Application IDs

The application IDs are needed to start the onboarding process in Aruba Central. To view the application IDs, complete the following steps:

1. In the search box on the home screen search for App registrations, select **App registrations** from the displayed service options.
2. In the **App registrations** page, select the application and the application details pane is displayed. Note the following IDs to be used during the onboarding in Aruba Central:

- **Application (client) ID**
- **Directory (tenant) ID**

Figure 384 *Viewing the application ids*



Creating a Resource Group

A resource group in Azure is a logical container that consists of resources required for deploying a virtual machine (VM). Resource groups allow you to logically group related resources such as storage accounts, virtual networks, and VMs. Resource groups also allow you to deploy and manage all these resources as a single entity.

Note the following important points about resource groups in Azure:

- A resource group can contain resources from different regions or locations.
- Access control for administrative actions can be scoped with a resource group.
- Resources can be added or removed from a group at any time.
- Resources can be moved from one group to another group.
- Each resource can only exist in one resource group.
- Resources can interact with other resources group containers.

To verify if your subscription has a resource group, click **Home** > **Resource Groups**.

If you do not have a resource group created in your Azure subscription, follow these steps to create a resource group:

1. Log in to Azure portal using your Azure account credentials.
2. Click **+ Create a Resource** to access Dashboard and then search for Resource Groups in the search box to access the **Resource Groups** configuration page.
3. Click **Create**.
4. In the **Basics** tab, enter the following information:
   - **Subscription**—Select your Microsoft Azure subscription.
   - **Resource group name**—Enter a name for the resource group.
   - **Region**—Select the geographic location for the resource group.

5. Click **Review+Create** and then click **Create**.

Creating a Storage Account

Storage account in Azure provides a unique namespace to store and access your Azure storage objects. Every storage account must belong to an Azure resource group.

For Aruba Virtual Gateway deployments, you will need a storage account to store the software image and also a separate storage account for Boot Diagnostics. The Boot Diagnostics option allows you to view logs pertaining to VM boot issues. You can enable the Boot Diagnostics option when configuring a VM.

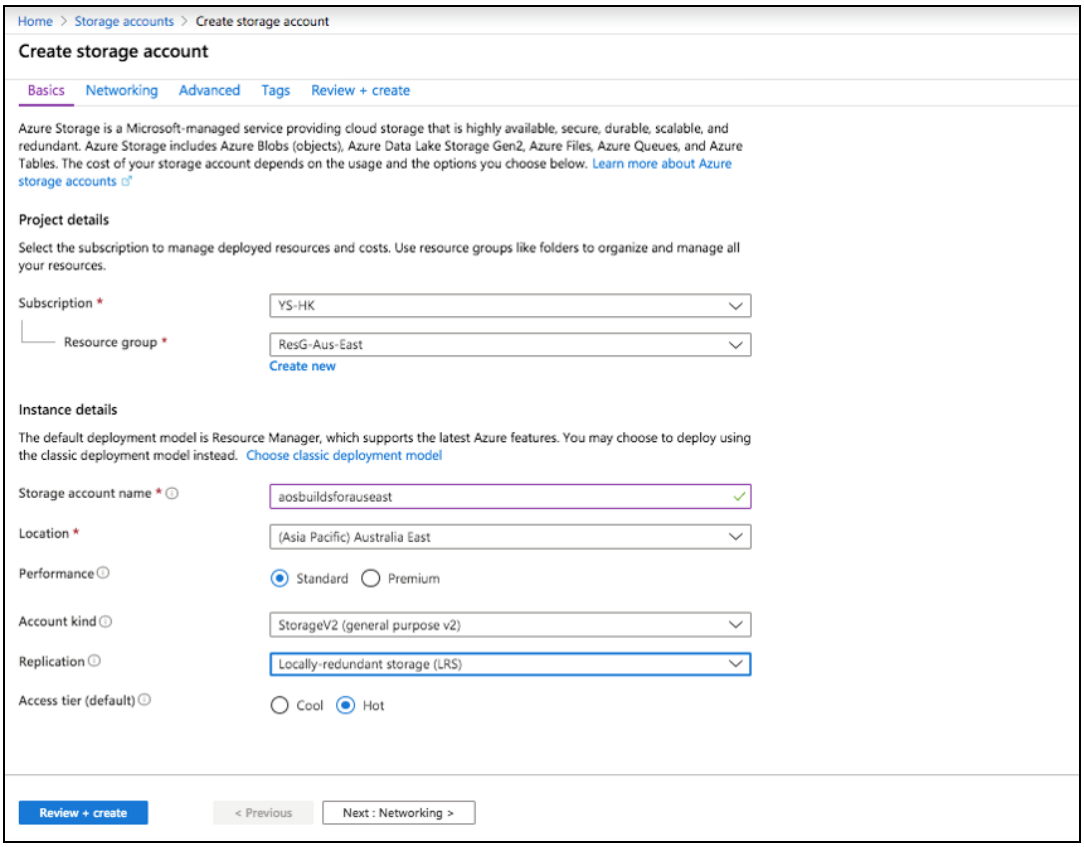
If you do not have a storage account created and mapped to the resource group that you want to use for Aruba Virtual Gateway deployment, complete the following steps:

1. Log in to your Azure account.
2. Select **Home** > **Storage Accounts**.
3. In the **Storage Accounts** window, click **Add**.
4. Enter a unique name for your storage account.

The name must be between 3 and 24 characters in length, and can include numbers and lowercase letters.

5. Choose a **Subscription** and **Resource group** that this account is linked to.
6. Enter the **Storage Account Name, Location, Account kind**, and **Replication**.
7. Click **Review + create**, validate the account before you proceed.
8. Enter the **Resource group** name that will be associated with this storage account.
9. Click **Create** to complete the storage account creation procedure.

Figure 385



Configuring Containers

Virtual machines create a partition for each operating system deployment. Each partition simulates a machine using software. Containers offer near-instant deployment and are a great way of moving code, the deployment time is shorter and they are easier to maintain.

1. In the **Storage accounts** window, select the account that was created, and click **Containers**.
2. Click on **Containers** to add a container.
3. In the new container window, enter a **Name** for the container, and the **Public Access level**, click **Ok** to proceed.
4. Click on the new container, in the container window, select the required .vhd file and click **upload**.

Figure 386 *Selecting the container*

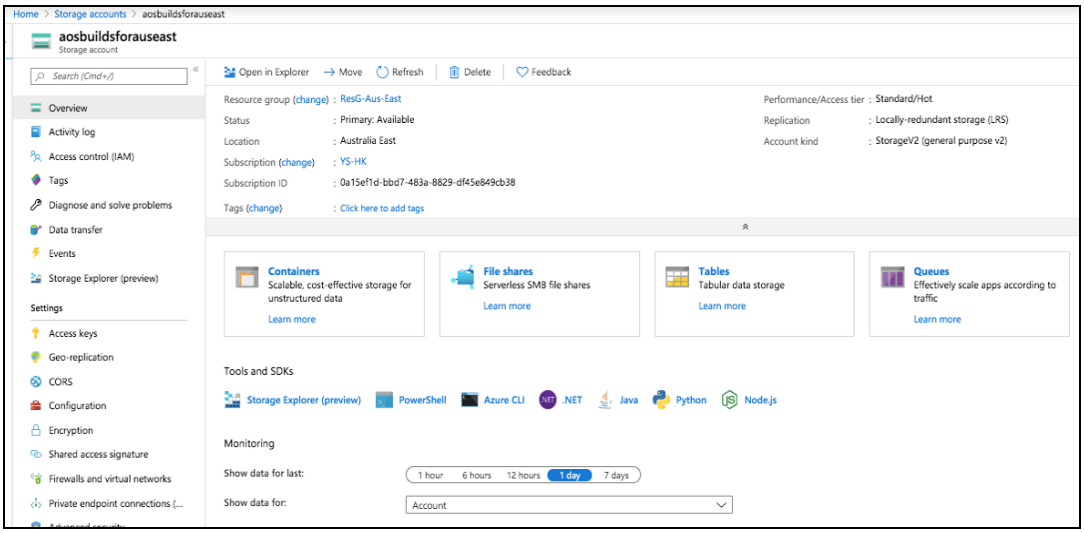


Figure 387 *Adding a new container*

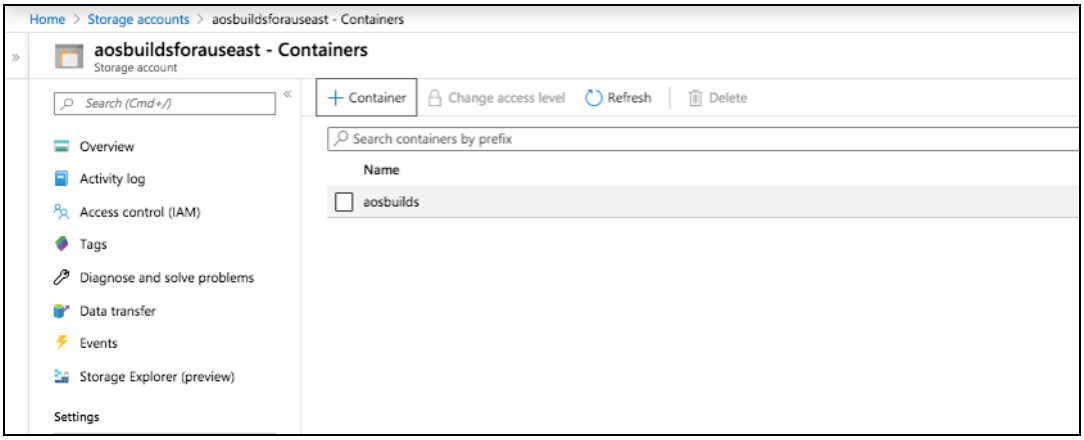
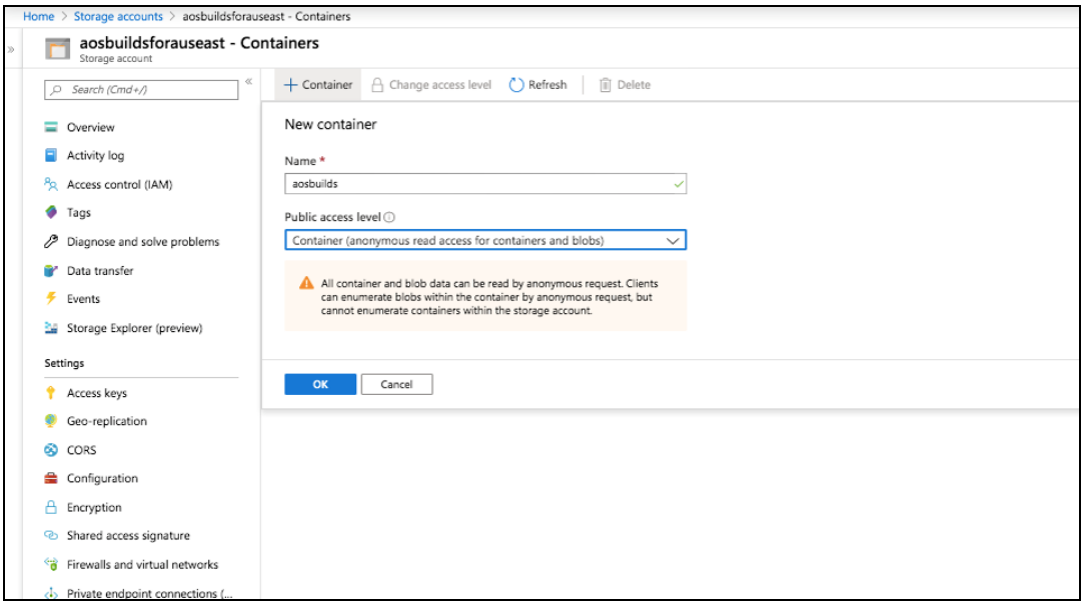


Figure 388 *Creating a new container*



Creating a VNET

The Azure VNETs enable you to securely connect your Azure resources with each other. You can use VNETs to provision and manage VPNs in Azure and, optionally link the VNets with other VNETs in Azure, or with your on-premises IT infrastructure to create hybrid or cross-premises solutions.

Deploying an Aruba Virtual Gateway in a customer VNET brings the SD-WAN fabric into the VNET and thus enables connectivity to physical sites, such as branches and data centers.

Azure deletes your VNETs when a subscription is disabled. If the subscription is re-enabled, you must recreate the resources.

The orchestration app creates 8/27 subnets, ensure that that the VNET has a /24 block reserved for the interconnect subnets.

If you do not have a VNET created in your Azure subscription, complete the following steps to bring up the VNET in Azure:

1. On the Azure portal, go to **Home** > **Networking** > **Virtual Networks**. You can also search for virtual network on the Home page to access the **Virtual Network** configuration page.
2. On the **Virtual Network** page, ensure that the selected deployment model is set as **Resource Manager**, and click **Create**. The **Create virtual network** page opens.
3. Configure the following parameters:
   - **Name**—Enter a name for the virtual network.
   - **Address space**—Enter the allocated address space details.
   - **Subscription**—Select a subscription.
   - **Resource group**— Select the resource group to which you want to attach the VNET.
   - **Location**—Select a valid location.
   - **Subnet**—Enter the following information:
   - **Name**—Name of the subnet.
   - **Address range**—Enter the address range for the subnet.
   - **DDoS Protection**(Optional)—Select either **Basic** or **Standard** based on your subscription plan.
   - **Service endpoints**(Optional)—Select either **Disabled** or **Enabled** based on your requirement. This is set to **Disabled** by default.
   - **Firewall**(Optional)—Select either **Disabled** or **Enabled** based on your requirement. This is set to **Disabled** by default.
4. Click **Create** to complete the creation of the virtual network.

Uploading the Aruba Virtual Gateway Software Image

To use the Aruba Gateway software image as the source for an Azure managed virtual disk, you must ensure that the Aruba Virtual Gateway software image is uploaded to a blob container in your storage account.

Aruba supports Azure VNET deployments on Virtual Gateway appliances running ArubaOS SD-WAN 8.5.0.0-2.0.0.0 or later software versions. To obtain access to a valid Virtual Harddrive (.vhd file) image for Virtual Gateways, contact your Aruba Sales Specialist.

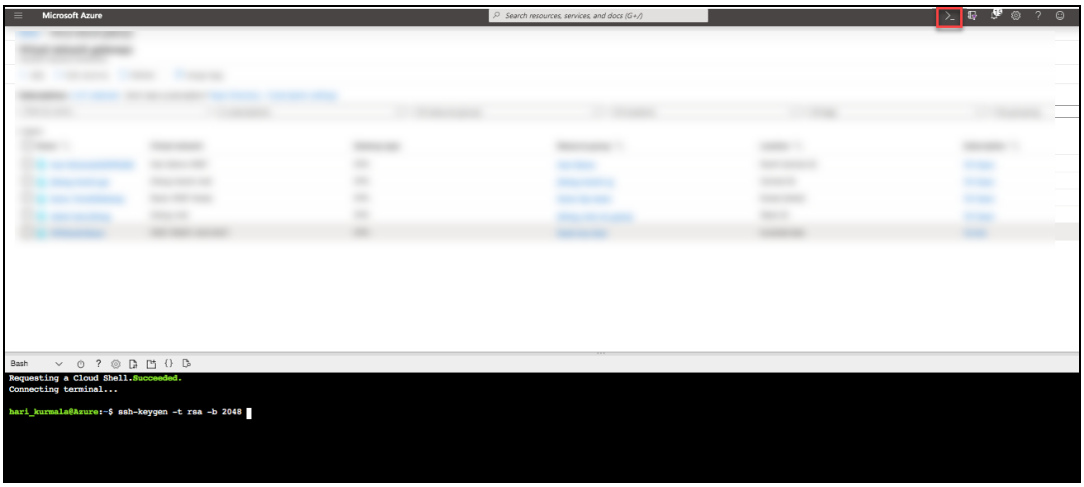
To upload the .vhd file, download and install the **Azure Storage Explorer** app. For more information, see Azure Storage Explorer.

Creating SSH keys

1. From the Azure portal, go to the Azure BASH Shell.
2. Create SSH key pair with the command ssh-keygen -t rsa -b 2048
3. Save the private key on your local machine to SSH into the Virtual Gateway
4. Save the public key and use it during the setup of the Virtual Gateway.

For more information see, Create and use an SSH public-private key pair for Linux VMs in Azure.

Figure 389 *Creating SSh Keys*

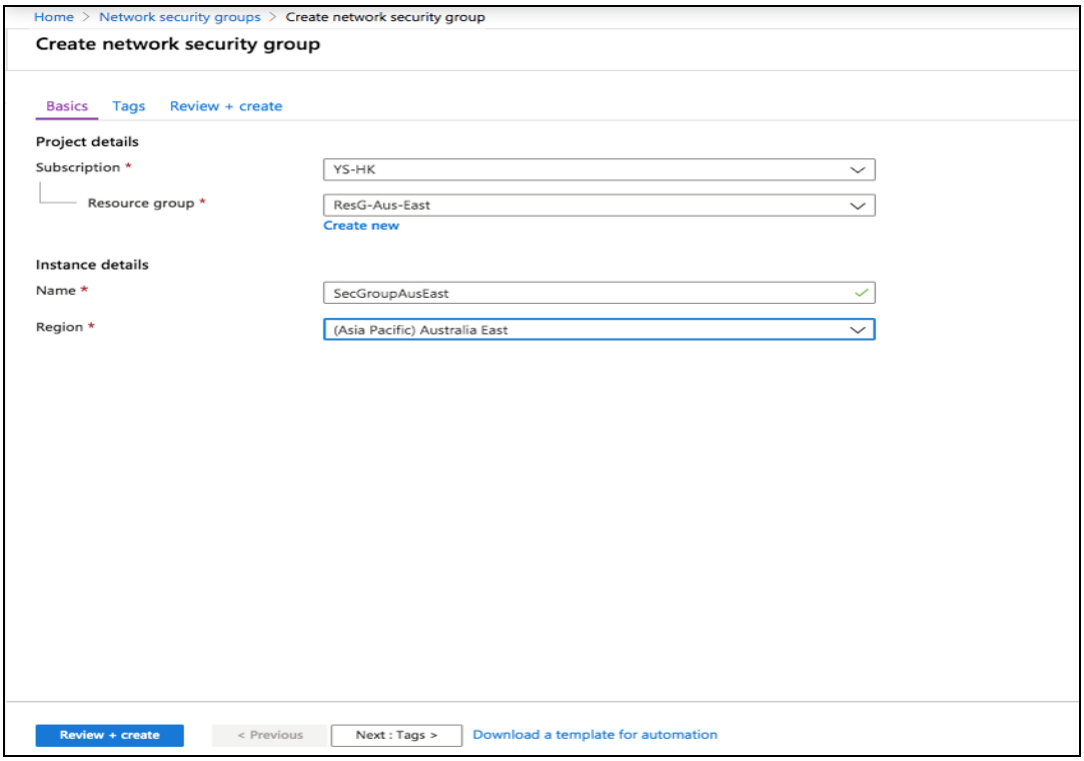


Creating a Security group

A network security group (NSG) in Azure is the way to activate a rule or access control list (ACL), which will allow or deny network traffic to your virtual machine instances in a virtual network. NSGs can be associated with subnets or individual virtual machine instances within that subnet.

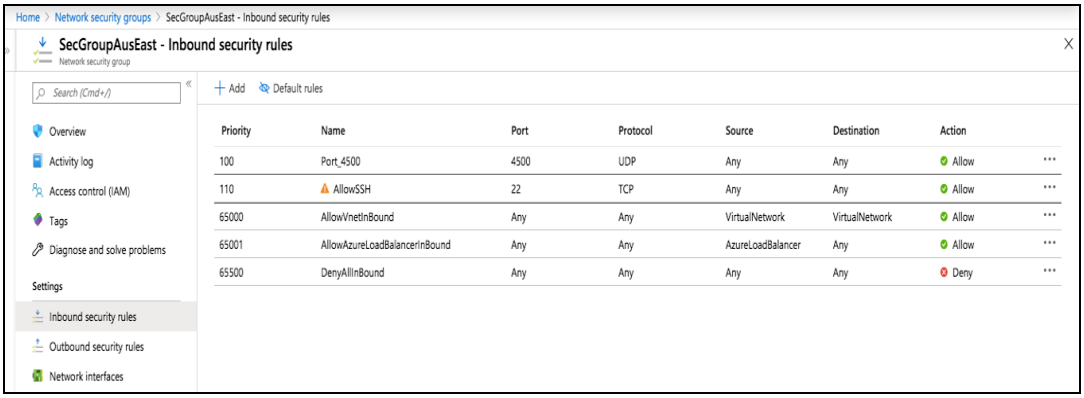
1. On the Azure portal, go to Home > Networking security groups, click + to start the creating the NSG.
2. In the Basics tab, enter the Subscription and Resource group that this NSG is linked to, also provide a unique Name and the Region for the NSG. Click Review + Create to proceed.

Figure 390 *Creating Security group*



3. On the Azure portal, go to Home > Networking security groups, click the NSG that was created.
4. Select Inbound security rules and click +Add. In the Basic tab, add UDP port 4500 in the Destination port ranges to allow incoming IKE connection from Branch Gateways.
5. Select Inbound security rules and click +Add. In the Advanced tab, add SSH port 110 as a Priority to allow incoming SSH connections.

Figure 391 *Security group summary*



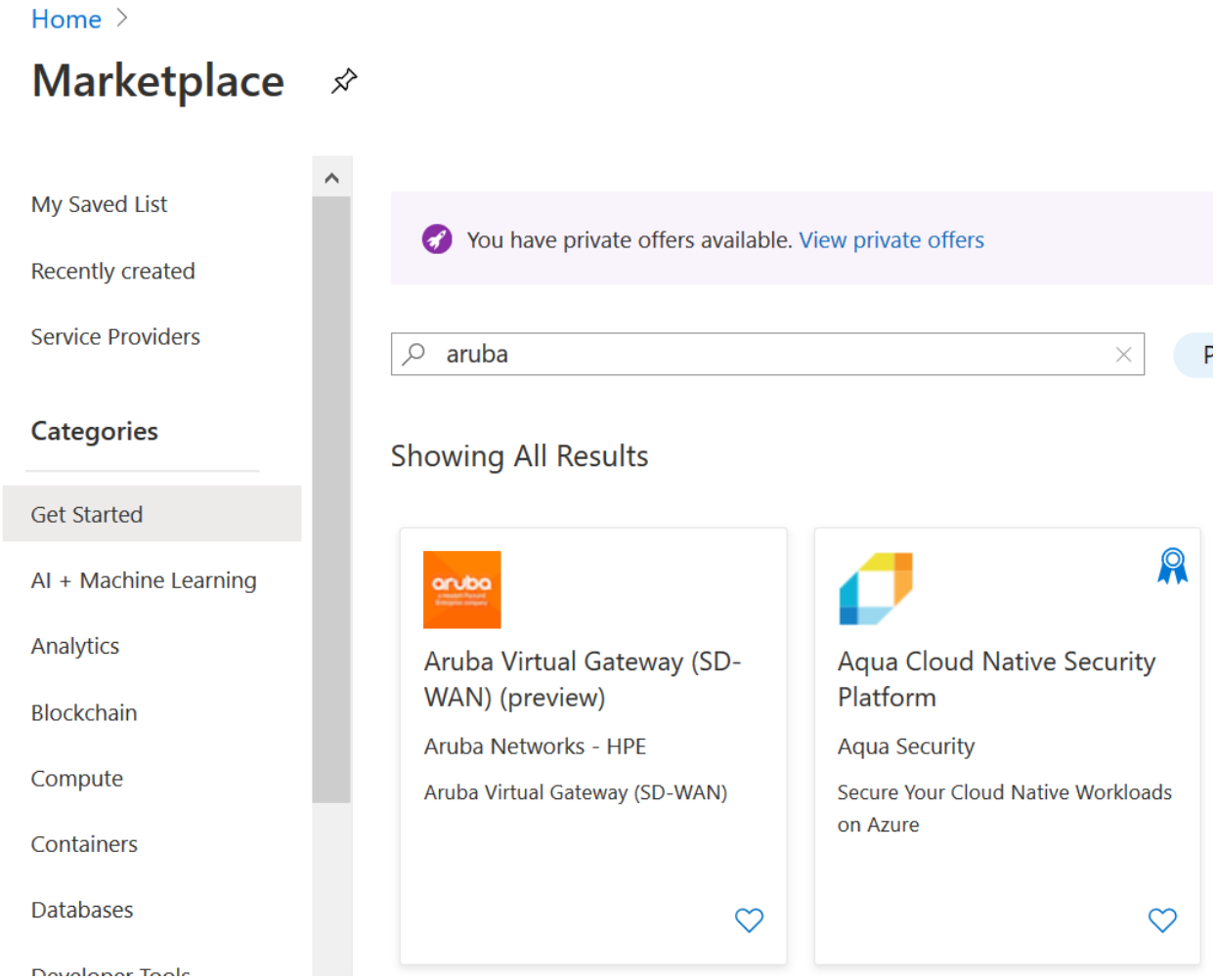
Enabling Aruba Virtual Gateway Subscription in Azure Marketplace

Aruba Virtual Gateway is available in the Azure Marketplace as a limited or private listing to host images. To enable the Aruba Virtual Gateway subscription in Azure Marketplace, complete the following steps:

1. Log in to the Azure portal.
2. In the search bar, type **Marketplace**.
3. Marketplace is listed under Services.

4. Click **Marketplace**.
5. In the **Search the Marketplace** search bar, type **Aruba Virtual Gateway**, and click the Aruba Virtual Gateway listing.

Figure 392 *Searching Aruba Virtual Gateway Listing*

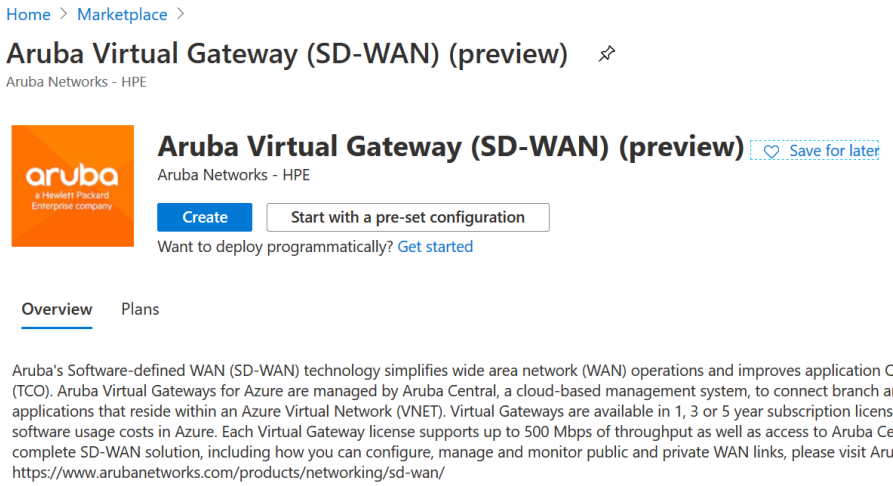


6. Under **Aruba Virtual Gateway (SD-WAN) (preview)** page, click **Create**.

NOTE

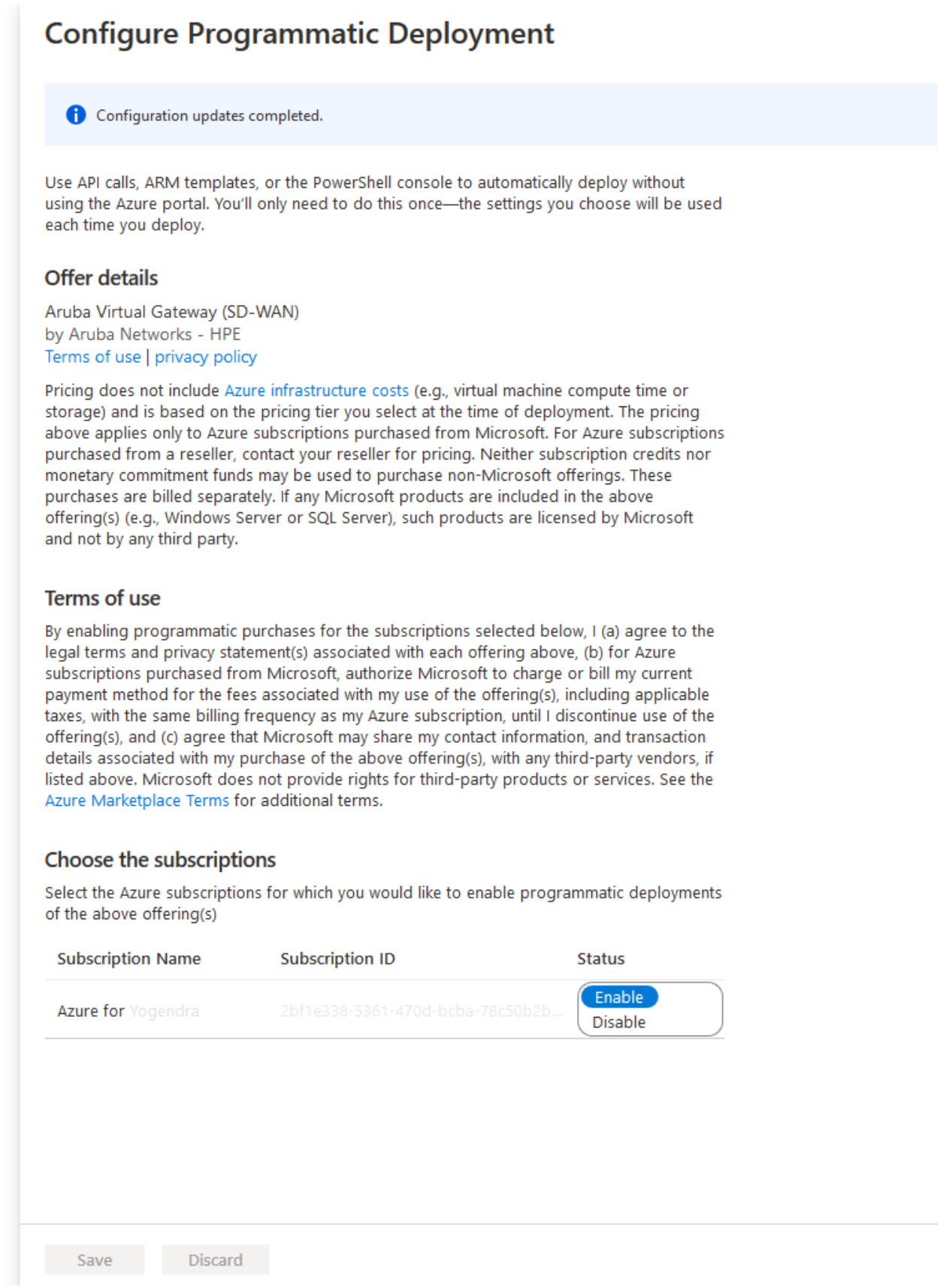
To add interfaces, click **Start with a pre-set configuration**, go to Azure portal, stop the VM, add existing interfaces, and restart VM.

Figure 393 *Aruba Virtual Gateway (SD-WAN) (preview)*



7. In **Configure Programmatic Deployment** page, under **Choose the subscriptions**, click **Enable**.

Figure 394 *Enabling Aruba Virtual Gateway Subscription*



8. Click **Save**.

Adding a Cloud Provider Account in Aruba Central

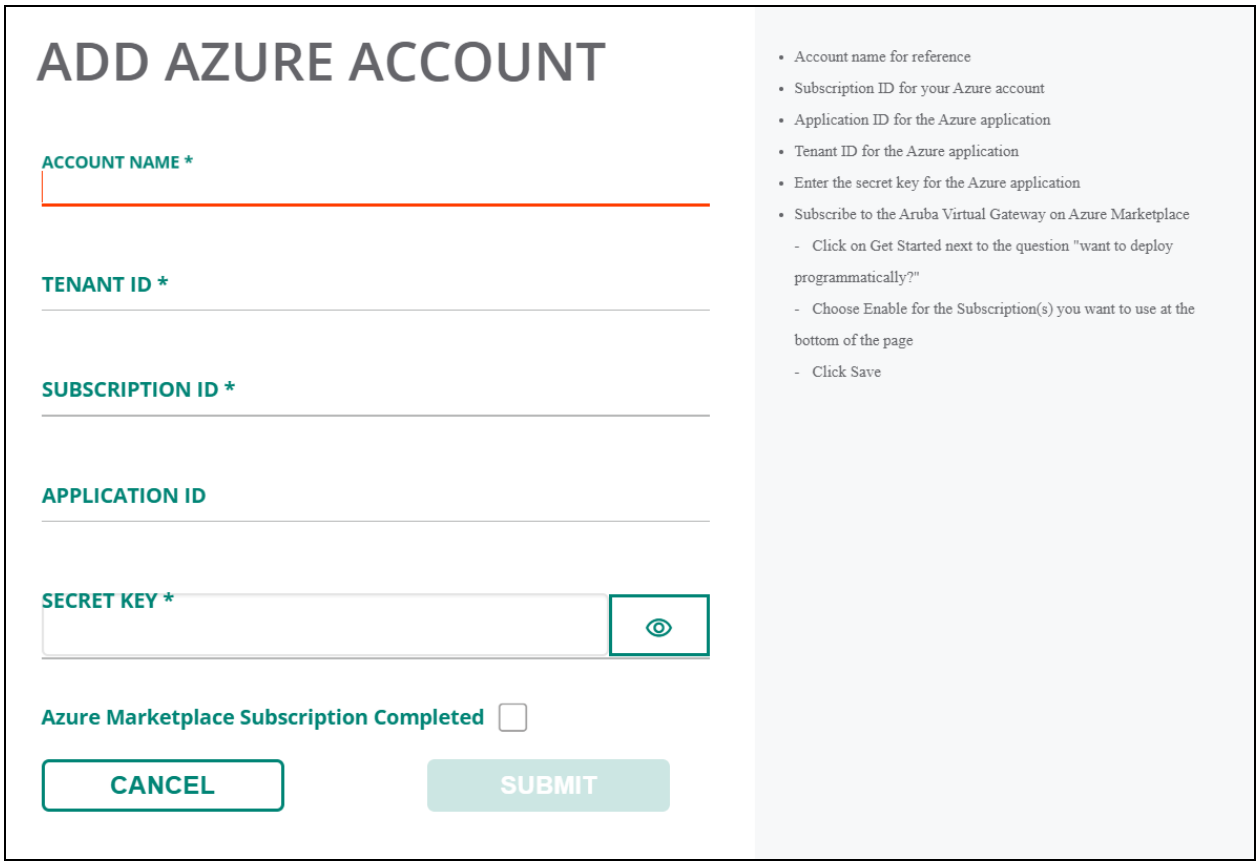
To deploy Virtual Gateway instances in a customer's VNET, you must create a cloud provider account in Aruba Central and map it to the customer's Azure account where the VNET is deployed.

1. Log in to Aruba Central.
2. In the **Network Operations** app, set the filter to **Global**.
3. Under **Manage**, click **Network Services** > **Virtual Gateways**> **Orchestrated**, to view the summary page for orchestrated Virtual Gateways with following columns:
   - **Cloud Provider**—Displays the name of the Cloud Provider.
   - **Account**—Displays the account name of the deployed Virtual Gateway.
   - **Region**—Displays the name of the location where the Virtual Gateway is deployed.
   - **VGW Serial**—Displays the serial number of the Virtual Gateway.
   - **VGW Public IP**—Displays the public IP address of the Virtual Gateway.
   - **High Availability**—Displays the High Availability mode (Active or Passive) of the Virtual Gateway.
   - **Orchestration**—Displays the status of the Virtual Gateway orchestration.
   - **VM Status**—Displays the status (Up, Down, or Stopped) of the Virtual Machine.
   - **VGW Status**—Displays the status of the deployed Virtual Gateway.
4. Click the **Config** icon to open the **Add Cloud Provider Accounts** page in the **Accounts** tab.
5. To add an account, select **Microsoft Azure** from the drop-down options and click **Add Account**.
6. In the **Add Azure Account** window, enter these details:
   - **Account Name**—Enter an account name for easy identification.
   - **Tenant ID**—Enter the Tenant ID from the Azure application.
   - **Subscription ID**—Enter the subscription ID for your Azure account.
   - **Application ID**—Enter the Azure Application ID. In the future, to edit this Azure account the Application ID will be needed. The Application ID can remain the same.
   - **Secret Key**—Enter the secret key for the Azure application. In the future, to edit this Azure account the Secret Key will be needed. This Secret Key will be different from the one that is used currently.
   - **Azure Marketplace Subscription Completed**—Enable this option after subscribing to Azure Marketplace Subscription in Azure console.

   Aruba Virtual Gateway is available in the Azure Marketplace as a limited or private listing to host images. Clicking on the listing deploys the hosted image using Virtual Gateway orchestration.

The **Tenant ID, Subscription ID, Application ID**, and **Secret Key** are information that were saved during the App creation process.

Figure 395 *Adding an Azure account*

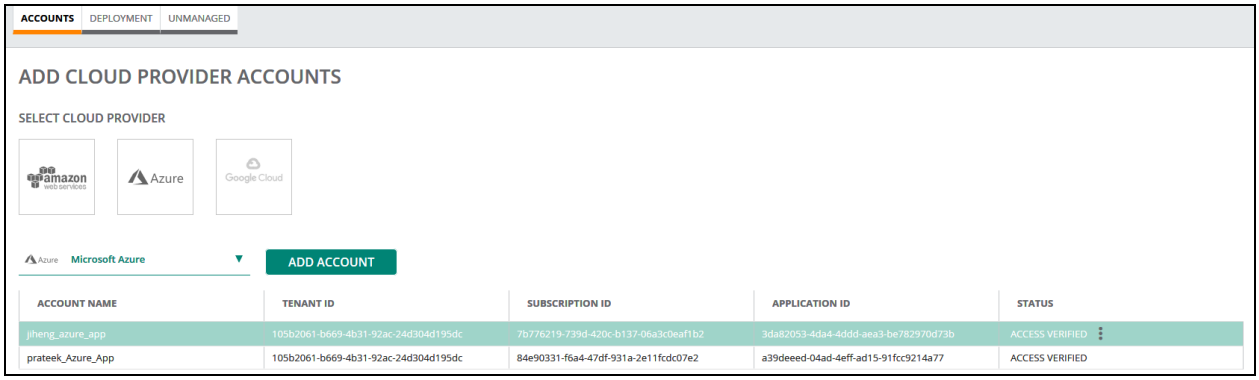


7. Click **Submit**. The account is added to list of accounts on the **Accounts** page.
8. Verify the status of the account. If the status column for the account is shown as **Access Verified**, proceed to deploy the Virtual Gateway instance.

NOTE

To edit or delete an account, select the account, and click the setting icon in the **Status** column to open the **Account Options** window.

Figure 396 *Reviewing the cloud provider accounts*



If the Azure account in Aruba Central displays an Access Denied error message, check the following details:

- Ensure that the VNET is configured and available present in your Azure account.
- Ensure that the subnet configured for the VNET is larger than /24.
- Ensure that the Subscription ID, Tenant ID, App ID, and Client Secret are correct.

Deploying the Virtual Gateway

To deploy a Virtual Gateway, complete the following steps:

1. On the **Virtual Gateways** page, select the **Deployment** tab and choose **Microsoft Azure** from the drop down menu and click on **Import VNETs** to ensure that the information is refreshed and up to date.
2. Select the region to host the virtual gateway, and click **Deploy Virtual Gateway**.
3. In the **Create Virtual Gateway** page update the fields listed here:
   - **Virtual Gateway Subnet**—Enter the gateway subnet
   - **Virtual Gateway Size**—Enter the virtual gateway SKU (currently limited to VGW-500MB)

The Virtual Gateway Size also displays the total number of licenses and the number of available licenses.

- **Azure Instance Type**—Enter the Azure instance type (currently limited to Standard_DS3_v2)
- **Marketplace Image**—Choose this option to select the ArubaOS image to be installed in Azure Marketplace. When this option is enabled, **Select Image** is automatically updated with the ArubaOS image to be installed in Azure Marketplace.
- **Private Image**—Choose this option to select a private ArubaOS image.
- **Select Image**—Displays the ArubaOS image to be installed.
- **SSH Public Key**—Enter the SSH key. For more information on creating the SSH key, see Create and use SSH keys in Azure.
- **Security Group (optional)**—Enter the Security Group details
- **Edge VNET**—Choose this option to enable or disable Edge VNET. When Edge VNET is enabled, the Virtual Gateways are deployed in an active-active high availability mode. All the Branch Gateways are connected to both Virtual Gateways. The Virtual Gateways in-turn connect to the VNETs through the Azure vHub Gateways, where the vHub Gateways are responsible for interconnecting all the VNETs.

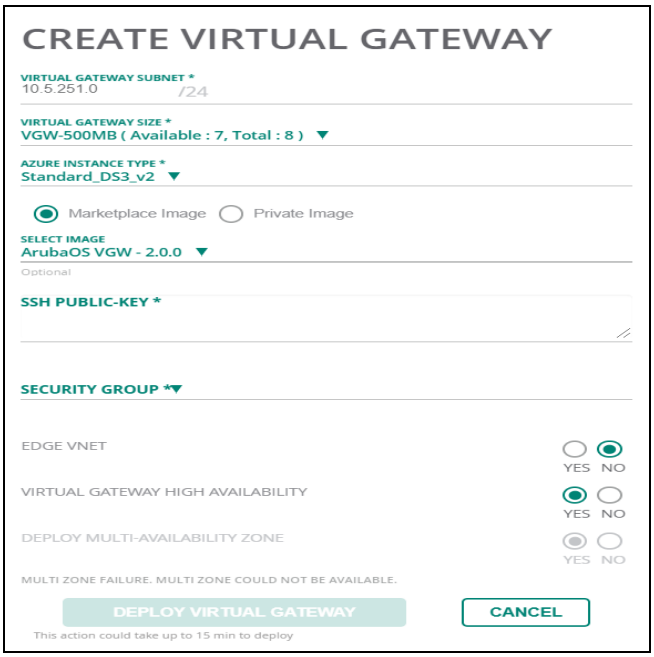
When Edge VNET is enabled, Connect/Disconnect Subnet option for VPC will be disabled.

- **Virtual Gateway High Availability**—Choose if this virtual gateway supports **High Availability**.
- **Deploy Multi-Availability Zone**—Select **Yes** if the virtual gateway will be available across multiple regions.

When Edge-VNET is enabled, this configuration option is disabled by default.

4. Click **Deploy Virtual Gateway** to initiate the virtual gateway deployment.

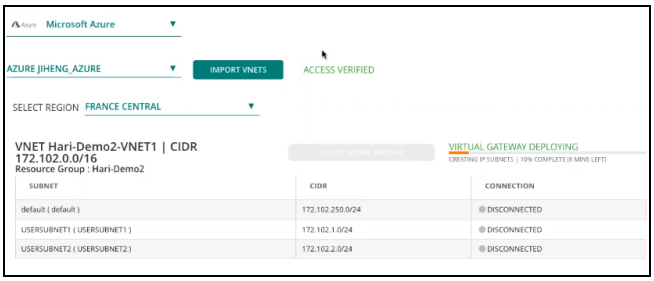
Figure 397 *Creating a virtual gateway*



NOTE

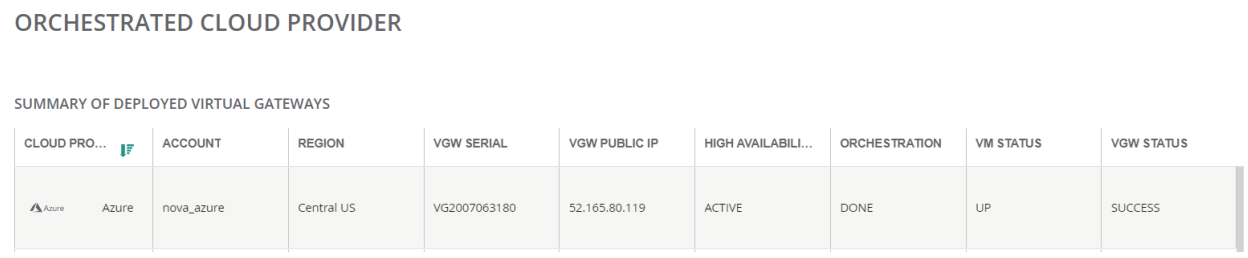
The Virtual Gateway deployment can take approximately 15 minutes to complete.

Figure 398 *Deploying the virtual gateway*



After the deployment is completed, **Virtual Gateway Deployed** message is displayed. A summary of the deployment is also displayed on the **List** view of the **Orchestrated Cloud Provider** page. Hovering the cursor over any of the columns displays additional information about the field.

Figure 399 *Summary of deployed virtual gateways*



NOTE

The Virtual Gateway deployment can take approximately 15 minutes to complete.

Licensing Confirmation

Ensure that the license is valid, for more information, see Assigning Subscriptions to Aruba Gateways.

Verifying the Deployment Status

To verify the Virtual Gateway deployment status, complete the following checks:

- Check if the Virtual Gateway is on-boarded to the device inventory in Aruba Central .
- Ensure that the Virtual Gateway is assigned to a device configuration group in Aruba Central.
- Verify if the Virtual Gateway is connected to Aruba Central.
- Configure a VPN tunnel between a Branch Gateway and the Virtual Gateway.
- In the Network Operations app, set the filter to Global and navigate to **Manage > Network Services > Virtual Gateways**. A summary of the deployment is displayed in the **List** view of the **Orchestrated Cloud Provider** page with the following columns:
- **Cloud Provider**—Displays the name of the cloud provider.
- **Account**—Displays the account name configured during the Virtual Gateway account creation.
- **Region**—Displays the region where the Virtual Gateway is deployed.
- **VGW Serial**—Displays the serial number of the Virtual Gateway.
- **VGW Public IP**—Displays the public IP address of the Virtual Gateway.
- **High Availability**—Displays the status of the High Availability mode for the deployed Virtual Gateway.
- **Orchestration**—Displays the orchestration status for the deployed Virtual Gateway.
- **VM Status**—Displays the VM status of the Virtual Gateway.
- **VGW Status**—Displays the status of the Virtual Gateway.

The **Device Inventory** page displays the devices that are in the inventory. Click the  to access the **Account Home** > **Device Inventory**.

After a successful deployment, the Virtual Gateway instances launch and connects to Aruba Central with the latest image.

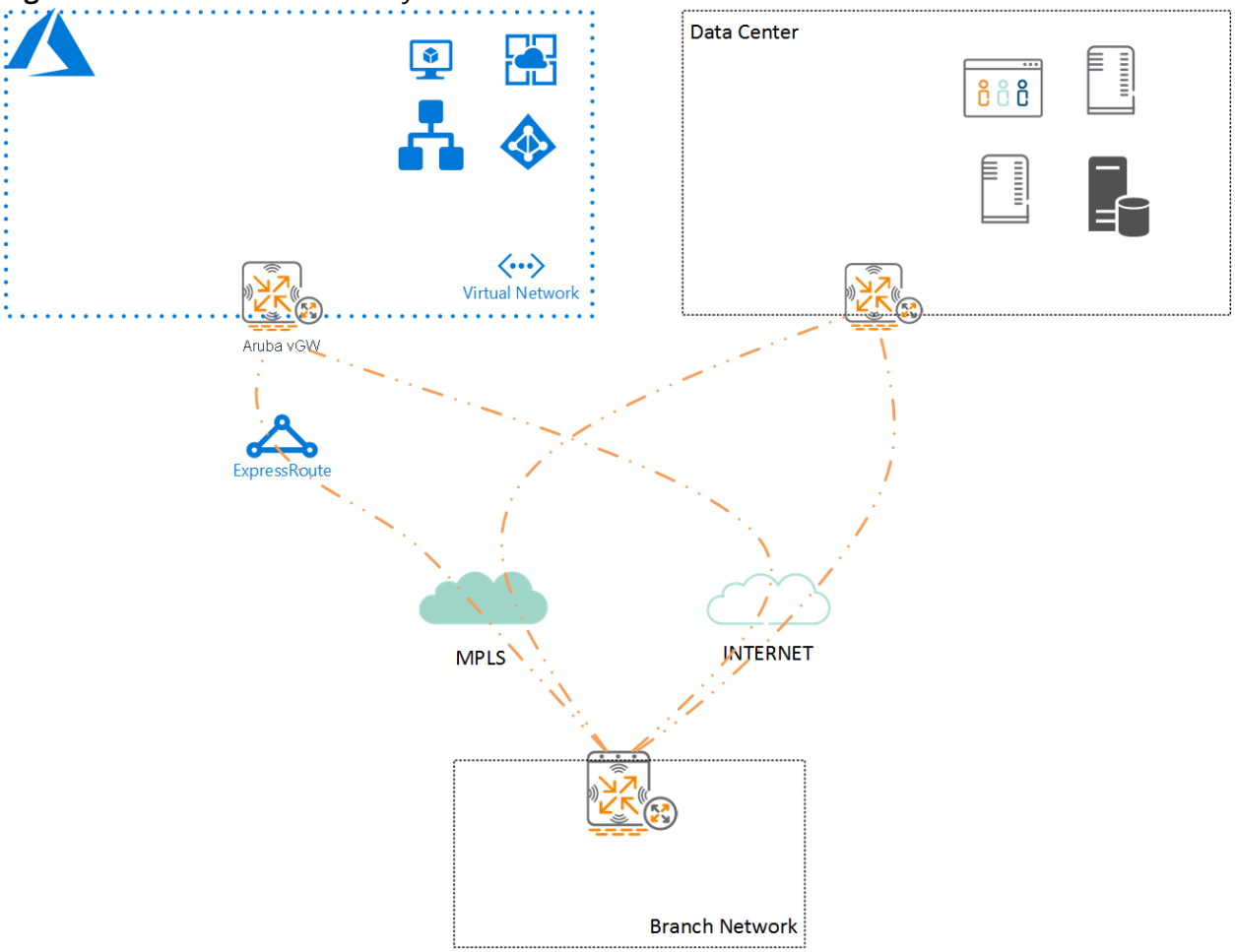
Deploying Aruba Virtual Gateway in Microsoft Azure (Unmanaged Mode)

Aruba Virtual Gateways can now be deployed in Microsoft Azure to create a secure SD-WAN overlay between physical sites and private virtual networks (VNETs) hosted in public cloud environments. Aruba Branch Gateways will establish tunnels to the Virtual Gateways both though the Internet as well as through the ExpressRoute communications between the customer's private network and Azure. This effectively results in bringing Azure VNETs into the SD-WAN fabric, ensuring that workloads hosted there will be easily accessible from branches as well as data centers.

An Azure VNET is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. Each VNET you create has its own CIDR block, and can be linked to other VNETs and on-premises networks as long as the CIDR blocks do not overlap. For more information on VNETs, see Azure documentation.

The following figure illustrates the communication flow between Aruba Gateways, SD branch network, and data centers:

Figure 400 *Aruba Virtual Gateway in Azure VNET*



Deployment Procedure

Before deploying Aruba Virtual Gateway deployment in Azure VNET, ensure that you have the following resources and account privileges:

- A valid subscription and administrator credentials to access your Azure account.
- A valid subscription and Aruba Central account credentials to deploy Virtual Gateways.
- Aruba Virtual Gateway VHD image.

NOTE

You can configure and set up an Aruba Virtual Gateway in Microsoft Azure using either the Azure Cloud Shell or the Azure graphical user interface (UI). The configuration steps described in this document are based on the UI workflows.

NOTE

Aruba supports deploying Virtual Gateways in the unmanaged mode. In the unmanaged mode, the administrators deploy the Virtual Gateway instance in the Azure portal and then onboard it into Aruba Central as a managed device.

To deploy the Virtual Gateways in the Azure VNET, complete the following steps:

1. Creating a Resource Group
2. Creating a Storage Account
3. Creating a VNET
4. Creating a Network Security Group
5. Creating Security Rules
6. Configuring Subnets
7. Creating Network Interfaces
8. Uploading the Aruba Virtual Gateway Software Image
9. Creating Image and Data Disk
10. Setting up a Virtual Machine
11. Creating SSH Key Pairs
12. Generating User Data in Aruba Central
13. Verifying the Deployment Status

Creating a Resource Group

A resource group in Azure is a logical container that consists of resources required for deploying a virtual machine (VM). Resource groups allow you to logically group related resources such as storage accounts, virtual networks, VMs, and also deploy and manage these resources as a single entity.

Note the following important points about resource groups in Azure:

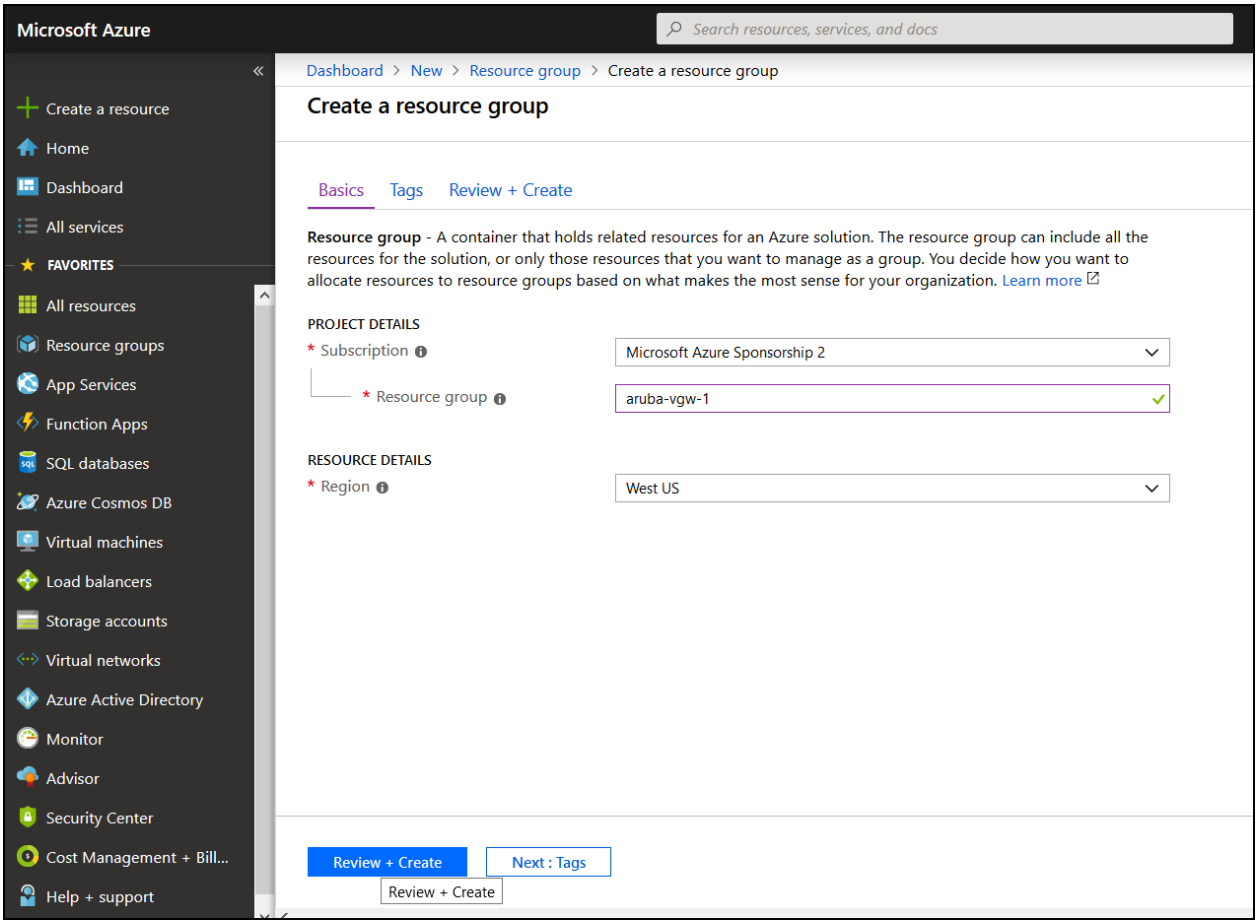
- A resource group can contain resources from different regions or locations.
- Access control for administrative actions can be scoped with a resource group.
- Resources can be added or removed from a group at any time.
- Resources can be moved from one group to another group.
- Each resource can only exist in one resource group.
- Resources can interact with other resources group containers.

To verify if your subscription has a resource group, click **Home** > **Resource Groups**.

If you do not have a resource group created in your Azure subscription, complete the following steps to create a resource group:

1. Log in to Azure portal using your Azure account credentials.
2. Click **+ Create a Resource** to access Dashboard and then search for Resource Groups in the search box to access the **Resource Groups** configuration page.
3. Click **Create**.
4. In the **Basics** tab, enter the following information:
   - **Subscription**—Select your Microsoft Azure subscription.
   - **Resource group name**—Enter a name for the resource group.
   - **Region**—Select the geographic location for the resource group.
5. Click **Review+Create** and then click **Create**.

Figure 401 *Creating a Resource Group*



Creating a Storage Account

Storage account in Azure provides a unique namespace to store and access your Azure storage objects. Every storage account must belong to an Azure resource group.

For Aruba Virtual Gateway deployments, you will need a storage account to store the software image and also a separate storage account for Boot Diagnostics. The Boot Diagnostics option allows you to view logs pertaining to VM boot issues. You can enable the Boot Diagnostics option when configuring a VM.

If you do not have a storage account created and mapped to the resource group that you want to use for Aruba Virtual Gateway deployment, complete the following steps:

1. Log in to your Azure account.
2. Select **Home** > **Storage** > **Storage Accounts**.
3. On the **Storage Accounts** window, click **Add**.
4. Choose a subscription that you want to map to the storage account.
5. Enter the **Resource group** name that will be associated with this storage account.
6. Enter a unique name for your storage account.

NOTE

The name must be between 3 and 24 characters in length, and can include numbers and lowercase letters.

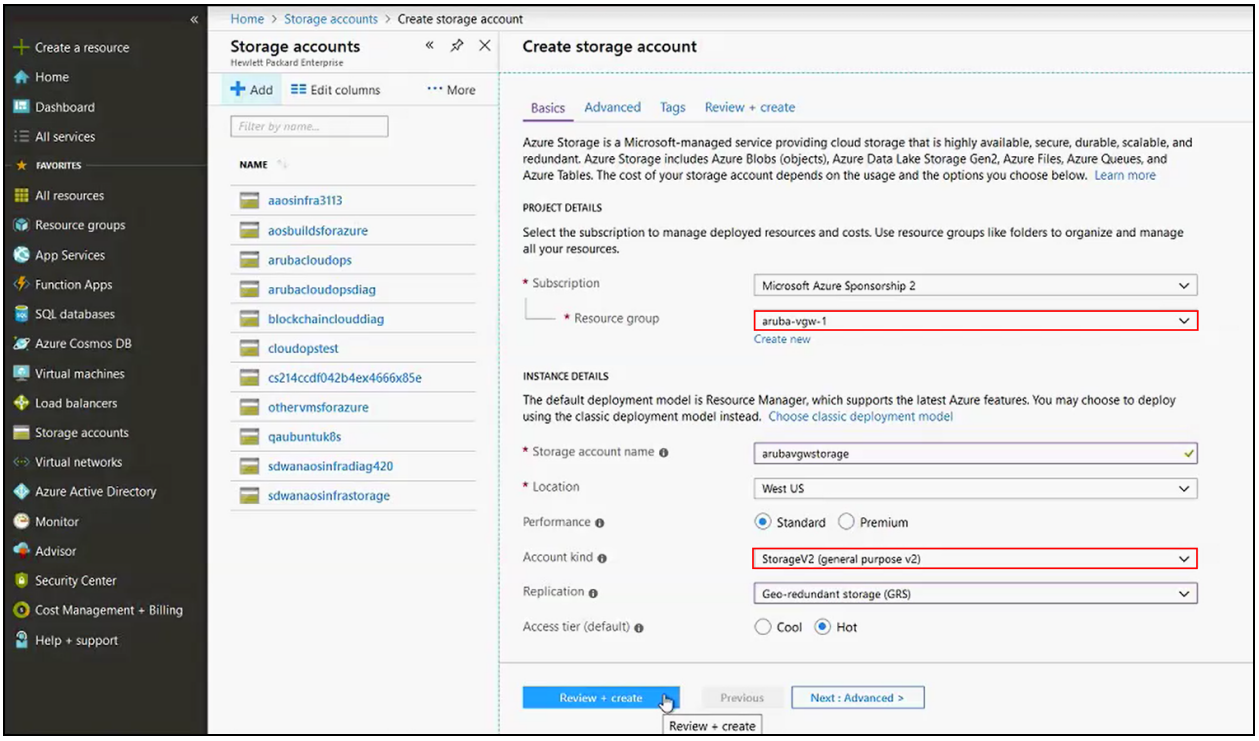
7. Select a location for your storage account.
8. Ensure that the values for remaining fields are defined as shown in the following table:

Table 296: *Storage Account Configuration Parameters*

Field	Value
Performance	Standard
Account kind	StorageV2 (general-purpose v2). **NOTE:** A general-purpose v2 storage account provides access to all of the Azure Storage services, such as blobs, files, queues, tables, and disks.
Replication	Geo-redundant storage (GRS)
Access tier	Hot

9. Click **Review + Create** and then click **Create**.

Figure 402 *Review + Create the Storage Account*



Creating a VNET

The Azure VNETs enable you to securely connect your Azure resources with each other. You can use VNETs to provision and manage VPNs in Azure and, optionally, link the VNets with other VNETs in Azure, or with your on-premises IT infrastructure to create hybrid or cross-premises solutions.

Deploying an Aruba Virtual Gateway in a customer VNET brings the SD-WAN fabric into the VNET and thus enables connectivity to physical sites, such as branches and data centers.

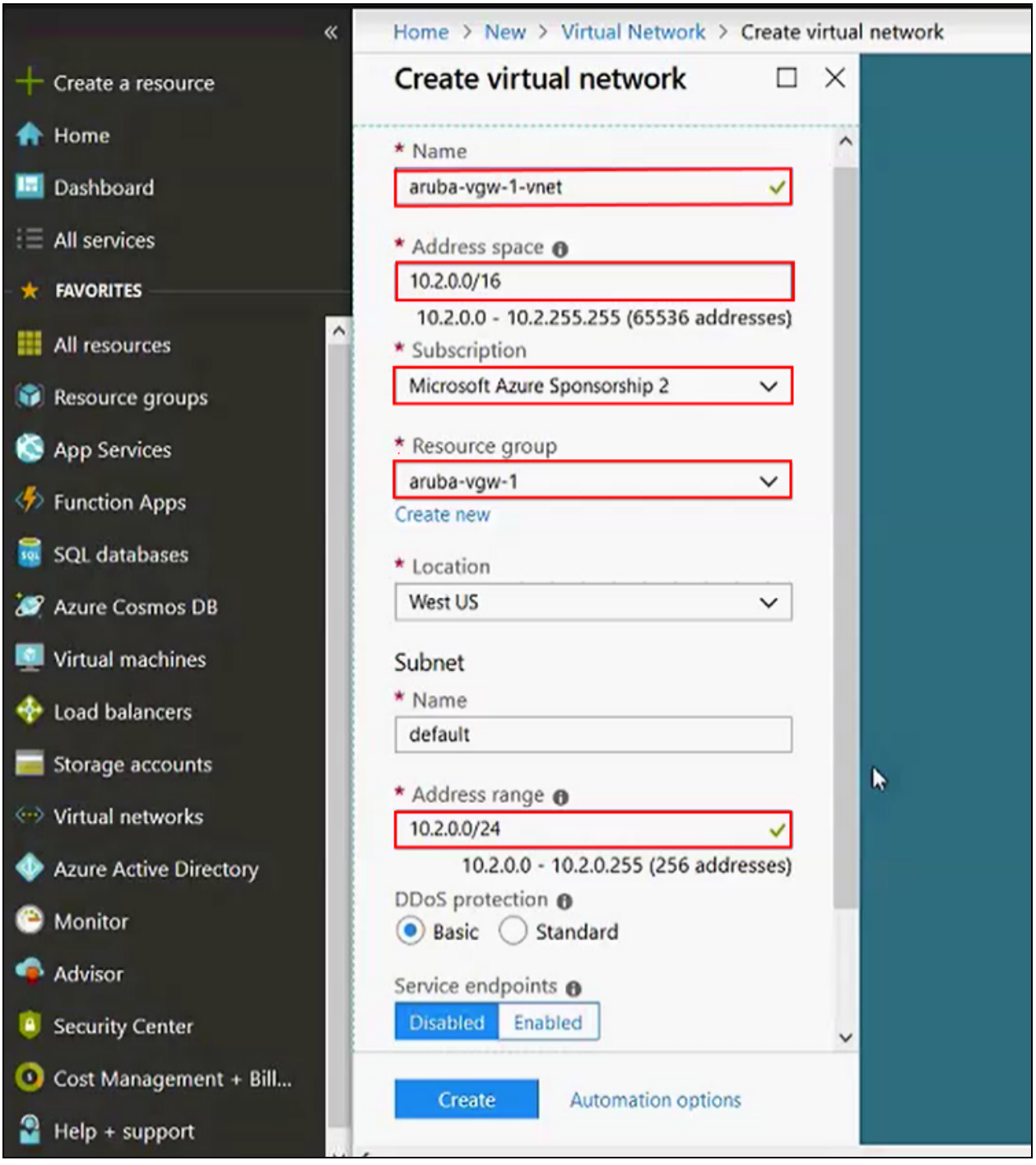
NOTE

Your VNETs are automatically deleted by Azure when a subscription is disabled. If the subscription is re-enabled, you must re-create the associated resources.

If you do not have a VNET created in your Azure subscription, complete the following steps to bring up the VNET in Azure:

1. On the Azure portal, go to **Home** > **Networking** > **Virtual Networks**. You can also search for virtual network on the Home page to access the **Virtual Network** configuration page.
2. On the **Virtual Network** page, ensure that the selected deployment model is set as **Resource Manager**, and click **Create**. The **Create virtual network** page opens.
3. Configure the following parameters:
   - **Name**—Enter a name for the virtual network.
   - **Address space**—Enter the allocated address space details.
   - **Subscription**—Select a subscription.
   - **Resource group**— Select the resource group to which you want to attach the VNET.
   - **Location**—Select a valid location.
   - **Subnet**—Enter the following information:
     - **Name**—Name of the subnet.
     - **Address range**—Enter the address range for the subnet.
   - **DDoS Protection**(Optional)—Select either **Basic** or **Standard** based on your subscription plan.
   - **Service endpoints**(Optional)—Select either **Disabled** or **Enabled** based on your requirement. This is set to **Disabled** by default.
   - **Firewall**(Optional)—Select either **Disabled** or **Enabled** based on your requirement. This is set to **Disabled** by default.
4. Click **Create** to complete the creation of the virtual network.

Figure 403 *Creating a VNET*



Creating a Network Security Group

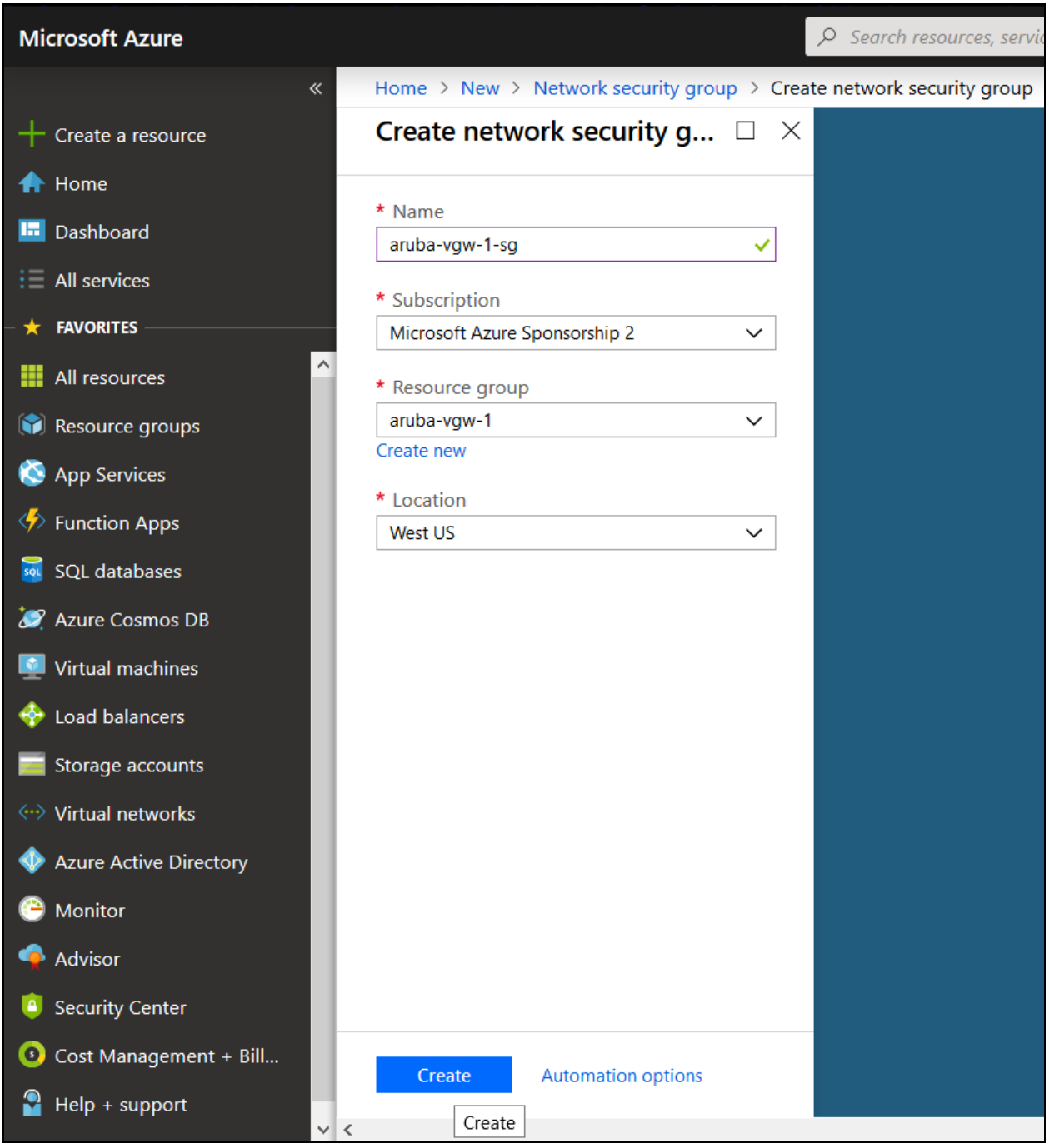
Using a network security group you can filter network traffic to and from Azure resources in an Azure VNET. A network security group is made up of security rules that allow or deny inbound traffic to, or outbound network traffic from, several types of Azure resources.

The number of network security groups that you can create for a VNET may vary based your location and your subscription plan. For more information, see *Microsoft Azure documentation*.

To create a network security group, complete the following steps:

1. Go to **Home** > **Networking** > **Network Security Group**. You can also use the search box on the **Home** page to access the **Network Security Group** configuration page.
2. On the **Network security group** page, ensure that the selected deployment model is set as **Resource Manager**, and then click **Create**. The **Create network security group** page opens.
3. Configure the following parameters:
   - **Name**—Enter a name for the network security group.
   - **Subscription**—Select a subscription.
   - **Resource group**— Select the resource group to which you want to map the network security group.
   - **Location**—Select your Azure location.
4. Click **Create**.

Figure 404 *Creating a Network Security Group*



Creating Security Rules

Security rules allow you to filter inbound and outbound network traffic that traverses through a VNET. When a network security group is created, several default rules are created. Default security rules cannot be deleted, but can be overridden with rules of a higher priority.

For Aruba Virtual Gateway deployment, you will need to create security rules to allow inbound traffic through UDP port 4500 for incoming IPsec tunnels. Similarly if you want to allow SSH traffic into the VPNC, you can create a rule to open port 22 for incoming traffic

To configure inbound security rules for the network security group associated with your VNET, complete the following steps:

1. Select the network security group that you just created for your VNET.
2. In the **Settings** list, select **Inbound security rules** and then click **+Add**. The **Add inbound security rule** pane opens.
3. Add a security rule for UDP port 4500 as described in the following table:

Table 297: *Security Rules*

Setting	Rule Parameters for UDP 4500
Source	Any
Source port ranges	*
Destination	Any
Destination port ranges	4500
Protocol	UDP
Action	Allow
Name	Port_4500
Description	4500 incoming

Figure 405 illustrates the procedure for creating an inbound security rule for the UDP port 4500:

Figure 405 *Adding Inbound Security Rules*

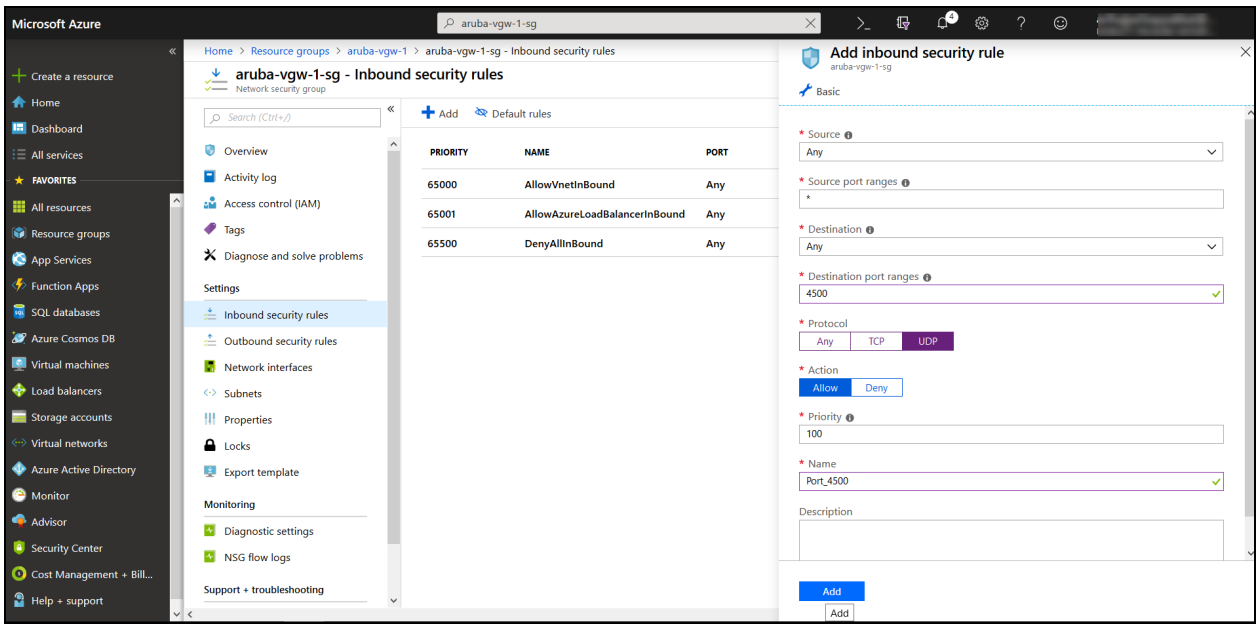
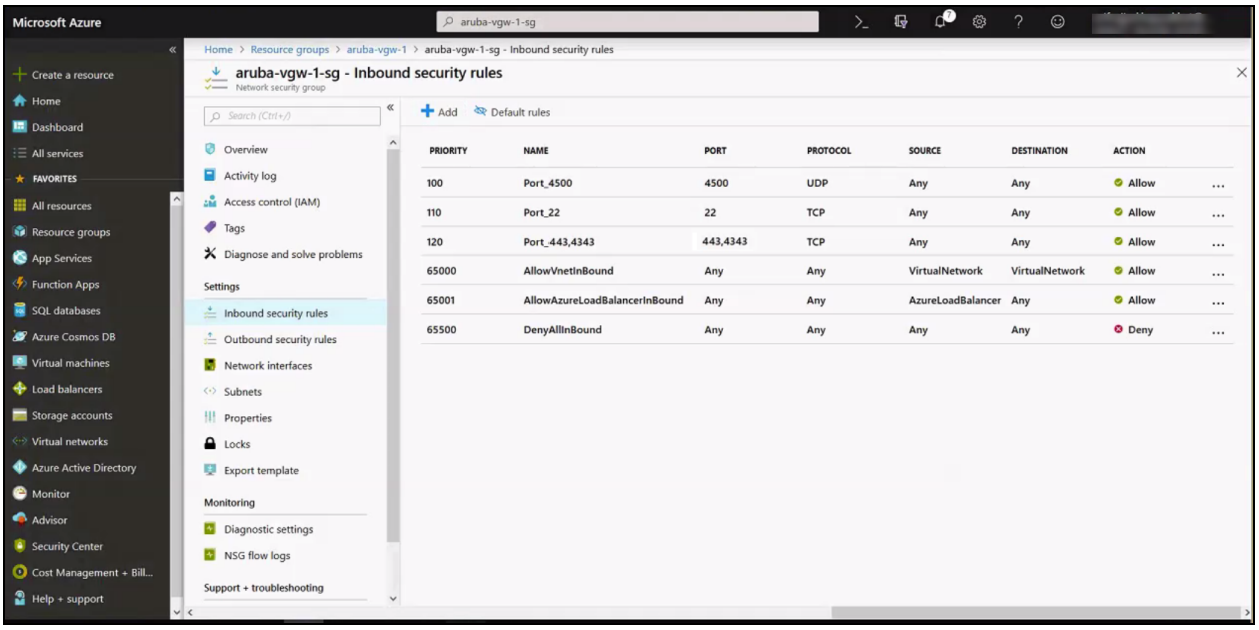


Figure 406 shows the inbound security rules created for the network security group for the Aruba Virtual Gateway deployment:

Figure 406 *Inbound Security Rules*



Configuring Subnets

An Azure VNET requires a specific subnet called the gateway subnet. Gateway subnet is required for configuring a virtual network gateway. Gateway subnet allocates a set of IP addresses that the virtual network gateway resources and services can use.

Apart from configuring the gateway subnet, you must also configure separate interconnection subnets for all network interfaces of Aruba Virtual Gateway. The interconnection subnets allow Aruba Virtual Gateway to connect to all relevant resources in a VNET.

The following procedures describe the steps for creating subnets:

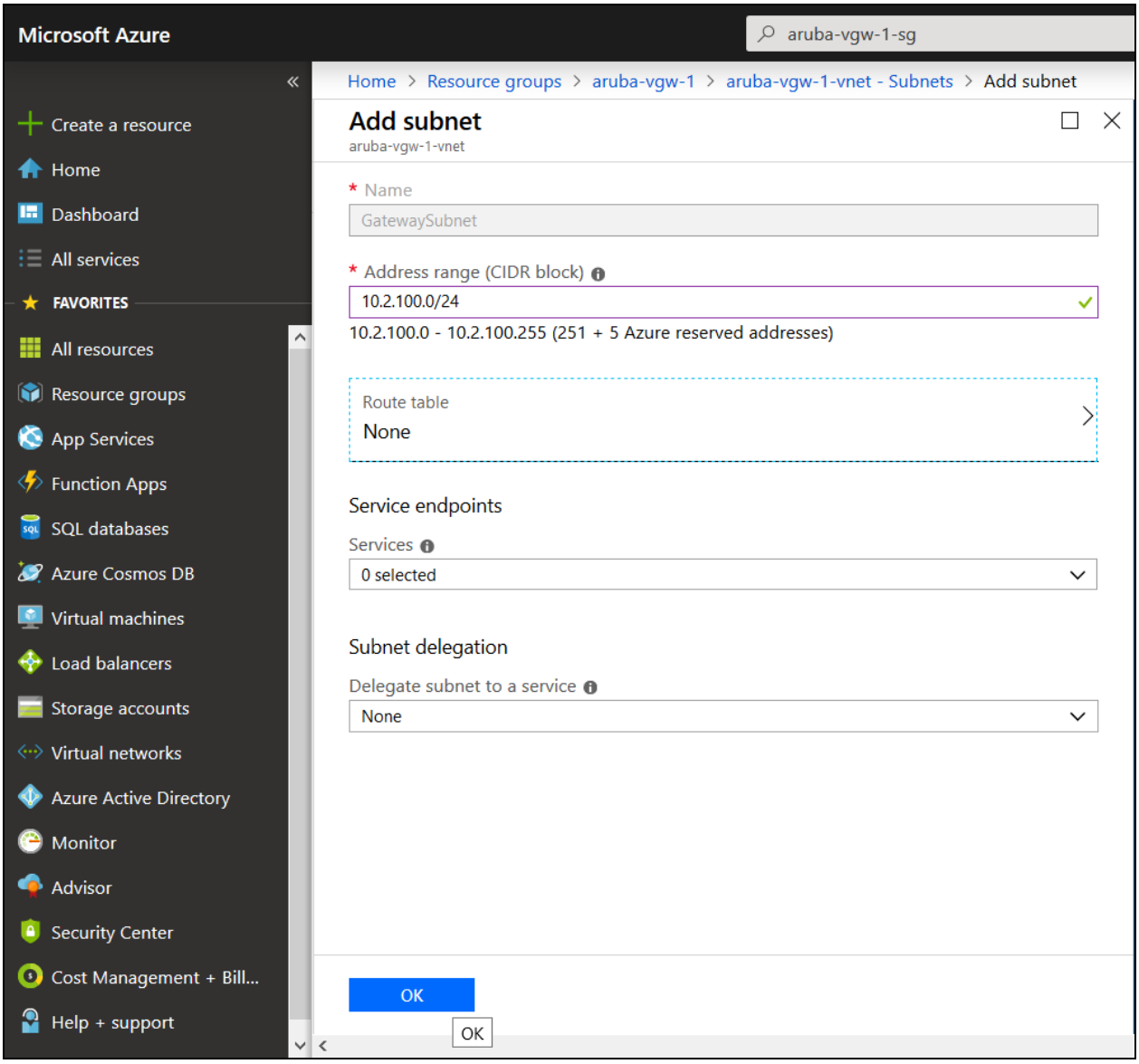
- Configuring a Gateway Subnet for a VNET
- Configuring Subnets for Virtual Gateway Network Interfaces

Configuring a Gateway Subnet for a VNET

1. Go to **Home** > **Networking** > **Virtual Networks**.
2. Select the VNET that you want to configure.
3. In the **Settings** list, select **Subnets**.
4. In the **Subnets** window, click **+Gateway subnet**.
5. By default, the gateway subnet name is set as **GatewaySubnet**.
6. Update the **Address range (CIDR block)** values to match your requirements.
7. Click **OK**.

Ensure that the gateway subnet is not associated to a network security group to avoid malfunctioning of the VPN gateway.

Figure 407 *Configuring Gateway Subnet*



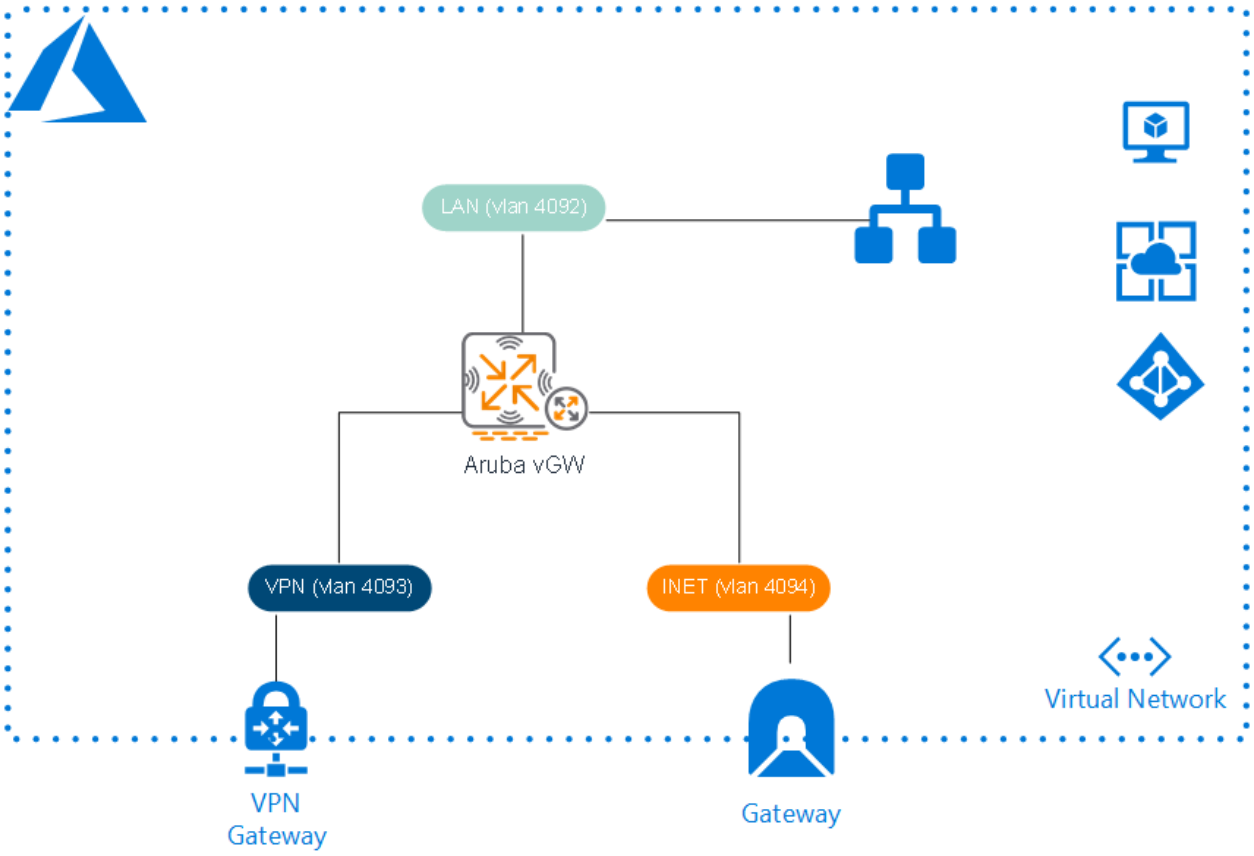
Configuring Subnets for Virtual Gateway Network Interfaces

To allow Aruba Virtual Gateway to connect to all relevant resources in your VNET, separate interconnection subnets should be created for all its network interfaces:

- Management
- INET
- VPN
- LAN

The following figure illustrates the subnet requirements for Virtual Gateway network interfaces:

Figure 408 *Aruba Gateway Network Interfaces*



NOTE

Aruba recommends that you create interconnection subnets from a CIDR block of /28 or /27. This ensures that there are sufficient IP address for future requirements.

To configure subnets for the Virtual Gateway network interfaces:

1. Go to **Home** > **Networking** > **Virtual Networks**.
2. Select the VNET that you want to configure.
3. In the **Settings** list, select **Subnets**.
4. In the **Subnets** window, click **+Subnet**.
5. Configure the following parameters:
   - **Name**—Enter a name that is unique within the VNET.
   - **Address range (CIDR block)**—Enter an IP address range that is unique within the VNET address space. This range must not overlap with any other subnet range in the VNET.
   - **Network security group**—Select an existing network security group from within the same subscription and location as the VNET.
   - **Route table**—Select an existing route table from the same subscription and location as the VNET.
   - **Service endpoints-Services**—From the **Services** list, select the services that you want enable for the network interfaces connected to the subnet.
   - **Subnet delegation-Delegate subnet to a service**—Subnet delegation allows explicit permissions to the service to create service-specific resources in the subnet using a unique identifier when deploying a service. To delegate for a service, select a service from the **Services** list.

6. Click **OK**.
7. Ensure that you have created subnets for each of following network interfaces:
    a. Management
    b. INET
    c. VPN
    d. LAN

Figure 409 *Configuring Subnets*

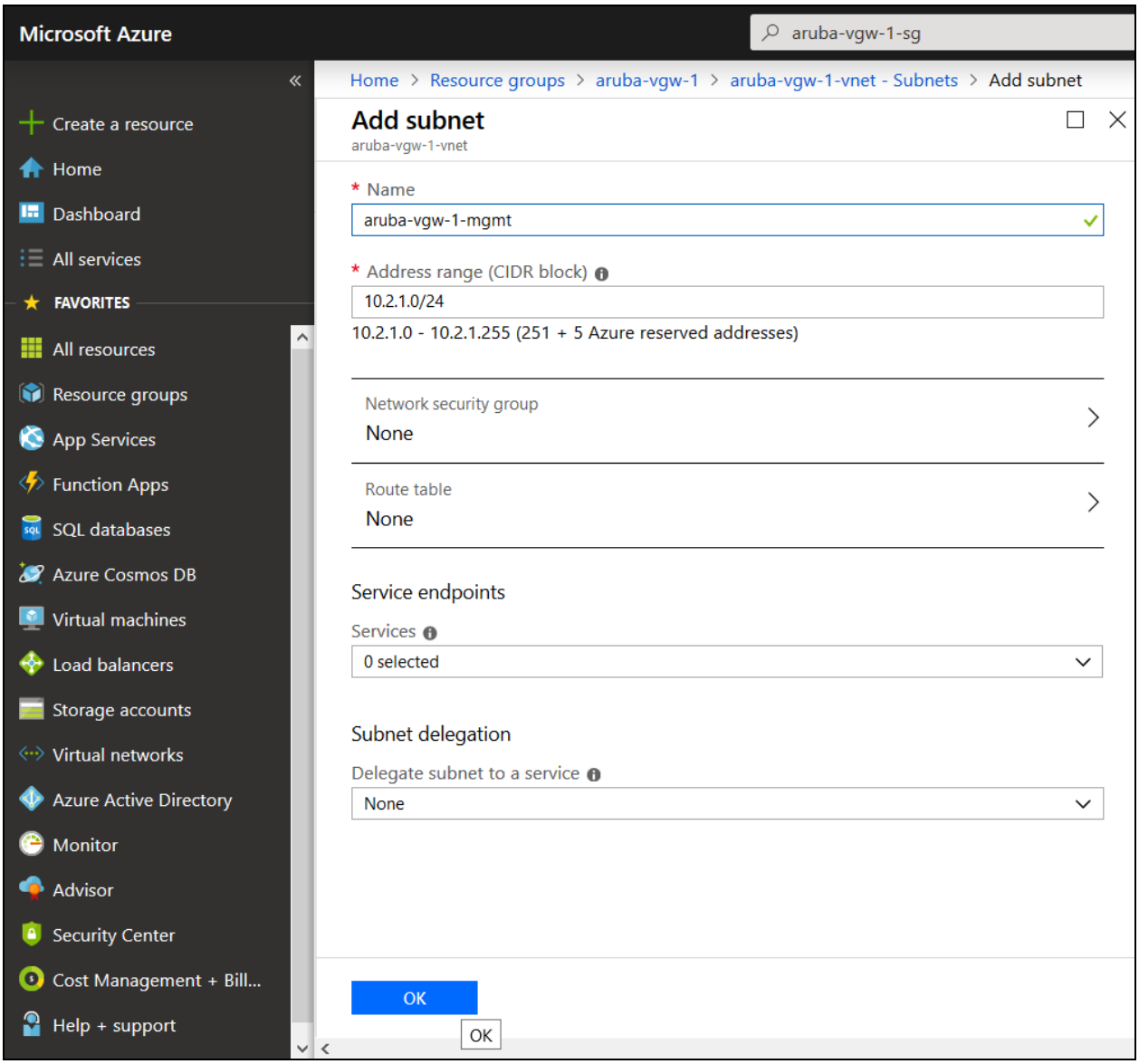
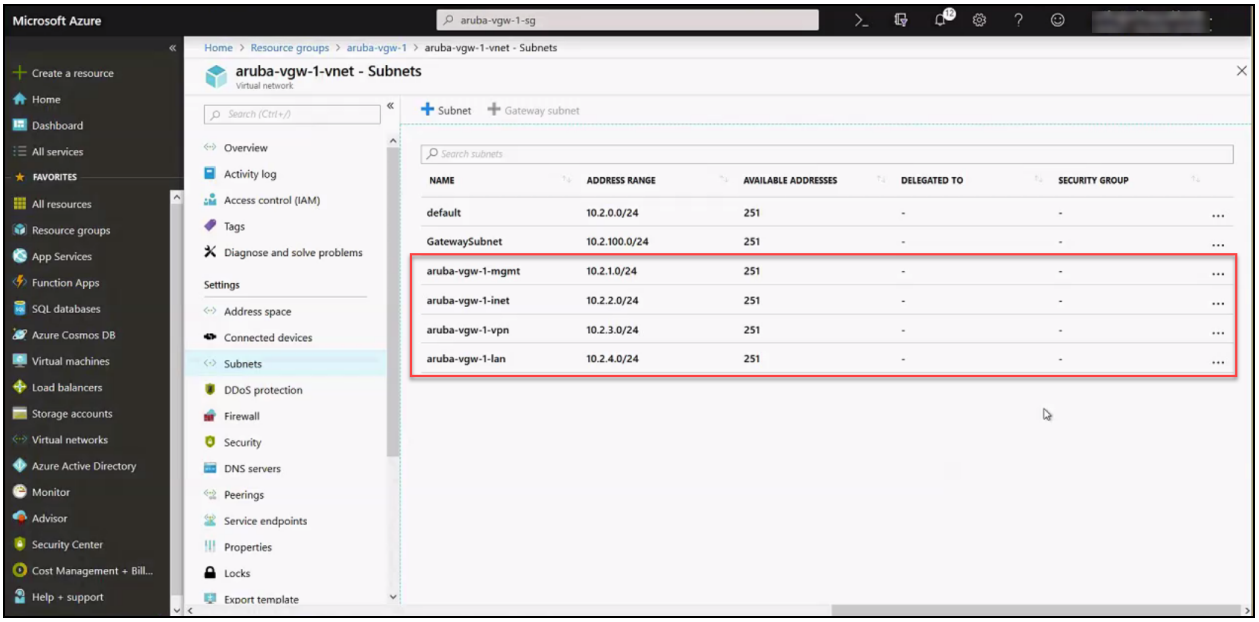


Figure 410 *Subnets added to a VNET*



Creating Network Interfaces

A network interface enables an Azure VM to communicate with the Internet, Azure, and other on-premises resources. A VM can have one or more network interfaces.

NOTE

Azure portal does not support attaching multiple interfaces to a VM using the GUI. Instead, you can create additional NICs in the GUI and attach then to the VM using the CLI during the VM creation phase.

For Aruba Virtual Gateway deployment, Aruba recommends that you create a separate network interface for each traffic type and map these to subnets in the following order:

- NIC1—Management traffic
- NIC2—Internet traffic– Requires a Public IP for connectivity to Aruba Central
- NIC3—VPN traffic
- NIC4—LAN traffic

NOTE

Aruba Virtual Gateways use DPDK internally and that includes bridging/switching functionality. However due to generic restrictions of cloud networks (ProxyARP and no direct L2 connectivity), NIC0 is used internally for management connectivity; for example, SSH or WEBUI and any configuration is optional. Ensure that NIC1 is used for all data traffic to and from the Aruba Virtual Gateway; for example, IPSec, SSH, and WEBUI.

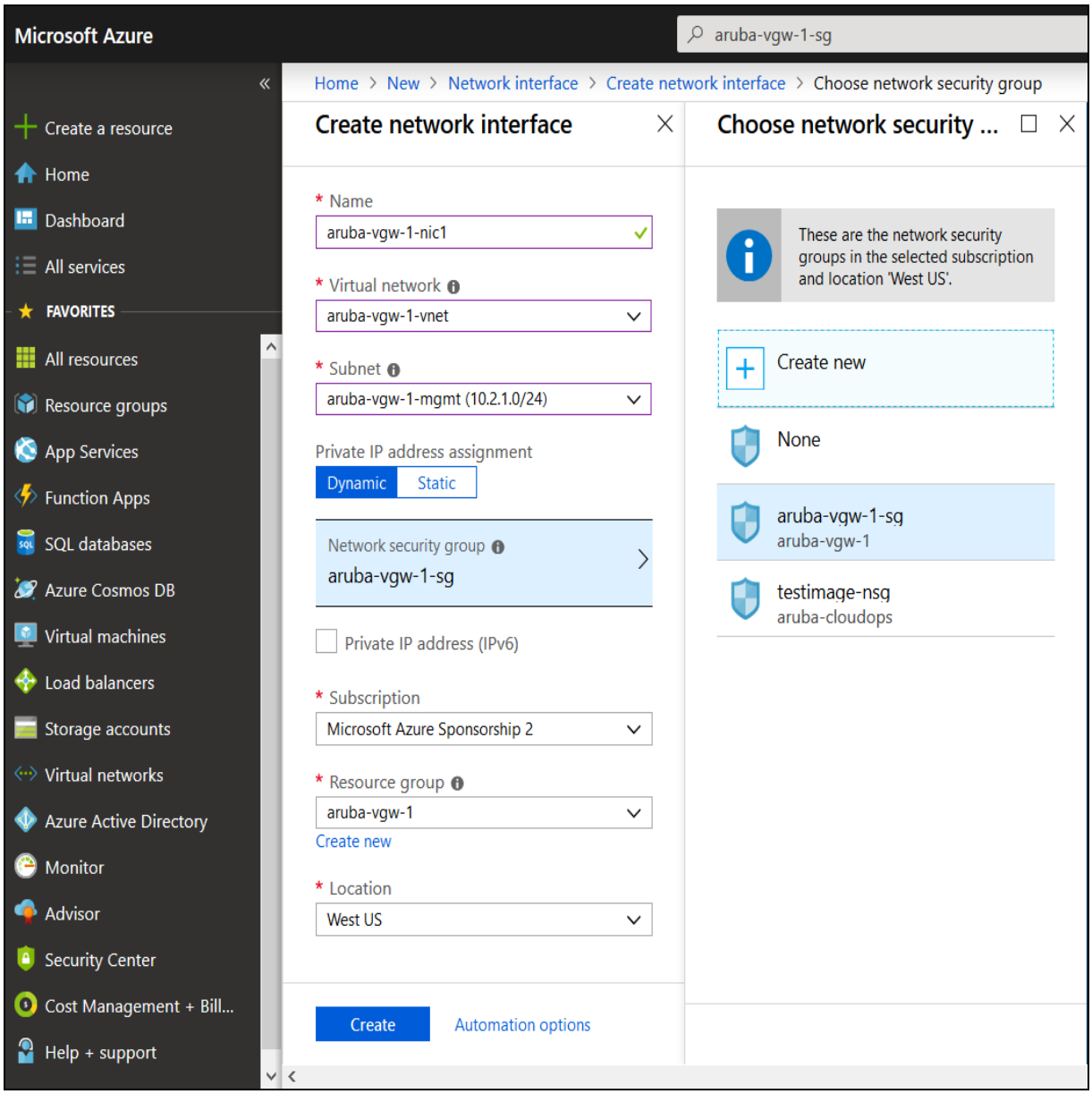
1. To create network interfaces follow these steps:
   a. In the Azure portal, click **Home** > **+Create a Resource** .
   b. On the **Home** page, enter network interface in the search box to access the **Network Interface** page.
   c. Click **Create**.
   d. In the **Create network interface** window, configure the following parameters:

- **Name**—Enter a name for the interface; for example, NIC1.
- **Virtual network**—Select the VNET to which you want to add the interface.
- **Subnet**—Select the subnet that you want assign to the interface.
- **Private IP address assignment**— Based on your configuration requirements, select either **Dynamic** or **Static** addressing.
- **Network security group**—Select the network security group to which you want to attach this interface.
- **Subscription**—Select the subscription.
- **Resource Group**—Select the resource group to which you want to map the interface.
- **Location**—Select the geographic location of your VNET.

e. Click **Create**.

f. Repeat these steps to create additional network interfaces, for NIC2, NIC3, and NIC4.

Figure 411 *Creating Network Interfaces*

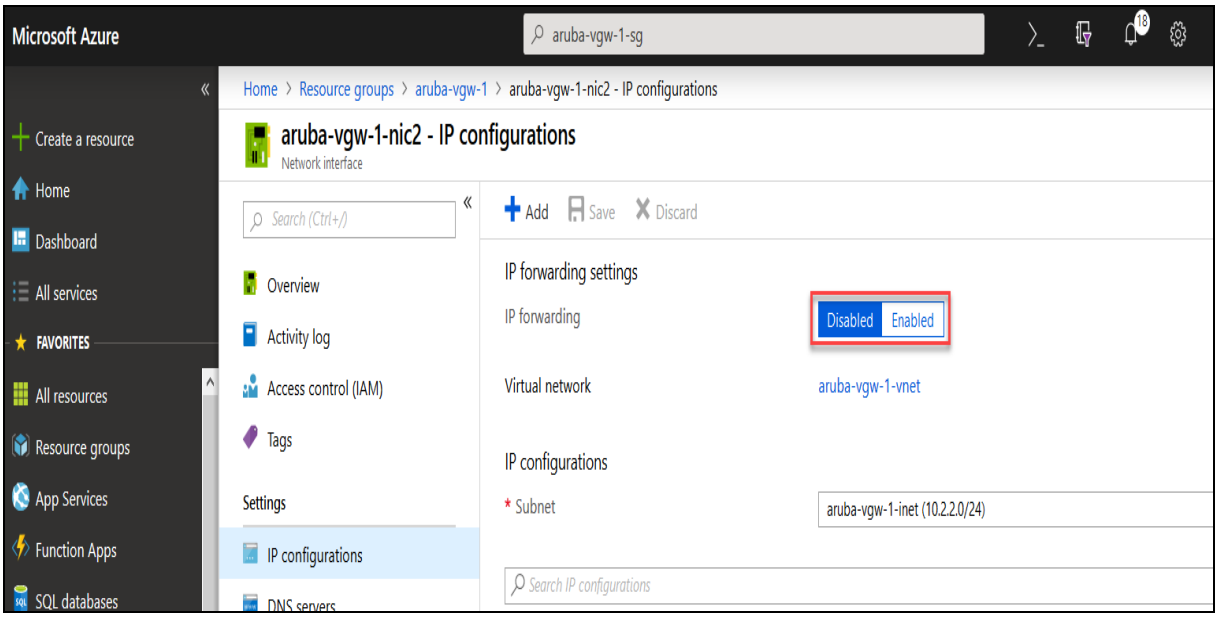


2. To enable IP forwarding for NIC2, NIC3, and NIC4, follow these steps:
   a. In the Azure portal, go to **Home** > **Resource groups**.
   b. Select the resource group associated to your VNET.
   c. From the list of network interfaces, select the NIC.
   d. Under **Settings**, select **IP configurations**.
   e. Configure the following parameters:

   IP forwarding settings

   IP forwarding— Set to **Enabled**.

   Figure 412 *Enabling IP forwarding*



3. To add Public IP to iNeT, follow these steps:
   a. Under **Settings**, select **IP configurations**.
   b. Set **IP forwarding** to **Enabled**.
   c. Click **Save**.
   d. Click the listed **ipconfig1**.
   e. In the new window, set the **Public IP address** as **Enabled**.
   f. Click **Save**.

Uploading the Aruba Virtual Gateway Software Image

To use the Aruba Gateway software image as the source for an Azure managed virtual disk, you must ensure that the Aruba Virtual Gateway software image is uploaded to a blob container in your storage account.

Aruba supports Azure VNET deployments on Virtual Gateway appliances running ArubaOS SD-WAN 8.4.0.0-1.0.5.0 or later software versions. To obtain access to a valid VHD image for Virtual Gateways, contact your Aruba Sales Specialist.

To upload the .vhd file, complete the following steps:

1. Download and install the **Azure Storage Explorer** app. For more information, see Azure Storage Explorer.
2. Open **Azure Storage Explorer**.

3. Log in with your Azure account credentials.
4. In the **Storage Explorer** window, navigate to your storage account, and select **Blob Container**.
5. Right-click and choose **Create Blob Container** and enter a name of the blob container. Ensure that the container name is in lowercase.
6. Press **Enter** to create the container.
7. Select **Upload** on the container ribbon. The **Upload Files** pop-up window opens.
8. Browse to your local directory and select the image to upload.
9. Select **Page Blob** as the blob type and ensure that the **Upload .vhd/vhdx file as page blobs (recommended)** check box is selected.
10. In the **Upload to folder (optional)** field, enter a folder name. If no folder is chosen, the files are uploaded directly under the container.
11. Click **Upload**.
12. Navigate to the container under your storage account and verify if the .vhd image is uploaded as a page blob.

Figure 413 *Uploading a VHD Image*

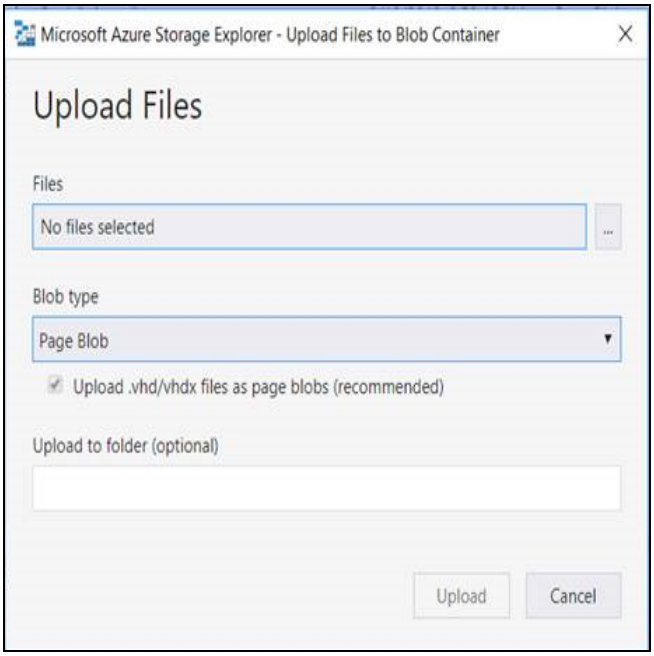
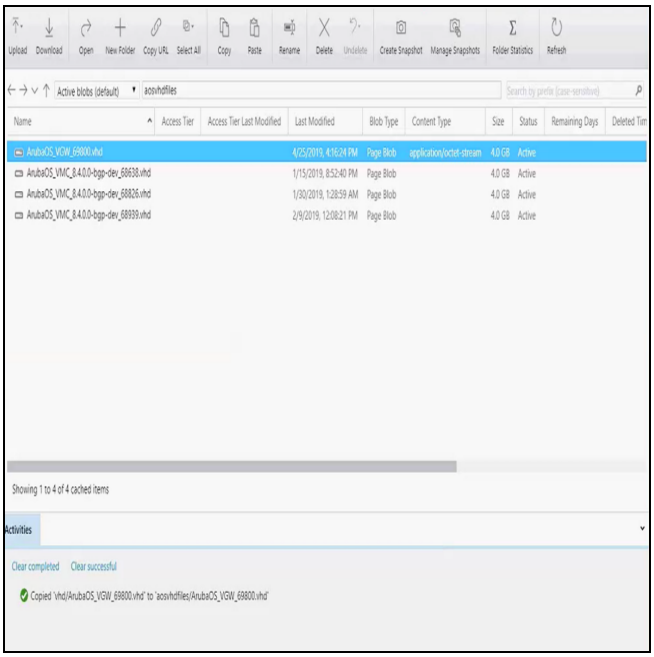


Figure 414 *View blobs in a container*



Creating Image and Data Disk

For Virtual Gateway deployment, an Image and data disk are required. Follow these steps to create the Image and data disk:

1. To create a an **Image** with ArubaOS software follow these steps:
    a. Log in to your Azure account.
    b. In the Azure portal click **+ Create a resource**.
    c. In the **Home>New** page, search for Image in the search box.
    d. Enter the **Name, Subscription, Resource group,** and **Location** in the new **Image** page.
    e. Select **Linux** as the **OS disk type**.
    f. In the **Storage blob** field, click **Browse**, to navigate to the **Storage accounts** page.
    g. In the **Storage accounts** page, select the container that has the .vhd file.
    h. In the container page, select the VHD file and click **Select** to add the file to the image.

Figure 415 *Creating an image*

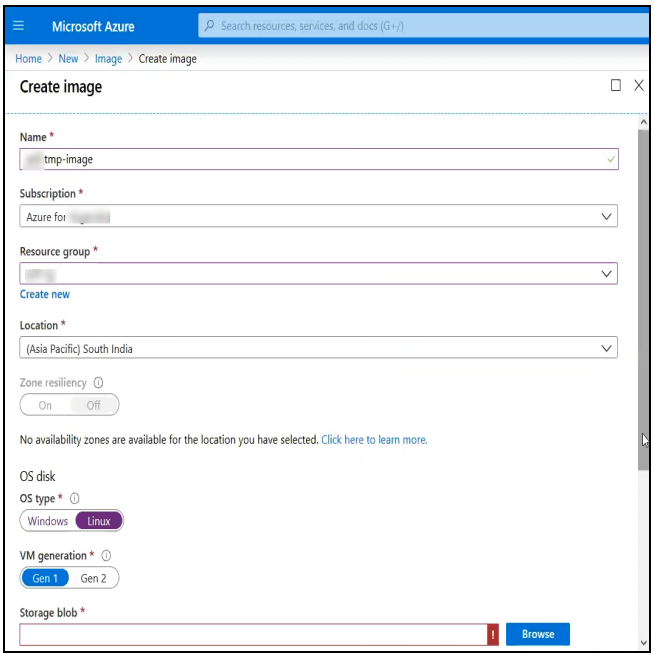


Figure 416 *Selecting the .vhd file*

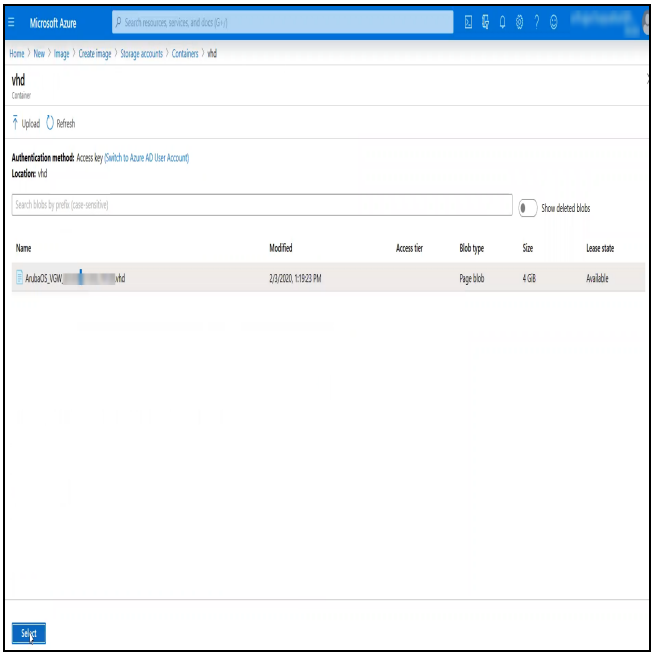
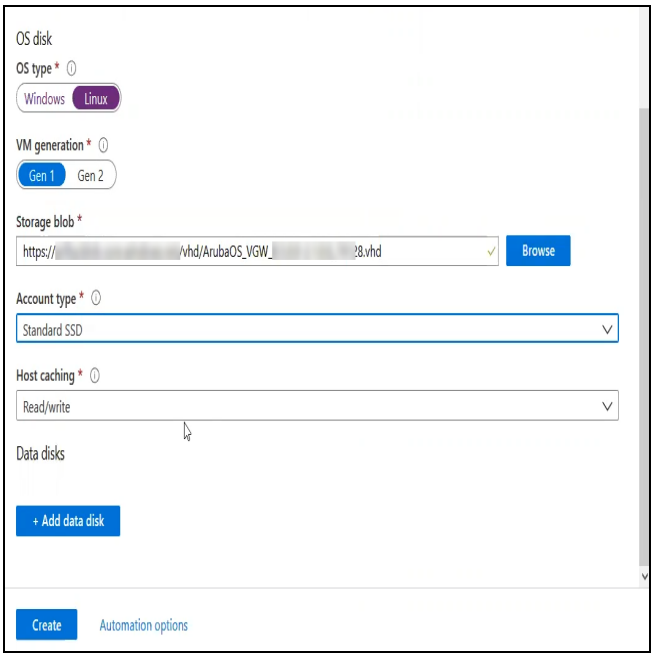


Figure 417 *Adding the .vhd file*



NOTE

OS disk—This is created from the image. Azure creates the disk during the VM deployment from the Image. The disk size is set to 4 GB.

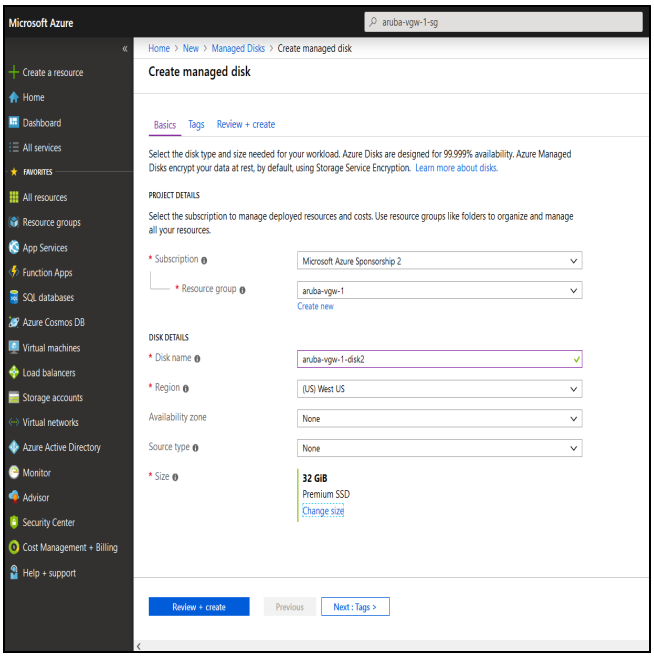
NOTE

Data disk—The secondary disk is the data disk. The capacity for the secondary disk should be double the size of the RAM.

2. To create a data disk follow these steps:

a. In the Azure portal, select **Home** > **Managed Disks**.
b. Select **Create managed disk**.
c. Select the subscription associated with your storage account.
d. Select the resource group mapped to your storage account.
e. Enter the following details to create the disk:
    1. **Disk name**—Create a uniquely identifiable name for the disk.
    2. **Region**—Select the region for the disk.
    3. **Availability zone**—Select the availability zone that this disk will be accessible from.
    4. **Source type**—Select the source type as **None**.
    5. **Size**—Set the size of the disk.
f. Click **Review + Create** to review your storage account settings and create the account.
g. Click **Create**.

Figure 418 *Creating a secondary disk*



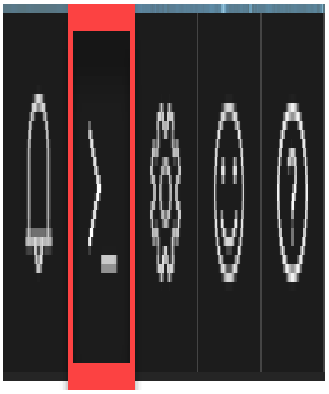
Setting up a Virtual Machine

Currently, Azure portal does not support creating VMs through the GUI. Use Azure Cloud Shell to create VMs.

To create a VM:

1. In the Azure portal, navigate to **Home** > **Virtual networks** and select the VM from the menu.
2. On the toolbar at the top of the page, click the Cloud Shell icon to launch **Cloud Shell**.

Figure 419 *Cloud Shell icon*



3. Log in with your credentials.
4. Create a VM using the **az vm create** command.
5. Ensure that you enter appropriate values for resource group, OS-type, boot diagnostics storage account, network interfaces and the VM size.

The recommended minimum configuration is with four CPUs and 14 GB of RAM (DSv2-series - Standard_DS3_v2). Ensure that you select Standard_DS3_v2 as the VM size.

NOTE

The name of the storage account created earlier, is to be entered in the **--boot-diagnostics-storage** command.

The **--nics** command is used to bind the network interfaces that were created earlier to the Virtual Machine.

The following command text shows the example values for all associated parameters of a VM:

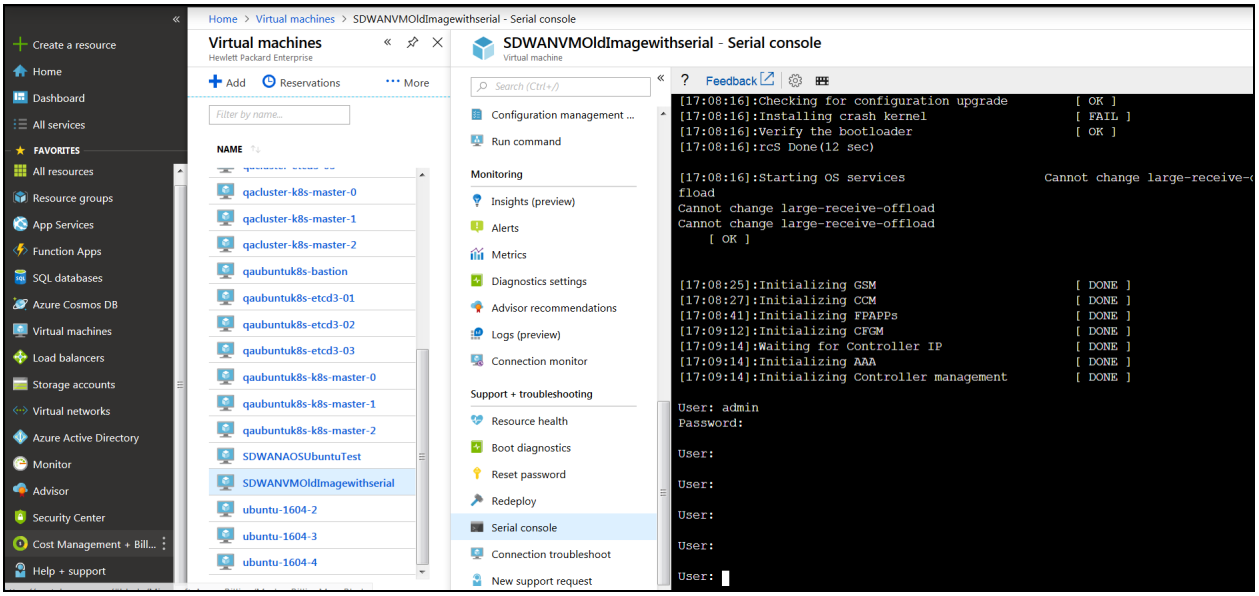
```
az vm create \
       --resource-group aruba-vgw-rg \
       --location eastus \
       --name aruba-vgw \
       --image aruba-vgw-image-xxxxx \
       --attach-data-disks aruba-vgw-data-disk \
       --boot-diagnostics-storage aruba-vgw-bootstorage \
       --size Standard_DS3_v2 \
       --nics aruba-vgw-nic1-mgmt aruba-vgw-nic2-inet aruba-vgw-nic3-vpn aruba-vgw-
nic4-lan \
       --admin-username vgw-user --ssh-key-value @key.pub \
       --custom-data userdata.txt
```

A sample of the user data file name is: `VG2003084499-UserData.txt`

NOTE

If the VM is up and running, try to access it using the SSH console (**Home** > **Virtual Machines** > **Serial Console**>. To access the VM console using SSH, use <username>@<external-IP-address>.

Figure 420 *Console Access to the VM*



Creating SSH Key Pairs

To create an SSH key pair, complete the following steps:

1. In the Azure portal, navigate to **Home** > **Virtual networks** and select the VM from the menu.
2. On the toolbar at the top of the page, launch **Cloud Shell** by clicking on the icon.
3. In the bash shell, use **ssh-keygen** to create an SSH key pair.

For example: `ssh-keygen -t rsa -b 2048`

4. The **ssh-keygen** command generates both public and private keys with the default name of `id_rsa` in the `~/.ssh directory`. The command returns the full path to the public key. This table lists the information required to complete the SSH key generation process:

Table 298: *SSH Key Generation Requirements*

Setting	Value
`Enter file in which to save the key`	The location where you want to save the key to. For example, aruba-vgw-1sshkey.
`Enter passphrase`	Enter a passphrase, or leave the field empty if there is no passphrase required.
`Enter same passphrase again`	Confirm the passphrase.

1. Note the path to the location of the public key
2. Use the **cat** command along with the path to the location of the public key to display the key.

For example: `cat AOS_aruba-vgw-1sshkey.pub`

3. Save the output of this command.

Generating User Data in Aruba Central

To allow Aruba Central to manage a Virtual Gateway that is deployed manually and directly in a customer's VNET, generate the device identity for the device in Aruba Central.

Ensure that you allow at least 30 seconds between the time the prompt appears and you enter the user data.

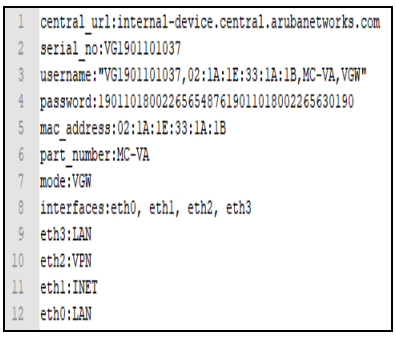
To generate device identity for the Virtual Gateway instance in an Azure VNET, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways**, click the **Config** icon. The configuration page is displayed.
3. Click **Unmanaged Virtual Gateway**.
4. In the **Unmanaged Virtual Gateway** page , select the Virtual Gateway model. Click **Create Device Identity**.
5. Click **Yes** to confirm identity creation. Aruba Central displays the download link for downloading user data.
6. Click **Yes** to confirm identity creation. Aruba Central displays the newly created VGW with the following fields:
    a. **Serial #**—Displays the serial number of the Virtual Gateway.
    b. **MAC**—Displays the sMAC address of the Virtual Gateway.
    c. **Model Number**—Displays the model number of the Virtual Gateway.

d. **Device Identity**—Displays the device identity of the Virtual Gateway.
e. **Status**—Displays the status as User Generated for the created device identity of the Virtual Gateway.

7. Click the three vertical dots icon next to the Status to view the **Account Options**.
8. Click **Download txt**. The user data includes the following information:
   - Aruba Central URL
   - Serial Number
   - User name and password for the Virtual Gateway. Virtual Gateways use these credentials to connect to the Activate and EST servers for EST enrollment
   - MAC Address of Virtual Gateway
   - Part Number of the Virtual Gateway instance
   - Deployment mode
   - Network interfaces configured on a Virtual Gateway
   - Activate URL

Figure 421 *Sample User data*



9. Ensure that you enter the Aruba Central-generated user data in the VM serial console during the initial boot of VM instance. This step is required to add Virtual Gateways as a managed device in Aruba Central.

NOTE

It is recommend that the user data be viewed in Wordpad or Notepad++ to retain the formatting.
The downloaded user data values must be converted to a single command, with each value separated by a semicolon.

Here is a sample of the user data command:

```
Azure user-data: central_url:internal-device.central.arubanetworks.com; serial_
no:VG1901101037; username:"VG1901101037,02:1A:1E:33:1A:1B,MC-VA,VGW";
password:190110180022656548761901101800226563019O; mac_address:02:1A:1E:33:1A:1B;
part_number:MC-VA; mode:VGW; interfaces:eth0, eth1, eth2, eth3; eth3:LAN; eth2:VPN;
eth1:INET; eth0:LAN;
```

Verifying the Deployment Status

To verify the Virtual Gateway deployment status, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways** > **Manual**, to view the summary page for manually orchestrated Virtual Gateways with following columns:
   - **Tenant**—Displays the name of the tenant network.
   - **Serial Number**—Displays the serial number of the Virtual Gateway.
   - **MAC Address**—Displays the MAC address of the Virtual Gateway.
   - **Model Number**—Displays the model number of the Virtual Gateway.
   - **IP Address**—Displays the IP address of the Virtual Gateway.
   - **Name**—Displays the name of the Virtual Gateway.
   - **Device Identity**—Displays the device identity of the Virtual Gateway.
   - **Status**—Displays the Enrollment over Secure Transport (EST) status of the Virtual Gateway.
3. Check if the Virtual Gateway is onboarded to the device inventory in Aruba Central .
4. Ensure that the Virtual Gateway is assigned to a device configuration group in Aruba Central.
5. Verify if the Virtual Gateway is connected to Aruba Central.
6. Configure a VPN tunnel between a Branch Gateway and the Virtual Gateway.

To check the Virtual Gateway operational status and the VPN tunnel status follow these steps:

1. In the **Network Operations** app, use the filter to select the gateway
2. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway. The dashboard context for a group is displayed.
3. Under **Manage**, click **Devices** > **Gateways**.
4. A list of gateways is displayed in the **List** view.
5. Click a gateway under **Device Name**. The dashboard context for the gateway device is displayed.
6. Go to **Manage** > **Overview**.

For more information, see the Gateway monitoring help topic in *Aruba Central Help Center*.

Deploying Aruba Virtual Gateways in VMware ESXi (Unmanaged Mode)

Aruba Central supports deploying Virtual Gateways in VMware compute virtualization platforms using the unmanaged mode. In the unmanaged mode, IT administrators can bring up and configure the Virtual Gateway instances in VMware ESXi version 5.5 or later using a vSphere client or the vCenter application. The Virtual Gateway instances can then be configured to provide VPNC functions and can be monitored using Aruba Central.

Deployment Procedure

Before deploying Aruba Virtual Gateway in VMware ESXi, ensure that you have the following resources and account privileges:

- Server infrastructure having adequate compute, memory and storage resources required for the Virtual Machine instance.
- VMware ESXi version 5.5 or later.
- Administrator credentials to access VMware ESXi.
- vSphere Client/vCenter 5.5 or above to access the server running the ESXi hypervisor.

- Aruba Central account and valid subscription to deploy Virtual Gateways.
- Download the OVA from the Aruba Support Portal. For more information, contact your Aruba Sales Specialist.

To deploy a Virtual Gateways in VMware ESXi using the unmanaged mode, complete the following steps:

1. Generate the device identity data for the Virtual Gateway instance in Aruba Central in the ISO format.
2. Download the Virtual Gateway OVA image from the Aruba Support Portal. For example, the OVA image name format is— *ArubaOS_VGW_8.6.0.4-2.2.0.0_76431.ova*.
3. Create the VM using Virtual Gateway OVA and device identity data.
4. Connect the Virtual Gateway to Aruba Central by either using zero-touch provisioning or one-touch provisioning.
5. Verify the deployment status.

Virtual Gateway Sizing

The Aruba Virtual Gateway requires the use of a supported VMware ESXi instance with a minimum of 500 Mbps of throughput and can support up to 1600 IPsec tunnels. This table lists out the supported VMware ESXi instances for each Aruba Model/SKU:

Aruba Model/SKU Name	Throughput	vCPU	RAM Memory (GB)	Flash Memory (GB)	Tunnels
VGW-500MB	500 Mbps	4	7	15	1600
VGW-2GB	2 Gbps	8	15	30	4096
VGW-4GB	4 Gbps	16	30	60	8192

If a higher number of tunnels are required, contact your Aruba Sales Specialist.

Generating User Data in Aruba Central

For Aruba Central to manage a Virtual Gateway that is deployed manually and directly in a customer's VPC, generate device identity for the device in Aruba Central.

To generate device identity for the Virtual Gateway instance, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways**, click the **Config** icon. The configuration page is displayed.
3. Click **Unmanaged**.
4. Select the Virtual Gateway model.
5. Click **Create Device Identity**.
6. Click **Yes** to confirm identity creation. Aruba Central displays the newly created VGW with the following fields:

a. **Serial #**—Displays the serial number of the Virtual Gateway.
b. **MAC**—Displays the MAC address of the Virtual Gateway.
c. **Model Number**—Displays the model number of the Virtual Gateway.
d. **Device Identity**—Displays the device identity of the Virtual Gateway.
e. **Status**—Displays the status as User Generated for the created device identity of the Virtual Gateway.

7. Click the three vertical dots icon next to the Status to view the **Account Options**.
8. Click **Download ISO**. The ISO format of the user data file is downloaded.
9. Ensure that you load the Aruba Central-generated ISO file in the vSphere Client during the initial boot of VM instance. This step is required to add Virtual Gateways as an unmanaged device in Aruba Central.

Creating and Configuring Virtual Gateway

To create and configure the Virtual Gateway using the Virtual Gateway OVA and device identity data, complete the following steps:

1. Deploy the OVF template.
2. Pre-allocate memory and CPU utilization.
3. Upload ISO File in to the ESXi Sever Datastore.
4. Create VM Network.
5. Assign Network Connection.
6. Enable Security Profile Configuration.
7. Configure Serial Console for the VM.

Deploying the OVF Template

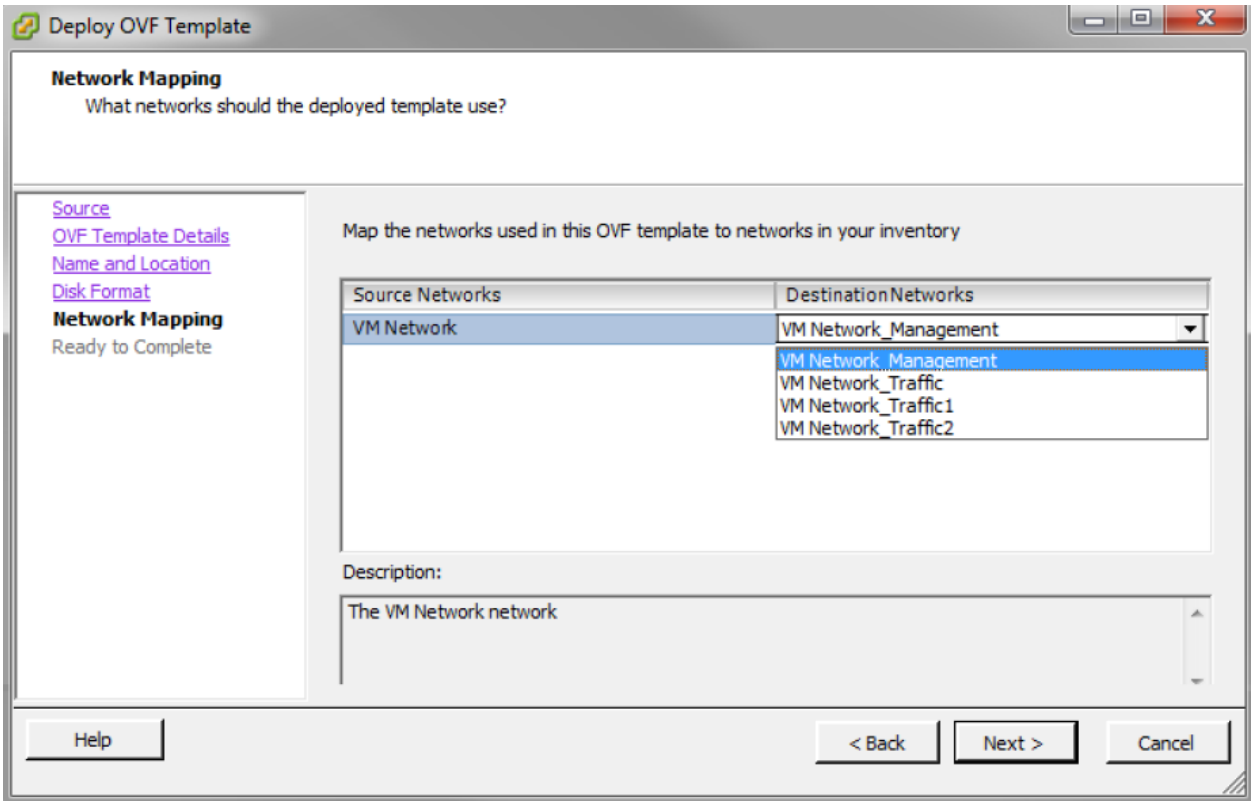
To deploy the OVF template, complete the following steps:

1. Log in to the vSphere Client.

It is recommended to use vSphere Client version 5.5 and above. For more information about the procedure, see VMware vSphere Documentation Center.

2. Click **File > Deploy OVF Template**. The **Deploy OVF Template Wizard** is displayed. It is recommended to copy the OVF template to the client machine before importing the OVF template.
3. Click **Browse** and navigate to the location of the OVA file and click **Next**. The OVF Template Details option in the left pane is displayed.
4. Click **Next**. The **Name and Location** option in the left pane is displayed.
5. In the **Name** field, enter a name for the OVF template and click **Next**. The Disk Format option in the left pane is displayed.
6. Select **Thick Provision Lazy Zeroed** option and click **Next**. The **Network Mapping** option in the left pane is displayed.
7. Select **VM Network_Management** from the Network Label drop-down list and click **Next**. The **Ready to Complete** option in the left pane is displayed.

Network Mapping



Review your preferences before clicking **Finish**.

NOTE

Ensure that the **Power on after deployment** check box is disabled in the **Ready to Complete** window.

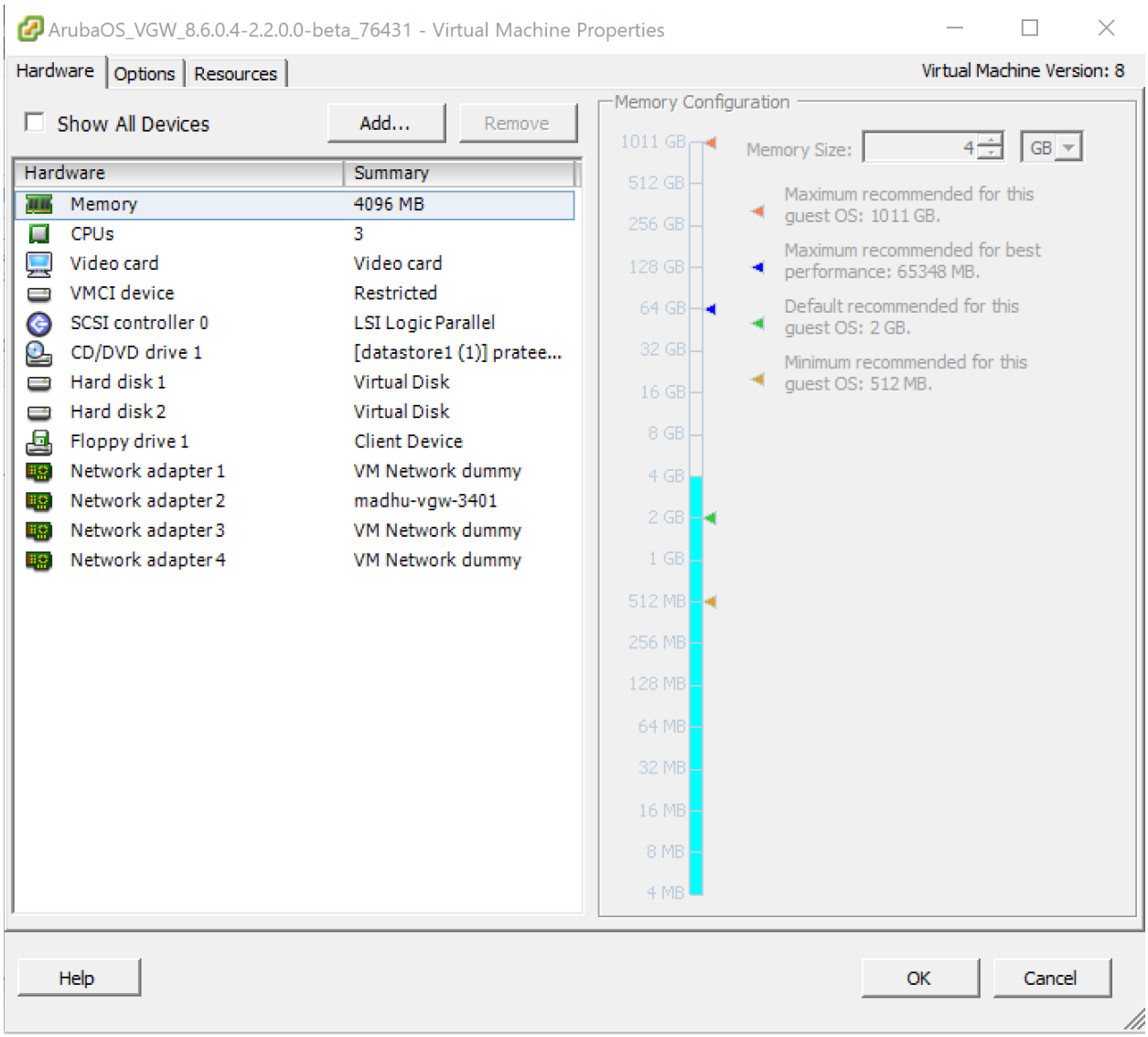
8. Click **Finish**. The OVF template is deployed.
9. Click **OK**.
10. Click **Close**.

Pre-allocating Memory and CPU Utilization

To pre-allocate memory and CPU utilization, complete the following steps:

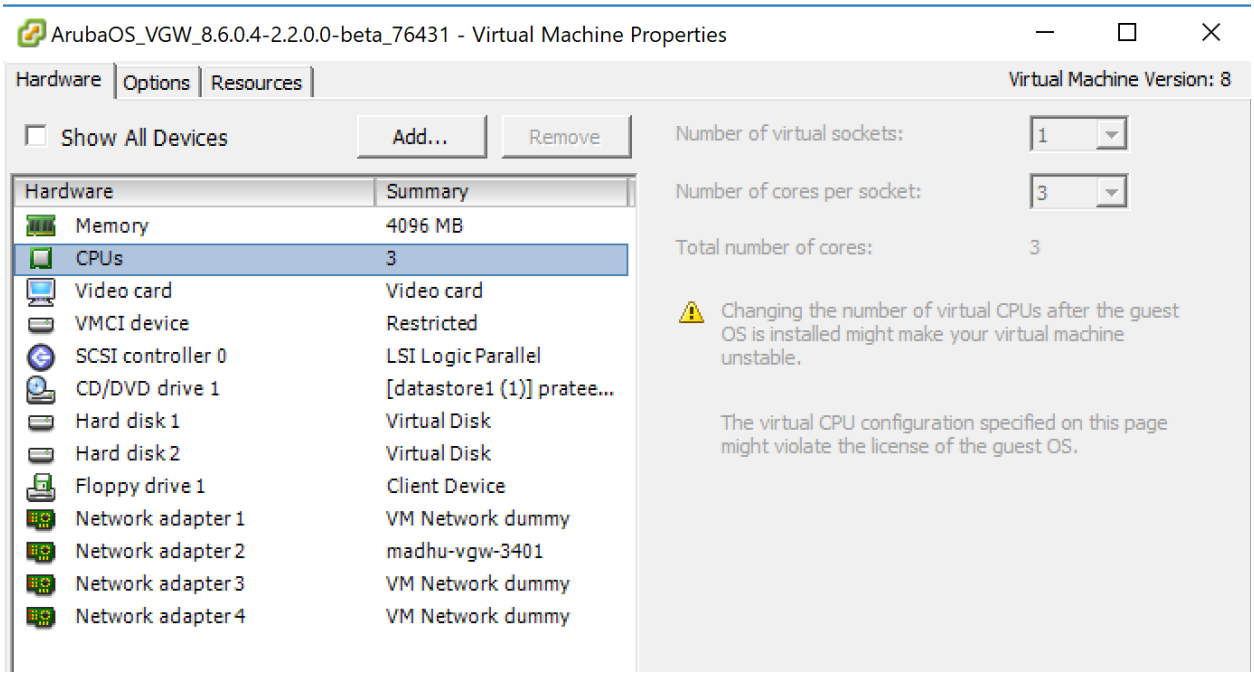
1. Right-click the VM and select **Edit Settings** or click **Edit virtual machine settings** from the **Getting Started** tab.
2. From the **Resources** tab, select **Memory** and configure the Memory Size as per the Virtual Gateway sizing table.
3. Click **OK**.

Figure 422 *Editing Memory Setting*



4. From the **Resources** tab, configure the **CPUs** as per the Virtual Gateway sizing table.
5. Click **OK**.

Figure 423 *Editing CPUs Setting*



Uploading ISO File in to the ESXi Sever Datastore

To upload the ISO in to the ESXi sever Datastore, complete the following steps:

1. Right-click the VM and select **Edit Settings** or click **Edit virtual machine settings** from the **Getting Started** tab.
2. From the **Resources** tab, select **CD/DVD drive**.

NOTE

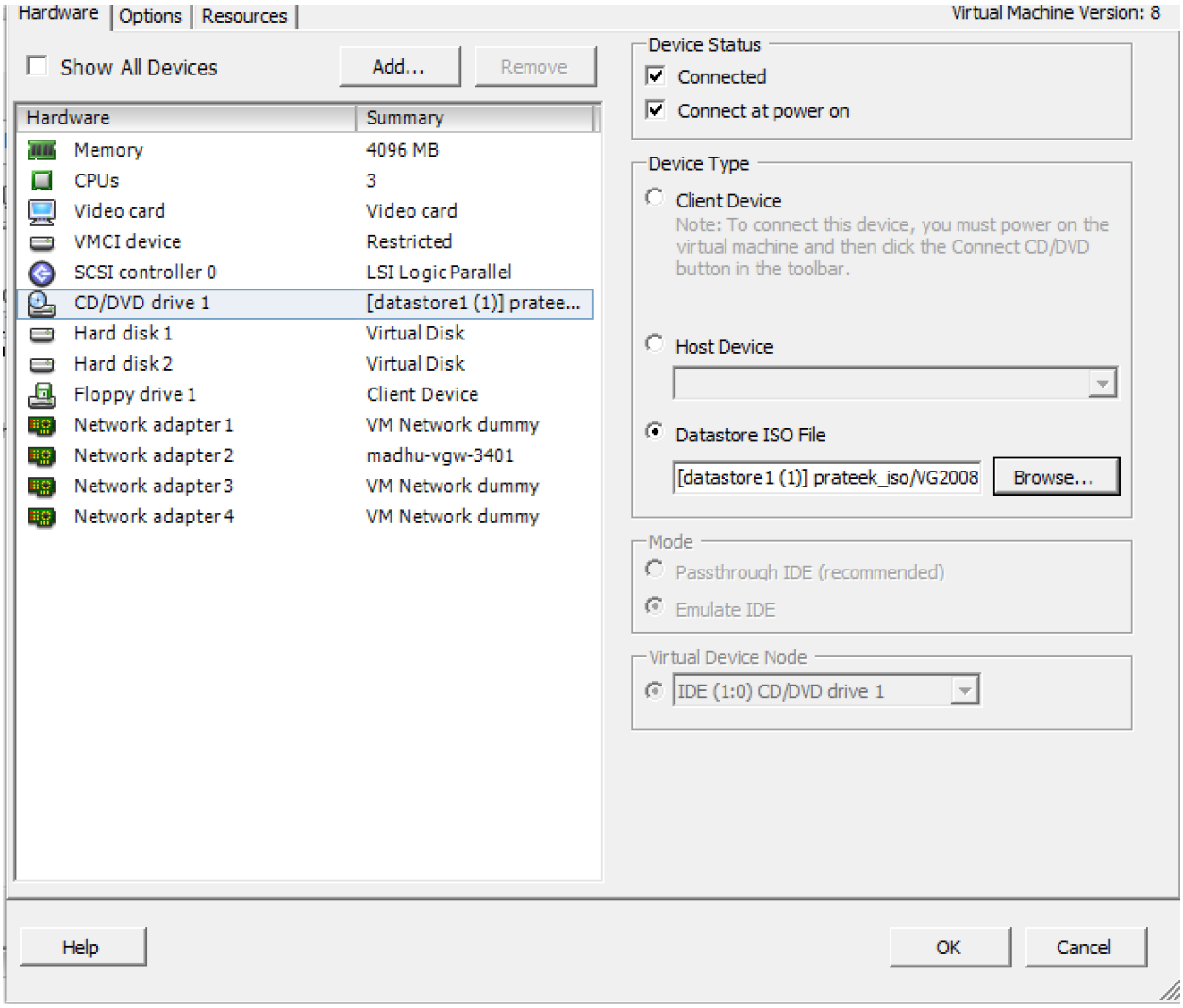
Ensure that the **Connected** and **Connected at power on** options under **Device Status** are enabled.

3. Under **Device Type**, select the radio button against **Datastore ISO File** and click **Browse**.
4. Navigate to the location where the Aruba Central-generated ISO file is stored, select the ISO file, and click **OK**.

NOTE

It is recommended to copy the Aruba Central-generated ISO file to the client machine before importing it.

Figure 424 *Uploading ISO File*



Creating VM Network

To create a VM network, complete the following steps:

1. Log in to the vSphere ESXi Host using vSphere client.
2. From the vSphere Client page, click **Inventory**.
3. Go to the **Configuration** tab. Under **Hardware** menu, click **Networking**.
4. Click **Add Networking**. The **Add Network Wizard** is displayed.
5. Select the **Virtual Machine** option and click Next.
6. Select the **vSwitch** that will handle the network traffic and click **Next**.
7. In the **Port Group Properties** section, provide a name for **Network Label** and select **All (4095)** from the **VLAN ID (Optional)** drop-down list. Click **Next**.
8. Click **Finish**.
9. Click the ESXi host IP address.
10. Go to the Configuration tab. Under **Hardware**, click **Networking**.
11. Click **Properties** of the **vSwitch**.
12. Select the port that was created earlier and click **Edit**.

13. Select **Promiscuous Mode**, **Forged Transmits** check boxes, and **Accept** from the drop-down list.
14. Click **OK**.
15. Click **Close**.

Assigning Network Connection

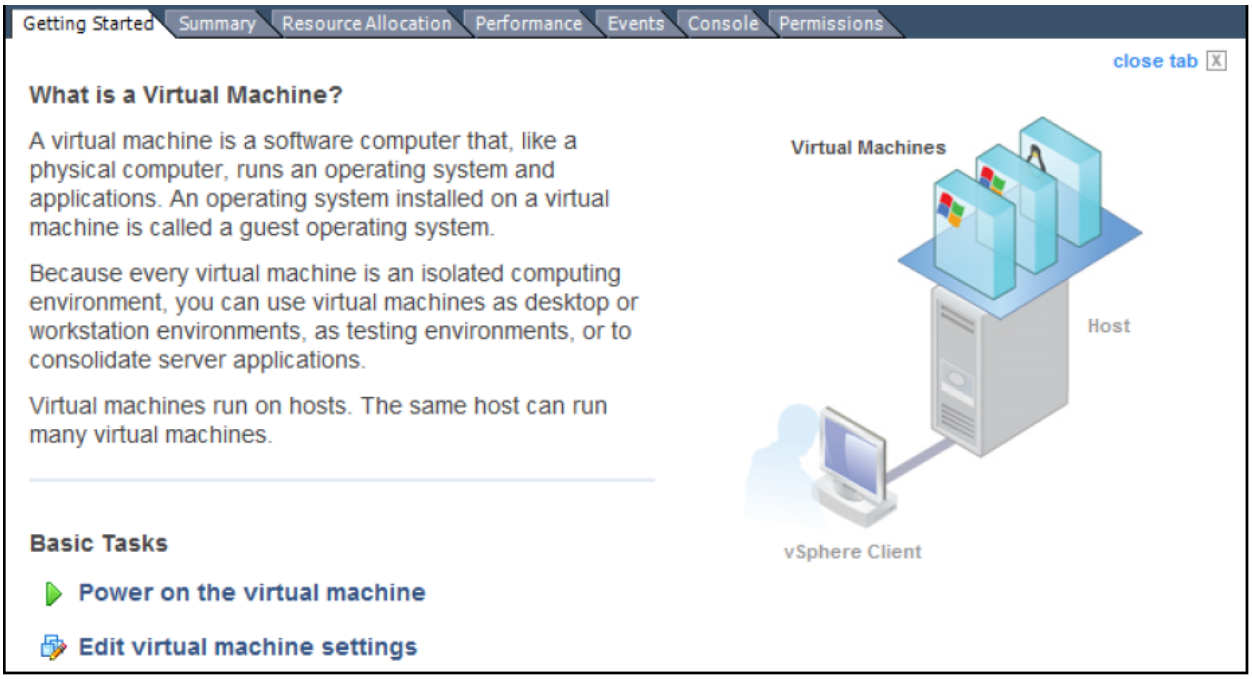
To assign network connection, complete the following steps:

NOTE

By default, the same network connection is assigned to all network adapters. This requires to be avoided as it will result in a network loop.

1. Click **Edit virtual machine settings**.

Figure 425 *Virtual Machine Settings*

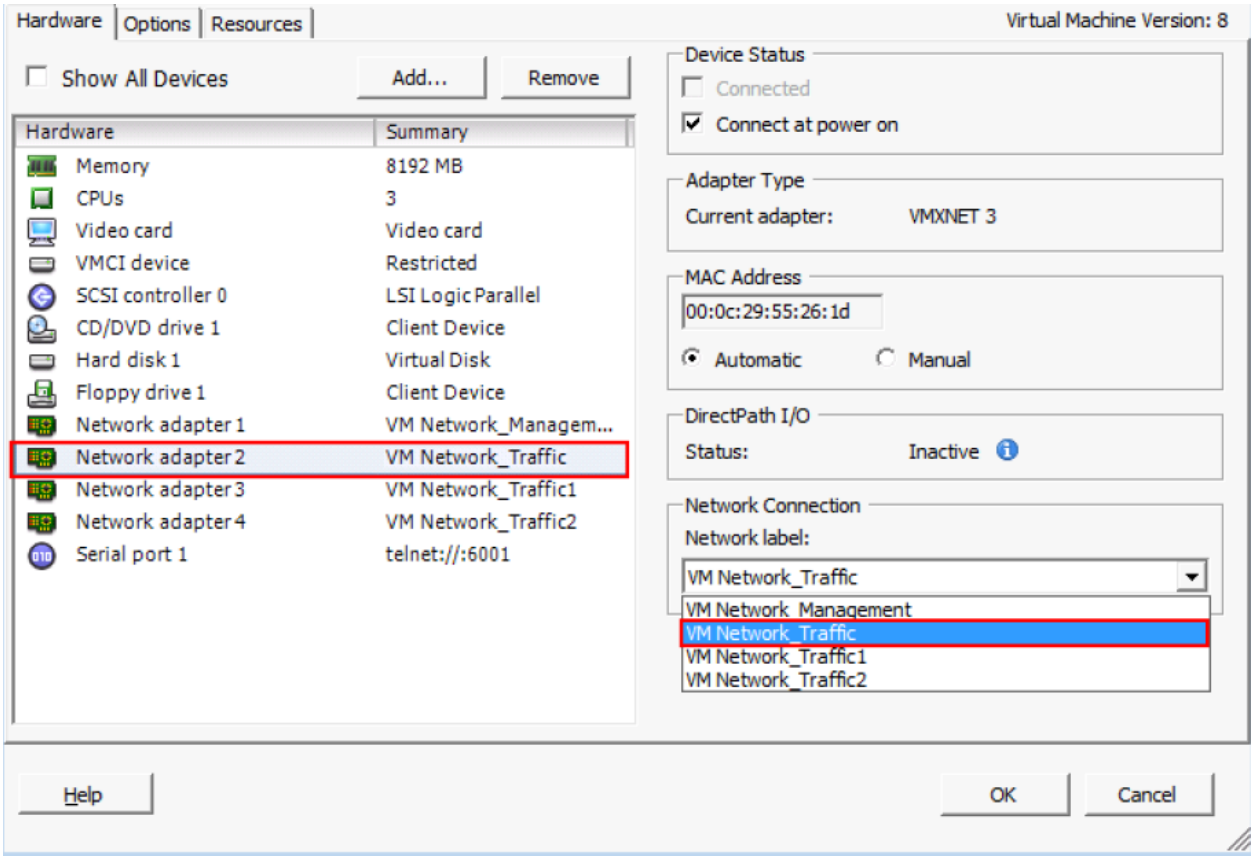


2. Select **Network adapter2** and select the preferred network label from the **Network label** drop-down list. Ensure that your network connection is not shared across all the network adapters as shown in the following figure.

NOTE

The VM should have network connectivity with the outside world through the **Network adapter 2** to connect with Aruba Central.

Figure 426 *Assigning A Network*



3. Click **OK**.

Enabling Security Profile Configuration

To enable security profile configuration, complete the following steps:

This is an optional step and should be used only if serial console redirection is required. To enable security profile configuration you need to Telnet over the network.

1. Click the ESXi host IP address.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Security Profile**.
4. In the **Firewall** section, click **Properties**.
5. Scroll down to **VM serial port connected over network** and ensure that the check box is selected.
6. Click **OK**.

Connecting Virtual Gateway to Aruba Central

To connect the Virtual Gateway to Aruba Central, use one of the following provisioning methods:

- Zero touch provisioning
- One touch provisioning

Zero Touch Provisioning

The Virtual Gateway connects to Aruba Central using Zero touch provisioning when there is a DHCP server in the network. The workflow is as follows:

1. The Virtual Gateway receives an IP address from the DHCP, triggers the EST enrollment, and connects to Aruba Central.
2. Verify the deployment status of the Virtual Gateway in Aruba Central. For more information, see Verifying the Deployment Status.

One Touch Provisioning

To connect the Virtual Gateway to Aruba Central using One touch provisioning, complete the following steps:

Ensure that there is no DHCP server in the network.

1. Boot the Virtual Gateway VM with the Aruba Central-generated ISO image. The VMware console displays the VM as a Virtual Gateway during the initial boot.
2. Select **vgw-static** from the initial provisioning wizard and provide the static IP address in the initial network configuration.
3. The Virtual Gateway triggers the EST enrollment and connects to Aruba Central.
4. Verify the deployment status of the Virtual Gateway in Aruba Central. For more information, see Verifying the Deployment Status.

Verifying the Deployment Status

To verify the Virtual Gateway deployment status, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways** > **Manual**, to view the summary page for manually orchestrated Virtual Gateways with following columns:
   - **Tenant**—Displays the name of the tenant network.
   - **Serial Number**—Displays the serial number of the Virtual Gateway.
   - **MAC Address**—Displays the MAC address of the Virtual Gateway.
   - **Model Number**—Displays the model number of the Virtual Gateway.
   - **IP Address**—Displays the IP address of the Virtual Gateway.
   - **Name**—Displays the name of the Virtual Gateway.
   - **Device Identity**—Displays the device identity of the Virtual Gateway.
   - **Status**—Displays the Enrollment over Secure Transport (EST) status of the Virtual Gateway.
3. Check if the Virtual Gateway is onboarded to the device inventory in Aruba Central .
4. Ensure that the Virtual Gateway is assigned to a device configuration group in Aruba Central.
5. Verify if the Virtual Gateway is connected to Aruba Central.
6. Configure a VPN tunnel between a Branch Gateway and the Virtual Gateway.

To check the Virtual Gateway operational status and the VPN tunnel status follow these steps:

1. In the **Network Operations** app, use the filter to select the gateway
2. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.

3. The dashboard context for a group is displayed.
4. Under **Manage**, click **Devices** > **Gateways**. A list of gateways is displayed in the **List** view.
5. Click a gateway under **Device Name**. The dashboard context for the gateway device is displayed.
6. Go to **Manage** > **Overview**.

For more information, see the Gateway monitoring help topic in *Aruba Central Help Center*.

Deploying Aruba Virtual Gateways in Google Cloud Platform (Unmanaged Mode)

Aruba Central supports deploying Virtual Gateways in Google Cloud Platform using the unmanaged mode. In the unmanaged mode, IT administrators bring up and configure the Virtual Gateway instances in Google Cloud and monitor the deployed Virtual Gateways from Aruba Central.

Deployment Procedure

Before deploying Aruba Virtual Gateway in Google Cloud, ensure that you have the following resources and account privileges:

- Administrator credentials to access Google Cloud.
- Aruba Central account and valid subscription to deploy Virtual Gateways.
- Download the Aruba Virtual Gateway image (.image.tar.gz) from the Aruba Support Portal. For more information, contact your Aruba Sales Specialist.

To deploy a Virtual Gateways in Google Cloud using the unmanaged mode, complete the following steps:

1. Generate User Data in Aruba Central.
2. Upload Aruba Virtual Gateway images into Google Cloud storage.
3. Create Virtual Gateway image using Google Cloud Shell console.
4. Create four VPCs on Google Cloud.
5. Configure firewall.
6. Create the VM instance using Aruba image.
7. Connect the VM instance to Serial Console.
8. Verify the deployment status.

Virtual Gateway Sizing

The Aruba Virtual Gateway requires the use of a supported GCP instance with a minimum of 500 Mbps of throughput and can support up to 1600 IPsec tunnels. This table lists out the supported GCP instances for each Aruba Model/SKU:

Aruba Model/SKU Name	Throughput	vCPU	RAM Memory (GB)	Flash Memory (GB)	Tunnels
VGW-500MB	500 Mbps	4	7	15	1600
VGW-2GB	2 Gbps	8	15	30	4096
VGW-4GB	4 Gbps	16	30	60	8192

NOTE

If a higher number of tunnels are required, contact your Aruba Sales Specialist.

Generating User Data in Aruba Central

To allow Aruba Central to manage a Virtual Gateway that is deployed manually and directly in Google Cloud, generate the device identity for the device in Aruba Central.

To generate user data for the Virtual Gateway instance in Google Cloud, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways**, click the **Config** icon. The configuration page is displayed.
3. Click **Unmanaged Virtual Gateway**.
4. In the **Unmanaged Virtual Gateway** page , select the Virtual Gateway model. Click **Create Device Identity**.
5. Click **Yes** to confirm identity creation. Aruba Central displays the download link for downloading user data.
6. Click **Yes** to confirm identity creation. Aruba Central displays the newly created VGW with the following fields:
   - **Serial #**—Displays the serial number of the Virtual Gateway.
   - **MAC**—Displays the sMAC address of the Virtual Gateway.
   - **Model Number**—Displays the model number of the Virtual Gateway.
   - **Device Identity**—Displays the device identity of the Virtual Gateway.
   - **Status**—Displays the status as User Generated for the created device identity of the Virtual Gateway.
7. Click the three vertical dots icon next to the Status to view the **Account Options**.
8. Click **Download txt** or copy the user data. The user data includes the following information:
   - Aruba Central URL
   - Serial Number
   - User name and password for the Virtual Gateway. Virtual Gateways use these credentials to connect to the Activate and EST servers for EST enrollment
   - MAC Address of Virtual Gateway
   - Part Number of the Virtual Gateway instance
   - Deployment mode
   - Network interfaces configured on a Virtual Gateway
   - Activate URL

Uploading Aruba Virtual Gateway Images into Google Cloud Storage

Prerequisites

1. Download the Aruba Virtual Gateway images `.image.tar.gz` and `.tar.gz` from the Aruba Support Portal. For more information, contact your Aruba Sales Specialist.
2. Log in to your Google Cloud account and create a **Project**.

Uploading Aruba Virtual Gateway images into Google Cloud Storage

To upload the Aruba Virtual Gateway image into Google Cloud storage, complete the following steps:

1. Log in to your Google Cloud account.
2. Navigate to **My Project** drop-down and select a **Project**.
3. Navigate to **Cloud Storage** > **Browser**.
4. Click **Create Bucket**.
   a. Enter a name of the bucket.
   b. Select the **Location type** to **Region**.
   c. Provide a **Location**.
   d. Set the **Storage class** to **Standard**.
   e. Set the **Access Control** to **Fine-grained**.
   f. Click **Advanced settings**.
   g. Set the **Encryption** to **Google-managed key**.
5. Click **Create**.
6. Click **Upload Files**.
7. Upload the Aruba Virtual Gateway image `.img.tar.gz`.

To create a Virtual Gateway image using Google Cloud Shell Console, see Creating Virtual Gateway Image using Google Cloud Shell Console.

Creating Virtual Gateway Image using Google Cloud Shell Console

Before creating a Virtual Gateway image using Google Cloud Shell, ensure that you have uploaded the Aruba Virtual Gateway images into Google Cloud storage. For more information, see Uploading Aruba Virtual Gateway Images into Google Cloud Storage.

For a Virtual Gateway to be able to communicate with other Virtual Gateway instances in directly connected subnets, it is required to enable **MULTI-IP-SUBNET** in the Aruba Virtual Gateway image (.tar.gz).

To enable**MULTI-IP-SUBNET** in the Aruba Virtual Gateway image, complete the following steps:

1. Log in to your Google Cloud account.
2. Navigate to **My Project** drop-down and select a **Project**.
3. Navigate to **Cloud Shell** > **Browser**.

   A Cloud Shell session appears at the bottom of the Cloud Shell console and displays a command-line prompt.

4. Enter the following command in the CLI.

```
gcloud compute images create <image-name> --project=<project-name> --source-uri=<URL to tar.gz file> --storage-location=<location> --guest-os-features MULTI_IP_SUBNET
```

The following is an example to create an image using Google Cloud Shell Console:

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to aruba-sdwan-project.
Use “gcloud config set project [PROJECT_ID]” to change to a different project.
aruba@cloudshell:~ (aruba-sdwan-project)$ gcloud compute images create aruba-vgw-xyz --project=aruba-sdwan-project --source-uri=aruba/ArubaOS_VGW_xyz.tar.gz file> --storage-location=us-east --guest-os-features MULTI_IP_SUBNET
```

```
Created [https://www,googleapis.com/compute/v1/projects/aruba-sdwan-
project/global/images/aruba-vgw-xyz
NAME                PROJECT                 FAMILY    DEPRECATED    STATUS
aruba-vgw-xyz       aruba-sdwan-project                               READY
aruba@cloudshell:~ (aruba-sdwan-project)$
```

To create VPC for a Virtual Gateway instance on Google Cloud, see Creating a VPC for Virtual Gateway Instance on Google Cloud.

Creating a VPC for Virtual Gateway Instance on Google Cloud

Before creating a VPC in Google Cloud, ensure that you have created the Virtual Gateway image using Google Cloud Shell console. For more information, see Creating Virtual Gateway Image using Google Cloud Shell Console.

To set up a Virtual Gateway instance in Google Cloud, complete the following steps:

1. Log in to your Google Cloud account.
2. Navigate to **Networking** > **VPC network** > **VPC networks**.
3. Click **Create VPC Network**.
4. Enter a name for the VPC.
5. Set the **Subnet creation mode**to **Custom**.
6. Enter the following details under New subnet.
   a. Enter a name for the subnet.
   b. Select a region.
   c. Enter an IP address range for the subnet.
   d. Click **Done**.
7. Set the **Dynamic routing mode** to **Regional**.
8. Click **Create**.

Ensure that you create four VPC networks.

To configure firewall, see Configuring Firewall in Google Cloud.

Configuring Firewall in Google Cloud

Before configuring the firewall, ensure that you have created a VPC for the Virtual Gateway instance on Google Cloud. For more information, see Creating a VPC for Virtual Gateway Instance on Google Cloud.

To configure a firewall in Google Cloud, complete the following steps:

1. Log in to your Google Cloud account.
2. Navigate to **Networking** > **VPC network** > **Firewall**.
3. Click **Create Firewall Rule**.
4. Enter a name for the firewall rule.
5. Provide a description for the new firewall rule.
6. Click the **Network** drop-down and select the newly created VPC.
7. Configure the **Priority** of the Firewall rule. The value range for Priority is 0-65535.

8. Set **Direction of traffic** to **Ingress**.
9. Set **Action on match** to **Allow**.
10. Click the **Targets** drop-down and select **All instances in the network**.
11. Click the **Source filter** drop-down and select **IP ranges**.
12. Configure the **Source IP ranges** to **0.0.0.0/0**.
13. Under **Protocols and ports**, enable **tcp**, **udp**, or **other protocols** based on your requirement.

    Enter the port numbers for **tcp** and **udp** if applicable.

It is required to configure port 4500 for Aruba Central communication and SSH port 22 to access the device.

14. Click **Create**.

To create a VM instance, see Creating a VM Instance in Google Cloud.

Creating a VM Instance in Google Cloud

Before creating a VM instance in Google Cloud, ensure that you have created configured firewall. For more information, see Configuring Firewall in Google Cloud.

To create a VM instance in Google Cloud, complete the following steps:

1. Create a new VM instance and configure the machine configuration.
2. Configure management.
3. Configure security.
4. Configure disks.
5. Configure network.

Creating VM Instance and Configuring Machine Configuration

To create a VM and configure the Machine configuration, complete the following steps:

1. Log in to your Google Cloud account.
2. Navigate to **Compute** > **Compute Engine** > **VM instances**.
3. Click **Create Instance**.
4. Enter a name for the VM instance.
5. Select a **Region**.
6. Select the **Zone**.
7. Enter the following details under **Machine configuration**:
   a. Set the **Machine family** to **General-purpose**.
   b. Set the **Series** to **N2** or **N1**.
   c. Set the **Machine type** to **n2-standard-4 (4 vCPU, 16 GB memory)**.
8. To add the boot disk image, click **Change** under **Boot disk**. The **Custom images** tab is displayed.
9. Click the **Show images from** drop-down and select your project.
10. Click the **Images** drop-down and select the Aruba Virtual Gateway image (.tar.gz).
11. Click **Done**.

Configuring Management

To configure the management, complete the following steps:

1. Go to the **Management** tab.
2. Set Metadata to Optional.
3. Set user-data to key-value pair.
4. Enter **userdata** in the **Key** field.
5. Copy and paste the content of the user data file generated in Aruba Central.

Configuring Security

To configure the security, complete the following steps:

1. Go to the **Security** tab.
2. Provide the public key in the following format: `ssh-rsa <key> vgw-user`.

To support multiple SSH keys in a Virtual Gateway deployment, only use **vgw-user** as the username while configuring the Virtual Gateway with the SSH key.

Configuring Disks

To configure the disk, complete the following steps:

1. Go to the **Disks** tab.
2. Click Add new disk.
3. Enter a name for the disk.
4. Set the **Type** to **Standard persistent disk**.
5. Set the **Source type** to **Blank disk**.
6. Set the **Size (GB)** to **16**.
7. Click **Done**.

Configuring Network

To configure the network, complete the following steps:

1. Go to the **Networking** tab and add the following networks:
   a. MGMT
   b. INET
   c. VPN
   d. LAN
2. Click **Add network interface**.
3. Select a network and subnetwork.
4. Set the Primary internal IP to Ephemeral.
5. Under External IP, set the second NIC to **Ephemeral** and other NICs to **None**.

Step 5 is applicable only while creating INET network.

6. Set the **IP forwarding** to **ON**. IP forwarding can be configured only under the first NIC. It gets enabled at the VM level and applies the same to all four NICs.
7. Click **Done**. Repeat the steps 2 to 7 to create other neworks (MGMT, INET, VPN, or LAN).
8. Click **Create**.

Connecting VM Instance to Serial Console in Google Cloud

Before connecting a VM instance to serial console in Google Cloud, ensure that you have created a VM. For more information, see Creating a VM Instance in Google Cloud.

To connect a VM instance to serial console in Google Cloud, complete the following steps:

1. Log in to your Google Cloud account.
2. Navigate to **Compute** > **Compute Engine** > **VM instances**.
3. Click the newly created VM instance to open the VM instance details window.
4. Select the check box for **Enable connecting to serial ports**.
5. Click **Save**.

Verifying the Deployment Status

To verify the Virtual Gateway deployment status, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Go to **Manage** > **Network Services** > **Virtual Gateways** > **Manual**, to view the summary page for manually orchestrated Virtual Gateways with following columns:
   - **Tenant**—Displays the name of the tenant network.
   - **Serial Number**—Displays the serial number of the Virtual Gateway.
   - **MAC Address**—Displays the MAC address of the Virtual Gateway.
   - **Model Number**—Displays the model number of the Virtual Gateway.
   - **IP Address**—Displays the IP address of the Virtual Gateway.
   - **Name**—Displays the name of the Virtual Gateway.
   - **Device Identity**—Displays the device identity of the Virtual Gateway.
   - **Status**—Displays the Enrollment over Secure Transport (EST) status of the Virtual Gateway.
3. Check if the Virtual Gateway is onboarded to the device inventory in Aruba Central .
4. Ensure that the Virtual Gateway is assigned to a device configuration group in Aruba Central.
5. Verify if the Virtual Gateway is connected to Aruba Central.
6. Configure a VPN tunnel between a Branch Gateway and the Virtual Gateway.

To check the Virtual Gateway operational status and the VPN tunnel status follow these steps:

1. In the **Network Operations** app, use the filter to select the gateway
2. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway.
3. The dashboard context for a group is displayed.
4. Under **Manage**, click **Devices** > **Gateways**. A list of gateways is displayed in the **List** view.
5. Click a gateway under **Device Name**. The dashboard context for the gateway device is displayed.
6. Go to **Manage** > **Overview**.

For more information, see the Gateway monitoring help topic in *Aruba Central Help Center*.

Deploying Aruba Virtual Gateways in MSP (Unmanaged Mode)

Aruba Central supports deploying Virtual Gateways in the Managed Service Providers (MSP) mode. In the unmanaged mode, IT administrators bring up and configure the Virtual Gateway instances and monitor the deployed Virtual Gateways from the MSP mode of Aruba Central.

Deployment Procedure

Before deploying Aruba Virtual Gateway for MSP, ensure that you have the following resources and account privileges:

- An Aruba Central account with MSP mode enabled.
- Administrator credentials to deploy the Aruba Virtual Gateway in MSP mode.
- A valid license for an Aruba Virtual Gateway. To check the list of available Virtual Gateway models for MSP mode, see Virtual Gateway Sizing
- Download the Aruba Virtual Gateway image from the Aruba Support Portal. For more information, contact your Aruba Sales Specialist.

Virtual Gateway Sizing

The Aruba Virtual Gateway in MSP mode has a minimum throughput of 500 Mbps, and can support up to 1600 IPsec tunnels. This table lists out the supported Virtual Gateway models for MSP mode:

Aruba Model/SKU Name	Throughput	vCPU	RAM Memory (GB)	Flash Memory (GB)	Tunnels
VGW-500MB	500 Mbps	4	7	15	1600
VGW-2GB	2 Gbps	8	15	30	4096
VGW-4GB	4 Gbps	16	30	60	8192

If a higher number of tunnels are required, contact your Aruba Sales Specialist.

Deploying Virtual Gateway in MSP Mode

To deploy a Virtual Gateways in MSP mode, complete the following steps:

1. Log in to Aruba Central in MSP mode.
2. In the **Network Operations** app, set the filter to **Global**.
3. Go to **Manage** > **Network Services** > **Virtual Gateways**. The **Config** view is set by default and the Unmanaged Virtual Gateway (Manual Workflow) page is displayed.
4. From the **Select VGW Model** drop-down menu, select an available Virtual Gateway model.
5. From the **Select Customer** drop-down menu, select or type the name of a customer.
6. From the **Select Group** drop-down menu, select or type the name of a group.
7. Click **Create Device Identity** to create the Virtual Gateway with a unique identity.

8. Click **Yes** to confirm the identity creation. Aruba Central displays the newly created Virtual Gateway with the following fields:
   a. **Serial #**—Displays the serial number of the Virtual Gateway.
   b. **MAC**—Displays the MAC address of the Virtual Gateway.
   c. **Model Number**—Displays the model number of the Virtual Gateway.
   d. **Device Identity**—Displays the device identity of the Virtual Gateway.
   e. **Status**—Displays the status as Userdata Generated for the created device identity of the Virtual Gateway.
9. Assign a license to the Virtual Gateway.
10. Navigate to **Account Home** > **Device Inventory** to view the newly added Virtual Gateway along with the assigned license.

1. Virtual Gateways can be deployed in MSP mode only.
2. When a Virtual Gateway is deployed, it is tied to a tenant and cannot be moved to another tenant.
3. A Virtual Gateway cannot be unassigned from a tenant. To delete a Virtual Gateway, navigate to **Manage** > **Network Services** > **Virtual Gateways** from the unmanaged mode.
4. A Virtual Gateway cannot be unassigned a from **Device Inventory**.

Provisioning Virtual Gateways to Groups

Virtual Gateways are the virtualized instance of Headend Gateways.

Before provisioning the Virtual Gateways, ensure that you assign Virtual Gateways to a VPNC group. For more information see Assigning a Group Role to an Aruba Gateway Group.

For information on configuring VPNCs, see Configuring an SD-Branch Network Using the Advanced Setup.

Troubleshooting Deployment Issues

If you have configured a key pair for the VPC, you can log in to Virtual Gateway console through SSH for verifying the deployment status.

Ensure that you open port 22 before accessing the console.

To log in to the console:

1. Open an SSH client.
2. Log in to console using the key pair and public IP address of the instance.

```
ssh -i "<key pair name>.pem" ec2-admin@<public IPv4 address>
```

3. Execute the following commands to verify the deployment status:

```
show ip interface brief
show ip route
show configuration effective | begin 0/0/0
```

4. To verify the status of EST enrollment, use the following commands:

```
show est profile vgw_est_srv
```

5. To verify the Aruba Central URL:

```
show aruba-central details
```

High Availability Support for Aruba Virtual Gateways

The High Availability (HA) solution for Aruba Virtual Gateways (Virtual Gateway) works in an Active-Passive paired configuration. In this setup there can be only one active Virtual Gateway which can forward data in and out of the Virtual Private Cloud's (VPC) connected subnets.

The Virtual Gateway Orchestrator app decides which of the virtual gateways becomes Active or Passive and communicates this decision to all the pivotal components.

The decision of setting the Active or Passive virtual gateway is based on the following requirements:

- Virtual machine health of each of the virtual gateways in a given HA-pair.
- The health of the Virtual Gateways control connectivity to the Central Overlay Router Orchestration component.
- The connectivity of each of the virtual gateways to all the Branch Gateways (BGW).

The Orchestration app decides the status based on the state of each virtual gateway. The app runs a poll every 20 seconds on each virtual gateway for these criteria:

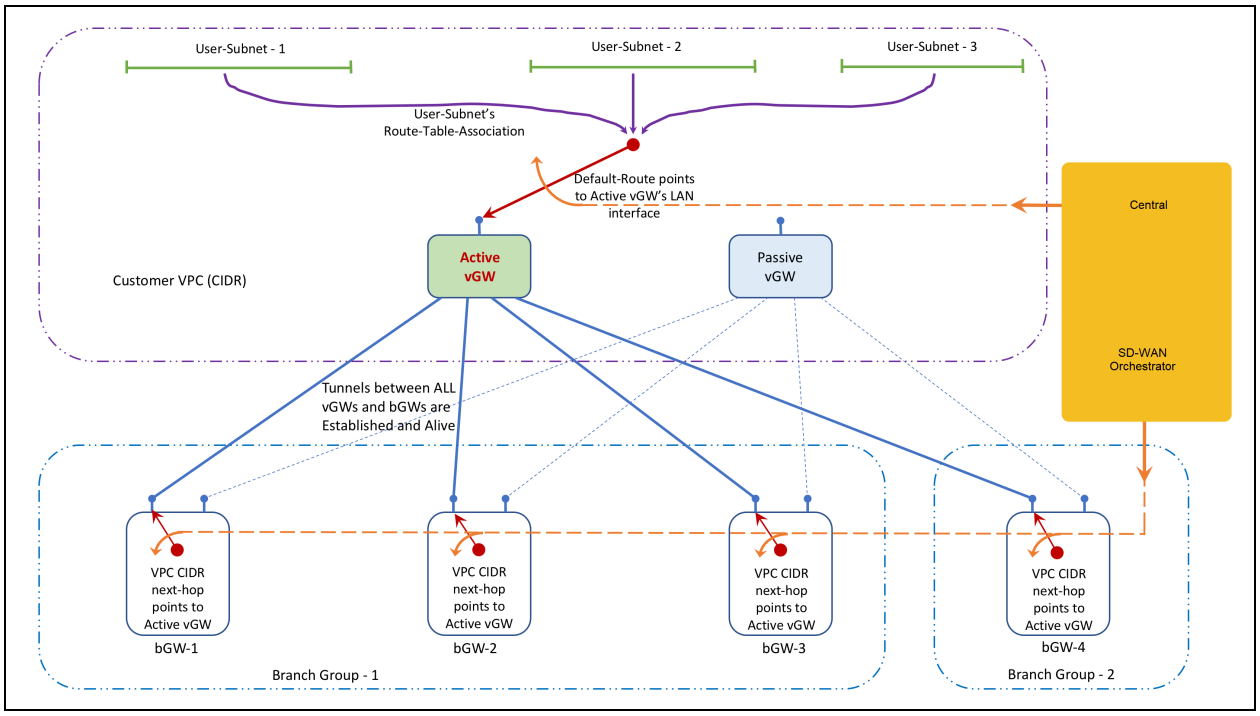
- VM Health: The VM health status is obtained from the cloud app (AWS, Microsoft Azure, VMware ESXi) for each of the gateways in all the VPCs or VNETs across each of the regions of a given cloud account.
- Control Health: The control health status is provided by the Overlay Route Orchestrator module.
- Data and Tunnel Health: The data and tunnel health status is provided by the Overlay Route Orchestrator module.

Definition of connected and disconnected:

- A pair of end-points are declared connected, if there is at least one tunnel that both sides (Virtual Gateway and Branch Gateway) have declared as being connected.
- A pair of end-points are declared disconnected, if all the configured tunnels have at least one side being declared as disconnected.

After the Orchestration app marks one of the virtual gateways as Active, there maybe some branches that lose connectivity (to the cloud), if they don't have at least one live tunnel connection to the chosen (Active) Virtual Gateway.

Figure 427 *Overview of High Availability Virtual Gateway*



Configuration using Overlay Route Orchestrator/Overlay Tunnel Orchestrator Service-Configuration

1. Create a pair of HA virtual gateways in a VPC.
2. Assign this HA-Pair to an exclusive "Managed Group" (consisting of only these two Virtual Gateway paired devices) marked with a VPNC persona.
3. Configure the chosen hub-group:

a. Configure all the connected subnets that are to be part of the chosen (hub) group's DC-Aggregate-Routes: Hub-Group > VPN > DC Aggregate Routes >Add subnets and masks to be advertised.

b. Disable the **Allow branch-to-branch:**. Use this option to disable branch to branch communication through the virtual gateway.

4. Configure individual Virtual Gateway devices:

a. configure the WAN interfaces: Ge-0/0/0 (INET GW) and Ge-0/0/1 (VPN GW) - typically on the vlan-4094 interface.

b. configure the VPC-CIDR reachability through GE-0/0/2 (eth3 interface subnet) AWS or cloud router's IP.

- Example:
- Virtual Gateway-Instance-0: AWS-router-IP: A.B.C.97
- Virtual Gateway-Instance-1: AWS-router-IP: A.B.C.225

A.B.C.0/24 is the reserved subnet chosen during the Virtual Gateway-Deployment phase.

5. Configure a given Branch Group's connectivity through Service Config:

a. Configure Overlay Orchestration: Branch-Group >VPN > Orchestration mode: **Orchestrated**.
b. Configure DC connectivity: Branch-Group >VPN >DC Preference >Add the Virtual Gateway-Hub-Group, choosing both the Virtual Gateway paired devices.

6. You may add this Virtual Gateway pair to one or more Branch Groups.

Configuration triggered message distribution and collection channels

Adding the Virtual Gateway pair to the Branch Group(s) initiates the addition of these Virtual Gateway pairs into one or more Multicast/Distribution Groups in the Overlay Route Orchestrator modules. There is one distribution group for each of the Branch Groups. This is a vital operation that binds the relationship between the Virtual Gateway Orchestrator app and the Overlay Route Orchestrator modules for each of the given Virtual Gateway device.

The Overlay Route Orchestrator creates a per-device based, unique topic to which the Virtual Gateway Orchestrator can publish its selection results. The decisions made are relayed to all the relevant devices in the distribution (all the branch-devices of all the interested Branch Groups).

The Virtual Gateway Orchestrator app communicates to the Overlay Route Orchestrator. The message could be either of the following:

- a HA-Selection Update message
- a Delete message

A HA-Selection Update message can further indicate whether a Virtual Gateway device has become Active or Passive. Changes to the Service-Config or Branch-to-Hub association will initiate a change in the Topic list and in the corresponding distribution channels.

Logical Flow Chart

The steps listed here, outline the logic used:

1. Virtual Gateway Orchestrator decides which Virtual Gateway with will be set as Active or Passive either if there is a service disruption or at initialization.
2. The Virtual Gateway Orchestrator runs a poll periodically and decides who the new Active or Passive Virtual Gateway is based on the criteria listed here:
    a. VM health
    b. Control health
    c. Tunnel and Datapath health

   If there is a change in the Active or Passive Virtual Gateway, the Orchestrator app updates the database.

3. The Active or Passive status decision is broadcast to the distribution lists and branch-groups of the Branch Gateways.
4. After the Branch Gateway receives the update, it either de-activates or re-activates the concerned Virtual Gateway (tunnel) in its DC/VPC prefix next-hop calculations for the Branch Gateway.
5. A message is sent to the updated Virtual Gateways, ensuring the that they are aware of the change regarding the updated Active or Passive status.

Active or Passive Selection Truth-Table (Version 1)

In the current version, there is no user interactive option available to select the preferred Virtual Gateway. The Virtual Gateway app has support to set the preferred Virtual Gateway using RestAPI. If both the Virtual Gateways are of equal operational quality, then the preferred Virtual Gateway is chosen to be the Active of the paired-Virtual Gateways.

In this table an "X" indicates that the value is of no consequence.

Virtual Gateway-A			Virtual Gateway-B			Previous Active	Preferred Virtual Gateway	Section Result		Description	Result
VM Health	gRPC Health	Tunnel Health	VM Health	gRPC Health	Tunnel Health			Active	Passive		
Down	Down/None	0 / None / X	Down	Down/None	0 / None / X	Virtual Gateway-A	Virtual Gateway-A	Virtual Gateway-A	Virtual Gateway-B	No action required	No traffic flow
Down	X	X	Down	X	X	Virtual Gateway-A	X	Virtual Gateway-A	Virtual Gateway-B	No action required	No traffic flow
X	Down/None	X	X	Down/None	X	X	X	X	X	Unusable	No traffic flow
X	X	0 / None	X	X	0 / None	X	X	X	X	Unusable	No traffic flow
Down	X	X	Up	At least one of the two columns changes to: Down/0/None		Virtual Gateway-A	X	Virtual Gateway-B	Virtual Gateway-B	Unusable	No traffic flow
Down → Up	At least one of the two columns changes to: Down/0/None		Up or Down	At least one of the two columns changes to: Down/0/None		Virtual Gateway-B	Virtual Gateway-A	Virtual Gateway-A	Virtual Gateway-A	Unusable	No traffic flow
At least one of the three columns changes to: Down/0/None			Up	Up	>=1	Virtual Gateway-A	X	Virtual Gateway-B	Virtual Gateway-B	HA failover triggered, Virtual Gateway_B is the only option	Distribute HA-Selection message(s)
Down → Up	Down → Up	0 → 1	Up	Up	=1	Virtual Gateway-B	X	Virtual Gateway-B	Virtual Gateway-B	Retain the previous selection, both options	No switching required

Virtual Gateway-A			Virtual Gateway-B			Previous Active	Preferred Virtual Gateway	Section Result		Description	Result
VM Health	gRPC Health	Tunnel Health	VM Health	gRPC Health	Tunnel Health			Active	Passive		
										are viable	
Up	Up	> 1	Up	Up	=1	Virtual Gateway-B	X	Virtual Gateway-A	Virtual Gateway-B	Virtual Gateway-A is prefferred over Virtual Gateway-B	Distribute HA-Selection message(s)
Up	Up	2 → 1	Up	Up	=1	Virtual Gateway-A	X	Virtual Gateway-A	Virtual Gateway-B	Retain the previous selection, both options are viable	No switching required
At least one of the three columns changes to: Down/0/None			Up	Up	>=1	Virtual Gateway-A	X	Virtual Gateway-B	Virtual Gateway-A	Virtual Gateway-B is prefferred over Virtual Gateway-A	Distribute HA-Selection message(s)

As noted in the Truth table version 1, if one or both the Virtual Gateway's Overlay Route Orchestrator state changes, which in-turn results in equal quality of Overlay Route Orchestrator connectivity, there is no change to the Active device allocation.

CREDIT-BASED HA Switchover

In the current setup there is no dampening in the Virtual Gateway HA logic, and this leads to the HA triggering based on differences between a pair of Virtual Gateways, resulting in any event, such as adding or deleting Branches resulting in momentarily altering the connectivity count and triggering an unwanted HA mode change.

The introduction of a CREDIT-BASED HA switchover solution dampens the switchover that may be caused by the changes of tunnel connectivity.

CREDIT-BASED Logic for Tunnel Connections

Instead of using Hold-Off-Time switchover to monitor status of tunnel connections of Virtual Gateways, a CREDIT-BASED logic reduces the number of unnecessary switchovers using THRESHOLD and STABLE_TIME_ELAPSED.

VM health status: **Hold-Off-time**

GRPC/Control status: **Hold-Off-Time**

Tunnel connections: **CREDIT-BASED Logic**

How does CREDIT-BASED Logic work

When a new pair of Virtual Gateways is deployed, a credit is assigned to this pair of Virtual Gateways. The credit calculation is listed here:

- The Active Virtual Gateway gets MAX_CREDIT. The default value is 60.
- The Passive Virtual Gateway gets MIN_CREDIT. The default value is 0.
- Adding the credit of the Passive Virtual Gateway with the credit of the Active Virtual Gateway gives us the MAX_CREDIT.

Virtual Gateway app will keep incrementing or decrementing credit on a pair of Virtual Gateways based on these situations:

- When a Passive Virtual Gateway has more tunnel connections than the Active Virtual Gateway:
- the credit of Passive Virtual Gateway is incremented by one
- the credit of Active Virtual Gateway is decremented by one

- When a Passive Virtual Gateway has more tunnel connections than the Active Virtual Gateway:
- the MAX_CREDIT is reset to the Active Virtual Gateway
- the MIN_CREDIT is reset to the Passive Virtual Gateway

Important Constants:

Sample or Snapshot interval = 20 seconds

MAX_CREDIT = 60

MIN_CREDIT = 0

DOWN_THRESHOLD = 1 (Default)

UP_THRESHOLD = 10 (Default)

Calculation:

STABLE_TIME_ELAPSED = ((MAX_CREDIT / 2) + 1) * 20 Seconds

For example: ((60/ 2) + 1) * 20 Seconds = 10 Minutes

NO_CHANGE_TIME = STABLE_TIME_ELAPSED * 10

For example: 10 Minutes * 10 = 100 Minutes

Credit Based Active and Passive selection

Listed here are a few practical examples of Credit Based Active and Passive Virtual Gateway selection:

The Active Virtual Gateway is the preferred choice:

- The Active Virtual Gateway has more data tunnels connections (Active gets MAX_CREDIT, Passive gets MIN_CREDIT)
- The Passive Virtual Gateway has more data tunnels connections but the Active Virtual Gateway is preferred based on:
- Both Active and Passive Virtual Gateways tunnel connections are growing (Active gets MAX_CREDIT, Passive gets MIN_CREDIT)
- Passive Virtual Gateway tunnel connections is decreasing (Active gets MAX_CREDIT, Passive gets MIN_ CREDIT)

The Passive Virtual Gateway is the preferred choice:

- Passive Virtual Gateway has more data tunnels connections:
- Active Virtual Gateway data tunnels connection is stable or is decreasing. The Passive Virtual Gateway data tunnel connections are stable or is growing (Passive Virtual Gateway: credit + 1, Active Virtual Gateway: credit - 1)
- HA switchover takes place when credit of the Passive Virtual Gateway is more than the credit of the Active Virtual Gateway (Passive Virtual Gateway credit > Active Virtual Gateway credit)

- Immediate HA switchover (HOLD-OFF) initiated if:

  1. The credit of the Active Virtual Gateway data tunnel connections=0 (the Active Virtual Gateway tunnel status is DISCONNECTED)
  2. The status of the Active Virtual Gateway is decreasing and all of the following criteria are met:

     a. Passive Virtual Gateway is stable or growing
     b. No crossover between Active Virtual Gateway and Passive Virtual Gateway, and no HA switchover was triggered for an extended time period that is defined by: >=STABLE_ TIME_ELAPSED)
     c. The Passive Virtual Gateway data tunnels - The Active Virtual Gateway data tunnels >= DOWN_THRESHOLD

  3. Active Virtual Gateway is slowly growing and all of the following criteria are met:

     a. The Passive Virtual Gateway is stable for enough time. The stable time is that is defined by: stable time >= STABLE_TIME_ELAPSED)
     b. The Passive Virtual Gateway data tunnels - The Active Virtual Gateway data tunnels >= UP_THRESHOLD

The Passive Virtual Gateway equal to The Active Virtual Gateway:

- Immediate HA switchover occurs if the following criteria are met:

     a. If they are both equal and no statuses changes (VM health, Control health, Tunnel health, and credit) for extended period time that is defined by: Current time - last time updated on both two Virtual Gateways >= NO_CHANGE_TIME
     b. Passive Virtual Gateway is the preferred Virtual Gateway

Monitoring Virtual Gateways

To view the Virtual Gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one Branch Gateway. The dashboard context for a group is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.
3. A list of gateways is displayed in the **List** view.
4. Click a gateway under **Device Name**.
5. The dashboard context for the gateway device is displayed.
6. Under **Manage**, Click **Overview**.

For more information, see Configuring an SD-Branch Network Using the Advanced Setup.

You can monitor gateways in Aruba Central from all the available dashboards including **Global**, **Groups**, **Sites**, **Labels**, and **Gateways**.

For a snapshot of all the gateways configured at the global, group or site level, in either list or summary view, see the following topics:

- Monitoring Gateway in the List View
- Monitoring Gateways in the Summary View

Monitoring Gateways in List View

The **List** view for gateways is available from the **Global**, **Group**, **Site**, and **Label** dashboards. In all applicable dashboards, the **List** view is under **Manage** > **Devices** > **Gateways**.

To view the list of gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   Ensure that the selected option has at least one gateway configured.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.

List View

The list view displays the following tabs:

- **Gateways**—Displays the total number of gateways configured.
- **Online**—Displays a list of gateways that are online and connected to Aruba Central.
- **Offline**—Displays a list of Gateways that are currently down.

List View > Gateways

The **Gateways** table displays the following details for **Gateways**, **Online** and **Offline** tabs:

- **Device Name**—Displays the gateway name.
- **Model**—Displays the model of the gateway.
- **Firmware Version**—Displays the firmware version of the gateway.
- **Uptime**—Displays the time period for which the gateway has been functioning.
- **IP Address**—Displays the IP address of the gateway.
- **Site**—Displays the site information.
- **MAC**—Displays the MAC address of the gateway.
- **Group**—Displays the gateway group name.

- **Labels**—Displays the labels assigned to the gateway.
- **Serial**—Displays the gateway serial number.

Apart from the above fields, you can see the following fields if IDPS is enabled:

- **Inspection Engine**—The Aruba IDPS engine version number.
- **Ruleset**—The ruleset version currently running on the device.
- **Last Successful Ruleset Update**—The timestamp of the last successful ruleset update.
- **Ruleset Update Status**—The ruleset update status could be one of the following:
  - **Failed**
  - **Success**
  - **Initialized**

Click the download icon to download the gateways details as a .csv file. For more information, see Downloading Gateway Details.

Click the ellipsis icon to perform the following additional operations:

- Select the columns that you want to display in the table.
- Adjust the column width of the table to fit the page evenly.
- Reset the table view to the default columns.

Monitoring Gateways in Summary View

The **Summary** view for gateways is available from the **Global**, **Groups**, **Sites**, and **Labels** dashboards. In all applicable dashboards, the **Summary** view is under **Manage** > **Devices** > **Gateways**. Displays a graphical representation of the gateway operations.

To view the summary of gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   Ensure that the selected option has at least one gateway configured.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices**>**Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click the **Summary** icon.

   A graphical representation of the gateway operations is displayed.

You can change the time range by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

If you have just set up a gateway, you may not see relevant data immediately.

Summary View

The **Summary** view displays a graphical representation for the following:

- **Usage**—Displays the overall usage metrics for the gateways provisioned in your Aruba Central account. Displays the incoming and outgoing traffic for the gateways with time plotted on the x-axis. You can

hover over the chart to see the incoming and outgoing traffic for a particular time frame.

- **WAN Compression**—Displays the data packet compression statistics for the WAN network. You can view the compressed, uncompressed, and saved bandwidth. By default, traffic between the Branch Gateway and VPNC is subject to compression. You can hover over the chart to see the compressed and uncompressed statistics for a particular time frame.
- **WAN Tag Provider Distribution**—Displays the number of online and offline uplinks per WAN provider.
- **WAN Transport Health**—Displays the Mean Opinion Score (MOS) score trends for each uplink for the selected time range. The uplink health trend is plotted using health indicators such as Good, Fair, and Poor. You can hover over the chart to see the uplink scores for a particular time frame. Click an uplink name to show or hide MOS score trends for that uplink.
- **WAN Type Provider Distribution**—Displays the number of online and offline uplinks per WAN circuit type.
- **Model Distribution**—Displays the total percentage of gateways distributed per hardware platform. You can hover over a donut slice to display the percentage for a specific hardware model. Click a hardware platform number to show or hide the distribution percentage for that platform.
- **Firmware Distribution**—Displays the total percentage of gateways distributed by software versions. Click a firmware number to show or hide the distribution percentage for that firmware.

Gateway > Overview > Summary

The **Summary** tab under **Manage** > **Overview** in the gateway dashboard displays the following three sections:

- Device Info
- WAN Summary
- Health Status

Viewing the Overview > Summary Tab

To navigate to the **Summary** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Summary** .

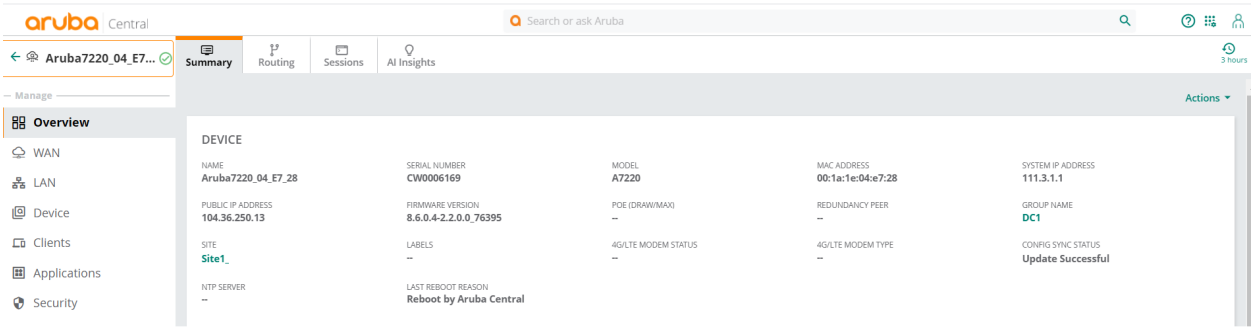
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Device Info

The **Device Info** section displays the following details.

Figure 428 *Device Info*

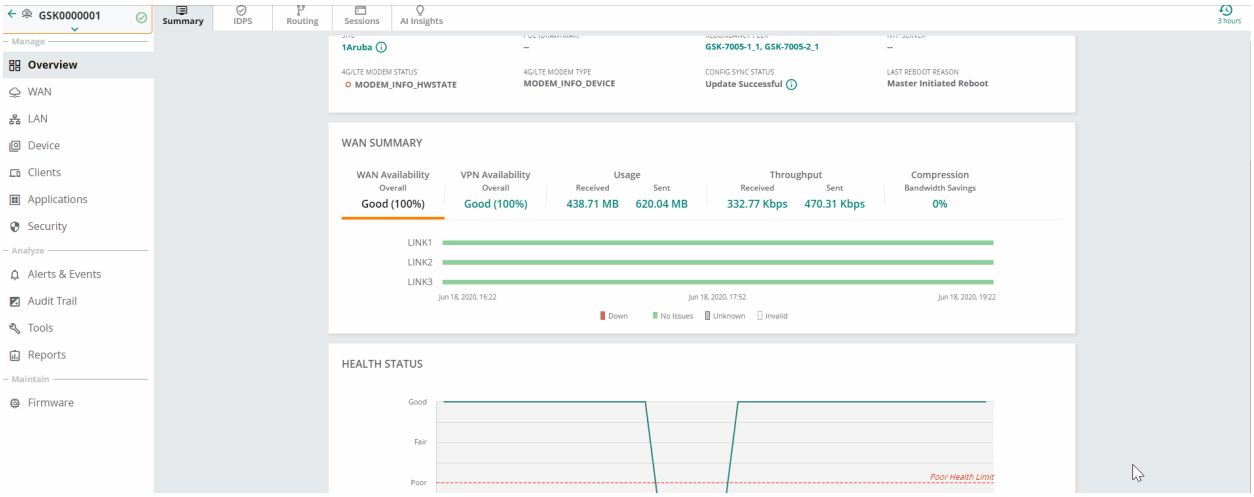


- **Name**—The name of the gateway.
- **Serial Number**—The serial number of the gateway.
- **Model**—The hardware model of the gateway.
- **MAC Address**—The MAC address of the gateway.
- **System IP address**—The IP address of the gateway.
- **Public IP address**—The public IP address of the gateway.
- **Firmware Version**—The firmware version running on the gateway. If a new version of the firmware is available, this information is also displayed. Clicking on the new firmware version redirects you to the **Maintain** > **Firmware** > **Gateways** page in the gateway dashboard, where you can select the gateway to be upgraded.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the Branch Gateway consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **Redundancy Peer**—Displays the redundant gateway if it is configured. Click the link to view the redundant gateway details.
- **Group Name**—The name of the group, if the gateway is configured as part of a group. Click the group name to go to the **Overview** > **Summary** page for that group.
- **Site**—The name of the site, if the gateway is configured as part of a site. Hover over the i icon to display the complete address of the site. Click the site name to go to the **Overview** > **Site Health** page for that site.
- **Labels**—The name of the label, if the gateway is configured as part of a single or multiple labels.
- **4G/LTE Modem Status**—Displays the modem connectivity status. The status shows only 'Connected' when the modem type is not internal.
- **4G/LTE Modem Type**—Displays the LTE connection type.
- **Config Sync Status**—The status of the configuration sync. Hover over the information icon to display the last successful configuration sync time.
- **NTP Server**—The name of the NTP server configured and its synchronization status.
- **Last Reboot Reason**—The reason for the last reboot.
- **Internal Modem Status** (Only for Gateway model: 9004-LTE)—Displays the name of the service provider and the signal strength. Hover over the information icon to view details about the active SIM, the IMEI number and the phone number.

WAN Summary

The **WAN Summary** section displays information of WAN Availability, VPN Availability, Usage, Throughput, and Compression.

Figure 429 *WAN Summary*



- **WAN Availability**—Provides a graphical representation of the WAN uplink availability for the Branch Gateway. The graph displays each WAN uplink availability for the selected time range. Availability is determined by the default gateway and monitored IP reachability. You can hover over the chart to see the WAN availability statistics for a particular time frame.
  - Red—Down
  - Yellow—(>50) Partial availability
  - Green—No Issues
  - Gray—Unknown
  - Dotted lines—Invalid
- **VPN Availability**—Provides a graphical representation of the VPNC reachability for the Branch Gateway. Availability is determined by the probe settings configured using the **Health Check** option.
  - Red—Down
  - Yellow—>50 percent availability
  - Green—No Issues
  - Gray—Unknown
  - Dotted lines—Invalid
- **Usage**—Displays the aggregate sent and received traffic usage by the WAN interface for the Branch Gateway. Displays the incoming and outgoing traffic for the gateways with time plotted on the x-axis. You can hover over the chart to see the incoming and outgoing traffic for a particular time frame. Select one of the following options from the drop-down list:
  - All
  - Internet
  - VPN

Click the following icons to see the chart in logarithmic scale or linear scale.

- Logarithmic Scale—Click this icon to view chart in logarithmic scale.
- Linear Scale—Click this icon to view chart in linear scale.

Click **Received** or **Sent** at the bottom of the chart to view or hide the usage chart for received or sent data.

- **Throughput**—Provides a graphical representation of the aggregated WAN interfaces throughput. The graph displays the transmit and receive performance in bps for a WAN interface. Displays the incoming and outgoing traffic for the gateways with time plotted on the x-axis. You can hover over the chart to see the received and sent throughput for a particular time frame.

Click the following icons to see the chart in logarithmic scale or linear scale.

- Logarithmic Scale—Click this icon to view chart in logarithmic scale.
- Linear Scale—Click this icon to view chart in linear scale.

Click **Received** or **Sent** at the bottom of the chart to view or hide the usage chart for received or sent data.

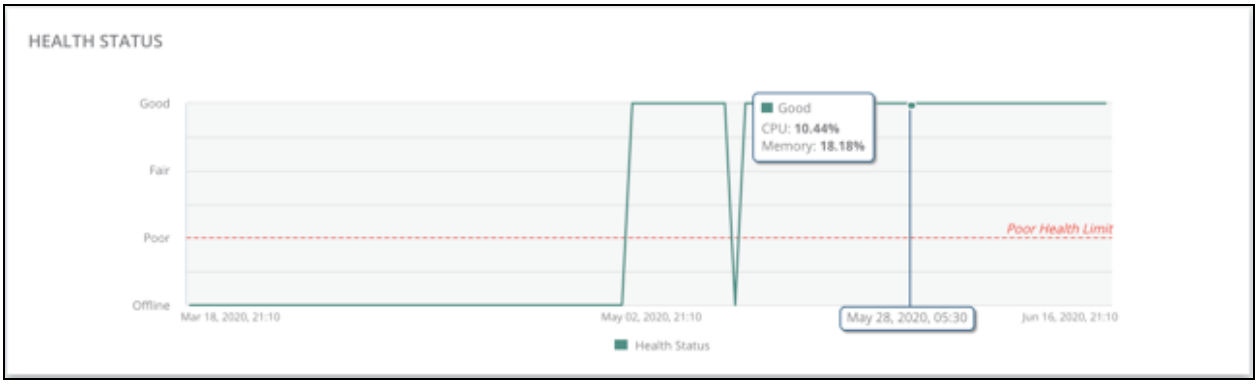
- **Compression**—Displays the aggregate WAN compression details across all uplinks. The average bandwidth savings is displayed as a percentage. The compressed and uncompressed bandwidth is displayed as vertical grouped bar graphs. You can hover over the chart to see the bandwidth savings statistics for a particular time frame.
  - Gray—Optimized
  - Red—Non Optimized

Health Status

The **Health Status** section displays the health of the gateway in terms of CPU, Memory, and device connectivity to Aruba Central.

The health status is plotted using health indicators such as Good, Fair, Poor, and Offline. You can hover over the chart to see the health status for a particular time frame.

Figure 430 *Health Status*



NOTE

The default view of gateways table shows only a few columns. To view the hidden columns, click the settings icon at the right side of the table. To reset the columns, click **Reset Columns**.

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

1. Under **Manage**, click **Devices** > **Gateways**.
2. Click a gateway under **Device Name**.
3. Under **Manage**, click **Overview.** By default, the **Summary** tab is displayed.

- **WAN**—Displays the total number of WAN interfaces that are currently operational or down. On clicking a port, the dashboard displays WAN interface details.
- **LAN**—Displays the total number of LAN interfaces that are currently operational or down. On clicking a port, the dashboard displays LAN and VLAN interface details.
- **Tunnels**—Displays the total number of VPN tunnels that are currently active or down. On clicking a port tunnel, the dashboard displays VPN tunnel details.
- **IDPS**—Displays details pertaining to the IDPS traffic inspection engine health and the number of packets dropped. The **IDPS** tab is displayed for 9004 gateways with a valid IDPS subscription.
- **Routing**—Displays details pertaining to the routing protocols such as BGP, OSPF, RIPv2 and Overlay.
- **Path Steering**—Displays the total number of path steering policies that are compliant with the performance criteria (SLAs) defined for each type of traffic.
- **Sessions**—Displays detailed information about the running sessions.
- **AI Insights**—Displays a report of network events that could possibly affect the quality of the overall network performance.
- **Alerts**—Displays the total number of open alerts that are yet to be acknowledged.

Gateways > Overview > IDPS

The **IDPS** tab under **Manage** > **Overview** in the gateway dashboard displays the following sections:

- Traffic Inspection Engine Status
- Traffic Inspection Engine CPU Usage
- Traffic Inspection Engine Memory Usage
- Dropped Packets

After you on-board the gateways and configure IDPS, you can view the IDPS traffic engine health and the number of packets dropped.

Viewing the Overview > IDPS Tab

To navigate to the **IDPS** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites** that has IDPS supported gateways. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.
   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.
   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **IDPS** .

To exit the gateway dashboard, click the back arrow on the filter.

You can change the time range for the **IDPS** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

NOTE

To set the charts to show data for specific duration, use the options in the time range filter. By default, the data is displayed for a duration of 3 hours. To view the graphs for different durations, click the time filter icon and select a time range of your choice. You can view data for 3 hours, 1 day, 1 week, 1 month, or 3 months. The **IDPS** tab is displayed for 9004 gateways with a valid IDPS subscription.

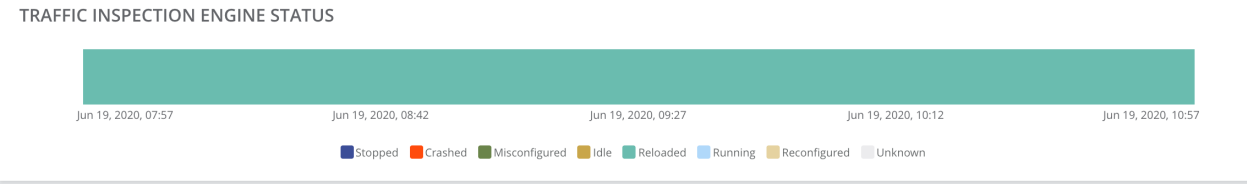
Traffic Inspection Engine Status

The **Traffic Inspection Engine Status** chart displays the status of the traffic inspection engine for the selected period in a timeline chart. Hover over the graph to view the status of the traffic inspection engine at a particular time. The legends represent different status of the traffic inspection engine.

NOTE

The **Traffic Inspection Engine Status** chart is available for a period of 3 hours, 1 day, 1 week, or 1 month.

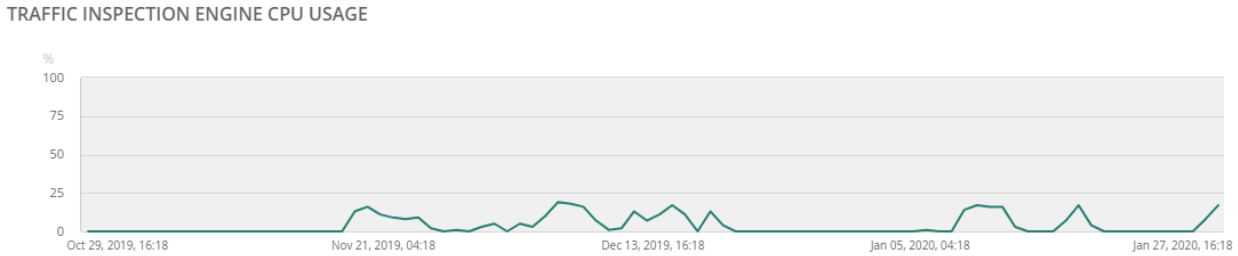
Figure 431 *Traffic Inspection Engine Status*



Traffic Inspection Engine CPU Usage

The **Traffic Inspection Engine CPU Usage** chart displays the CPU usage percentage of the traffic inspection engine for the selected period in a line chart. Hover over the graph to view the CPU usage percentage at a particular time.

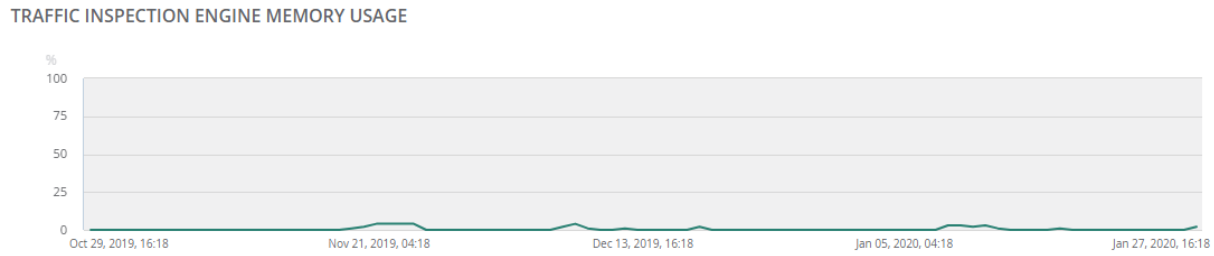
Figure 432 *Traffic Inspection Engine CPU Usage*



Traffic Inspection Engine Memory Usage

The **Traffic Inspection Engine Memory Usage** chart displays the percentage of memory usage by the traffic inspection engine for the selected period in a line chart. Hover over the graph to view the memory usage percentage at a particular time.

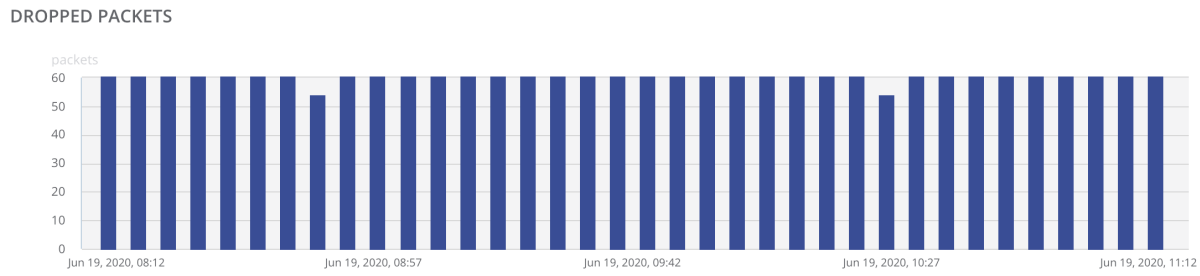
Figure 433 *Traffic Inspection Engine Memory Usage*



Dropped Packets

The **Dropped Packets** chart displays the number of packets dropped for the selected period in a vertical bar chart. Hover over the graph to view the packets dropped at a particular time.

Figure 434 *Dropped Packets*



Gateway > Overview > Routing

The **Routing** tab under **Manage** > **Overview** in the gateway dashboard displays the following sections:

- Gateway > Overview > Routing > Route Table
- Gateway > Overview > Routing > BGP
- Gateway > Overview > Routing > OSPF
- Gateway > Overview > Routing > Overlay
- Gateway > Overview > Routing > RIP

Viewing the Overview > Routing Tab

To navigate to the **Routing** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** .

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Routing** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Gateway > Overview > Routing > Route Table

The **Route Table** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- Routes Summary
- Routes

Viewing the Overview > Routing > Routes Table Tab

To navigate to the **Routes Table** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **Routes Table**.

   To exit the gateway dashboard, click the back arrow on the filter.

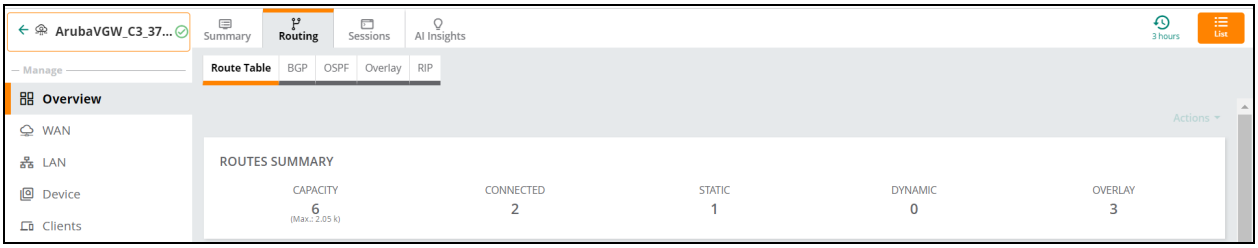
   You can change the time range for the **Routes Table** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Routes Summary

- **Capacity**—Number of routes currently configured. Also displays the maximum number of allowed routes.
- **Connected**—Number of connected routes.
- **Static**—Number of static routes.

- **Dynamic**—Number of dynamic routes.
- **Overlay**—Number of overlay connections.

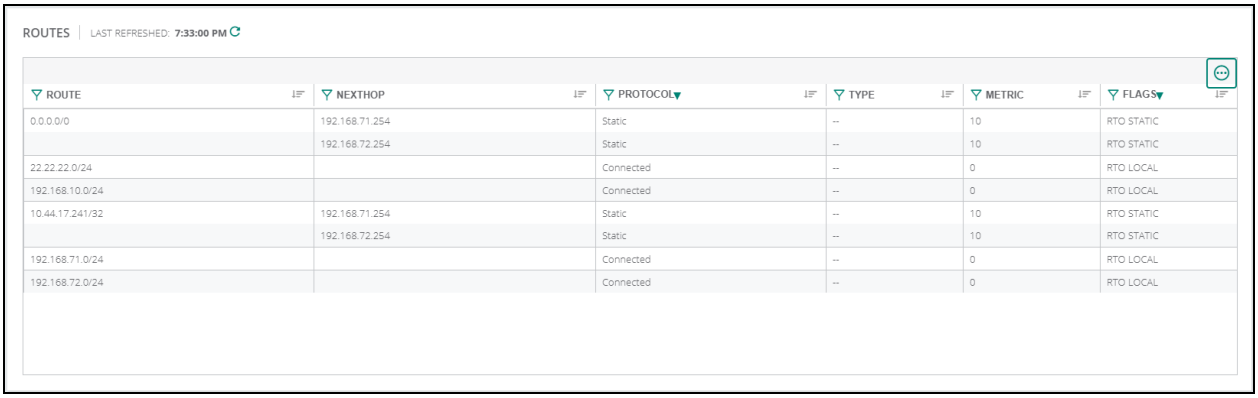
Figure 435 *Routes Summary*



Routes

- **Last Refreshed**—Indicates the time, in hr:mm:ss format, when the routes were last refreshed.
- **Prefix**—Controller prefix for the route.
- **Length**—Prefix length.
- **Address**—Destination IP address of the route.
- **Route**—The route IP address and subnet.
- **Nexthop**—The IP address of the next hop.
- **Protocol**—Routing protocol. Possible values are Unknown, Connected, Static, IKE, Overlay, BGP, OSPF, BOC, RAPNG, RIP, VPN, Application and Default
- **Type**—The type of connection.
- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
- **Flags**—Route flags that indicate the flags for the selected routes.

Figure 436 *Routes details*



NOTE

Click the settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to type in an applicable value, and then display the corresponding row. For Protocol column you can select a value from the drop-down list.

Click the icon on on each column header row to arrange the data in ascending or descending order.

Click the refresh icon on the Routes table to refresh the table data.

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Overview > Routing > BGP

The **BGP** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- BGP Summary
- BGP Details
- BGP Details > Neighbors
- BGP Details > Routes

Viewing the Overview > Routing > BGP Tab

To navigate to the **BGP** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in List view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **BGP**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **BGP** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

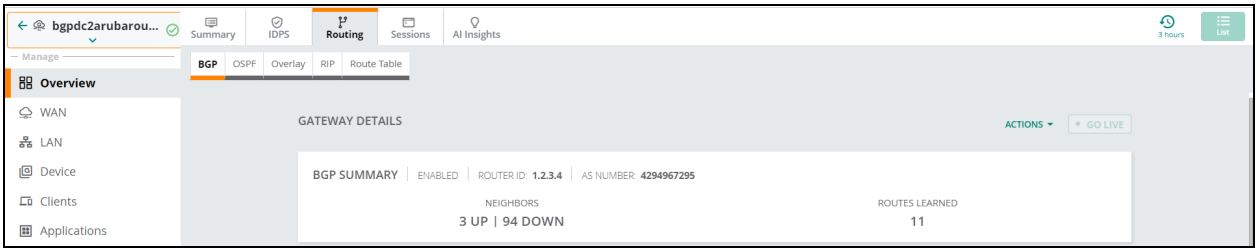
BGP Summary

The **BGP Summary** section displays the following information:

- **Router ID**—Displays the Router ID.
- **AS Number**—Displays the private Autonomous System (AS) number.

- **Neighbors**—Displays the number of neighboring connections.
- **Routes Learned**—Displays the number of routes that have been learned.

Figure 437 *BGP—Summary*



BGP Details

The **BGP Details** section displays the information categorized by **Neighbors** and **Routes**.

BGP Details > Neighbors

- **Total Neighbors**—Displays the total number of neighbors.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Neighbor**—Displays the available neighbors.
- **ASN**—Displays the private Autonomous System (AS) number.
- **State**—Displays the current state.
- **Type**—Neighbor type.
- **Last State Change**—Displays the last state change.
- **Down Count**—Displays the number of neighbors that are down.
- **Up Count**—Displays the number of neighbors that are up.
- **Hold Time**—Displays the time spent on hold.
- **Keep Alive Interval**—Displays the time set for the Keep Alive Interval.
- **Router ID**—Displays the Router ID.
- **Neighbor Version**—Displays the firmware version of the connected neighbors.
- **IP Precedence Value**—Displays the IP precedence.
- **Datagrams (Max = 1400Bytes)**—Displays existing datagrams.
- **Route Refresh**—Displays the latest route refresh.
- **Graceful Restart Capability**—Displays whether graceful restart is supported.
- **BGP Addtl-Paths Computation**—Displays the additional paths computation.
- **Recv Paths**—Displays the receive path information. A red dot in this field indicates that the number of routes received has exceeded the configured limit. Hover over for more information.
- **Send Paths**—Displays the send path information. Clicking the number of routes opens the **Routes Advertised** table which displays the routes advertised to that neighbor.
- **Sent**—Displays the number of routes sent.
- **Received**—Displays the number of routes received. Clicking the number of routes opens the **Routes Learned** table. This table displays a small red circle if the number of routes received exceeds the configured route limit and the corresponding action being taken on the routes (**Drop** or **Warning**) as configured in the BGP configuration page.
- **Recv Path Limit**—Displays the Route Limit per neighbor configured in the BGP configuration page.

- **Recv Path Action**—Displays the action specified in the BGP configuration page when the number of routes exceeds the route limit.
- **Source Address**—Displays the source information.
- **Nexthop**—Displays information about the next hop.
- **Link Address**—Displays the link address.
- **CFfg Hold Time**— Displays the minimum acceptable hold time.
- **CFfg Keep Alive Time**— Displays the configuration keep alive time.
- **IS Route Reflector**—Displays the net hop path.
- **IS Router Server**—Displays the IS Router Server details.
- **BGP Advertise-Best_External**—Displays the backup external route.
- **Up Time**—Displays the time that the connection has been up.

Figure 438 *BGP—Neighbors Details*

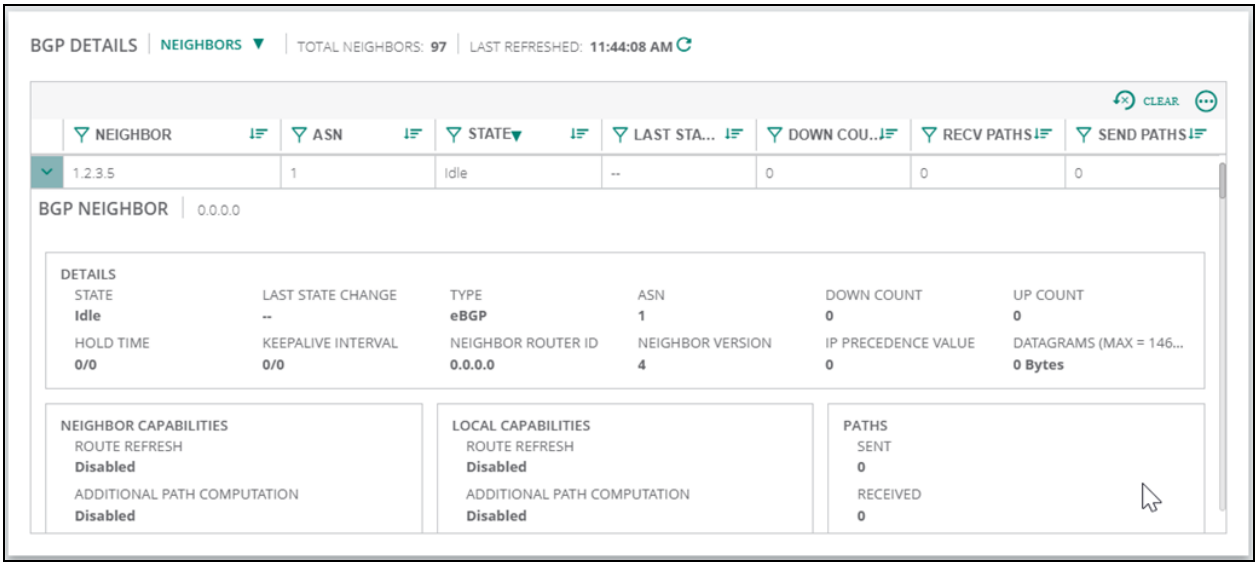
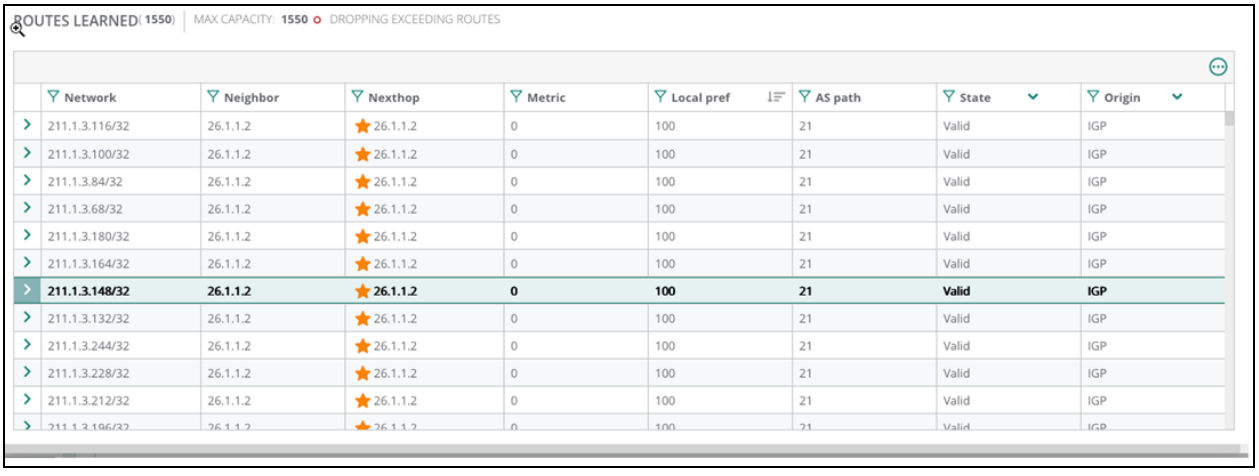


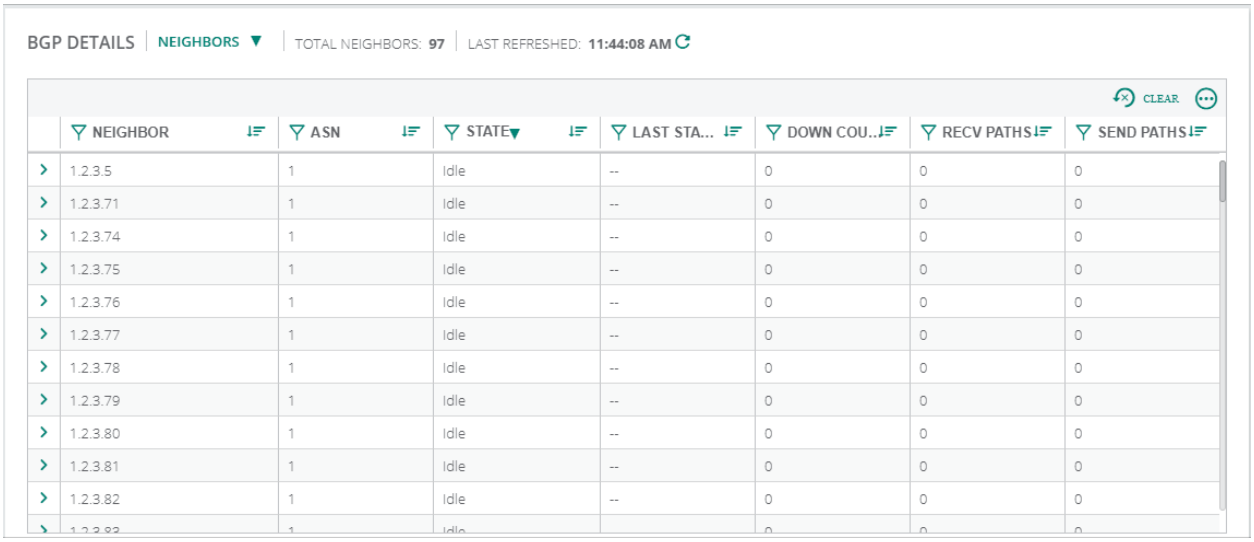
Figure 439 *BGP Routes Learned*



Clear Neighbor Sessions

- The **Clear** button allows you to clear BGP neighbor sessions.
- **Clear a neighbor session**—To clear a specific neighbor session, use the **Clear** button available for that particular neighbor row.
- **Clear all neighbor sessions**—To clear all neighbor sessions, use the **Clear** button available on the table header.

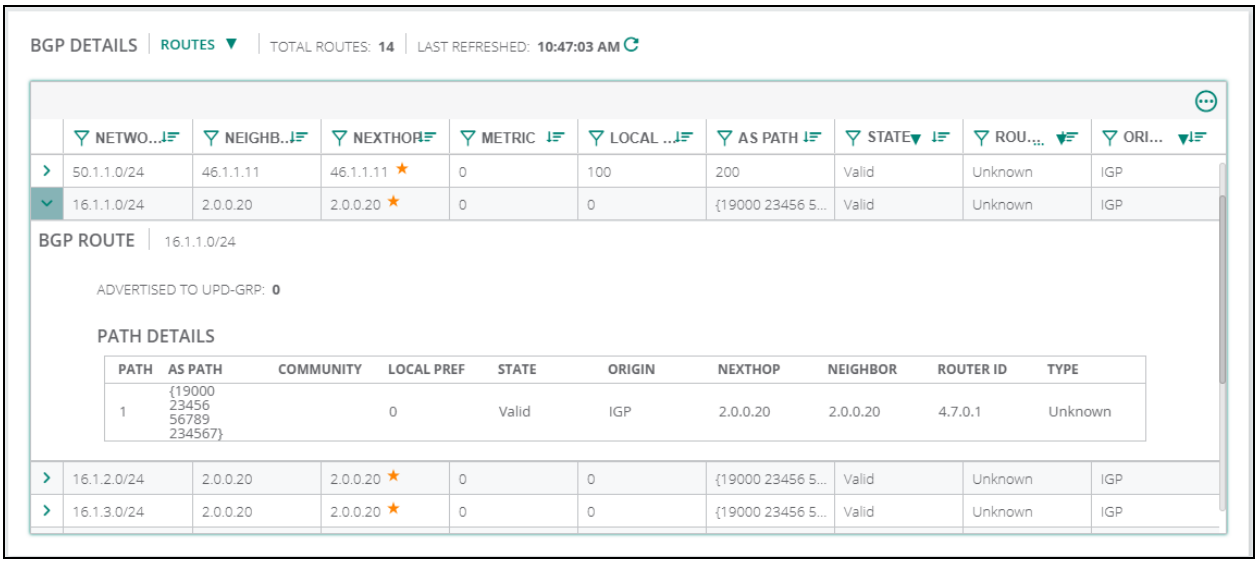
Figure 440 *BGP—Clear Neighbors*



BGP Details > Routes

- **Total Routes**—Displays the total number of routes.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Network**—Connected network.
- **Neighbor**—Displays the available neighbors.
- **Nexthop**—Displays information about the next hop.
- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
- **Local Pref**—Displays the outbound external path.
- **AS Path**—Displays the private Autonomous System path.
- **State**—Displays the connection state of the connection.
- **Route Source**—Displays the specific route the packet should take.
- **Origin**—Displays the origin attribute value.
- **Advertised to Upd-Grp**—Displays the Advertised Update-Group status.
- **Router ID**—Displays the router ID.

Figure 441 *BGP—Routes Details*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Gateway > Overview > Routing > OSPF

The **OSPF** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- OSPF Summary
- OSPF Details

Viewing the Overview > Routing > OSPF Tab

To navigate to the **OSPF** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.

3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.

4. Under **Manage**, click **Overview** > **Routing** > **OSPF**.

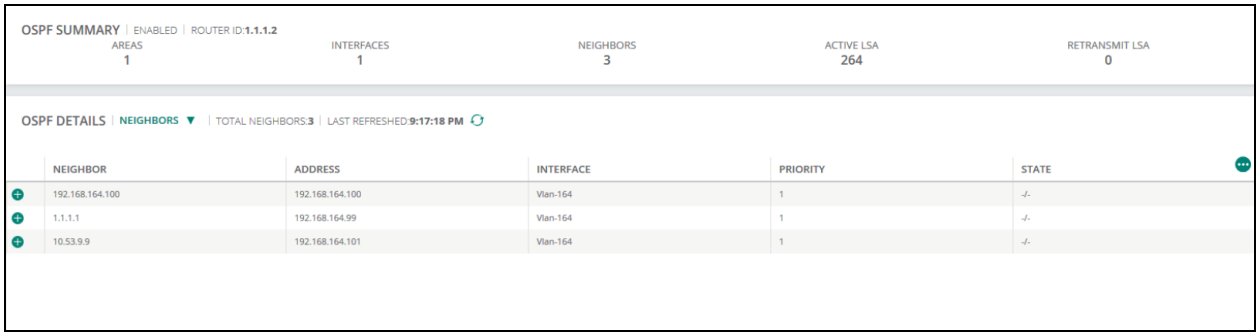
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **OSPF** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

OSPF Summary

- **Status**—Status is either Enabled or Disabled.
- **Router ID**—The routers identification details.
- **Areas**—Area type as specified in the OSPF parameters.
- **Interfaces**—Displays the current interface.
- **Neighbors**—Displays the number of neighbors available.
- **Active LSA**—Displays the Active Link-State Advertisements.
- **Retransmit LSA**—Displays the Retransmitted Link-State Advertisements.

Figure 442 *OSPF—Summary*

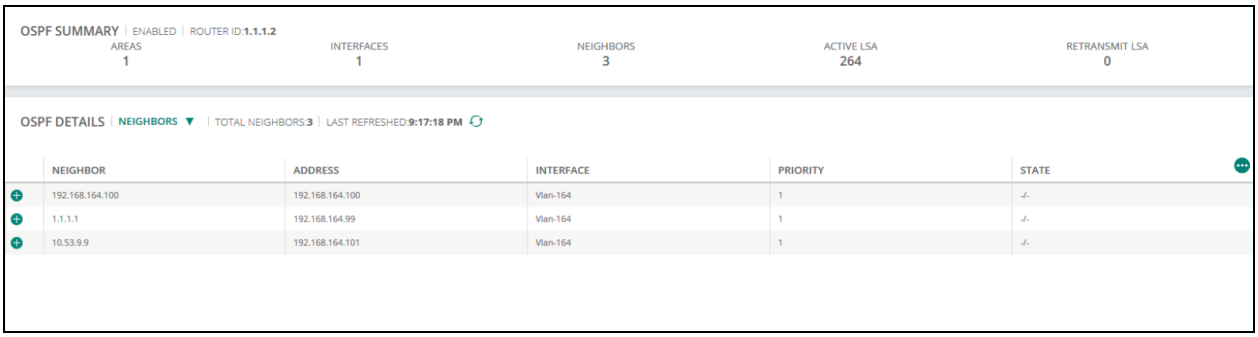


OSPF Details

Displays the information categorized by **Neighbors**, **Interfaces**, **Areas**, and **Link State Databases**.

- **Neighbors**
  - **Total Neighbors**—The total number of neighbors.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Neighbor**—Details of the neighbors.
  - **Address**—IP address of the neighbor.
  - **Interface**—Displays the current interface for the neighbor.
  - **Priority**—Displays the priority of each neighbor.
  - **State**—Displays the state of the connection.
  - **Area**—Displays the area of the neighbor.
  - **Options**—Available neighbor options.
  - **Dead Timer**—Displays the required time to wait before the neighbor connection is dead.
  - **Retransmit Timer**—Displays the time between OSPF and LSA retransmissions.

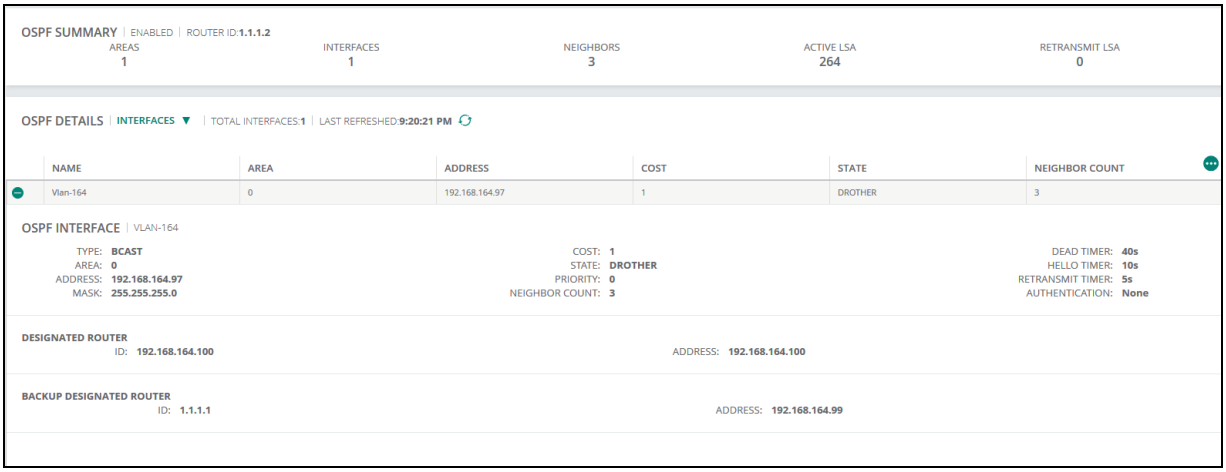
Figure 443 *OSPF—Neighbor details*



- **Interfaces**
  - **Total Interfaces**—The total number of interfaces.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Name**—Name of the interface.
  - **Area**—Displays the logical collection of devices that share the same area.
  - **Address**—IP address of the interface.
  - **Mask**—IP mask of the interface.
  - **State**—Displays the state of the connection.
  - **Type**—Displays the type of connection.
  - **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
  - **Neighbor Count** —Displays the number of neighbors.
  - **ID**—Displays the interface ID.
  - **Address**—Displays the IP address of the interface.
  - **Priority**—Displays the priority of the interface to determine the default router.
  - **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.
  - **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
  - **Retransmit Timer** —Displays the retransmit interval time for link state advertisements.
  - **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.
    Click on an interface listed in the table to view the following details:
  - **Type**—Displays the type of connection.
  - **Area**—Displays the logical collection of devices that share the same area.
  - **Address**—IP address of the interface.
  - **Mask**—IP mask of the interface.
  - **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
  - **State**—Displays the state of the connection.
  - **Priority**—Displays the priority of the interface to determine the default router.
  - **Neighbor Count**—Displays the number of neighbors.
  - **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
  - **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.

- **Retransmit Timer**—Displays the retransmit interval time for link state advertisements.
- **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.

Figure 444 *OSPF— Interfaces details*



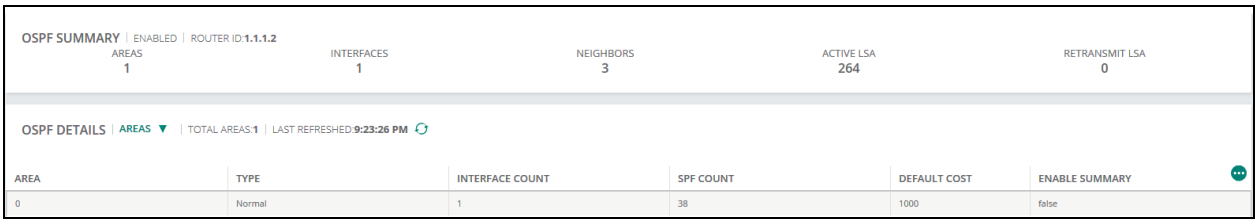
Areas

NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Areas**—The total number of areas.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Area**—Displays the logical collection of devices that share the same area.
- **Type**—Displays the type of connection.
- **Interface count**—Displays the interface count.
- **SPF Count**—Displays the Shortest Path First count.
- **Enable Summary**—Displays if summary collection is enabled.

Figure 445 *OSPF— Areas details*



Link State Databases

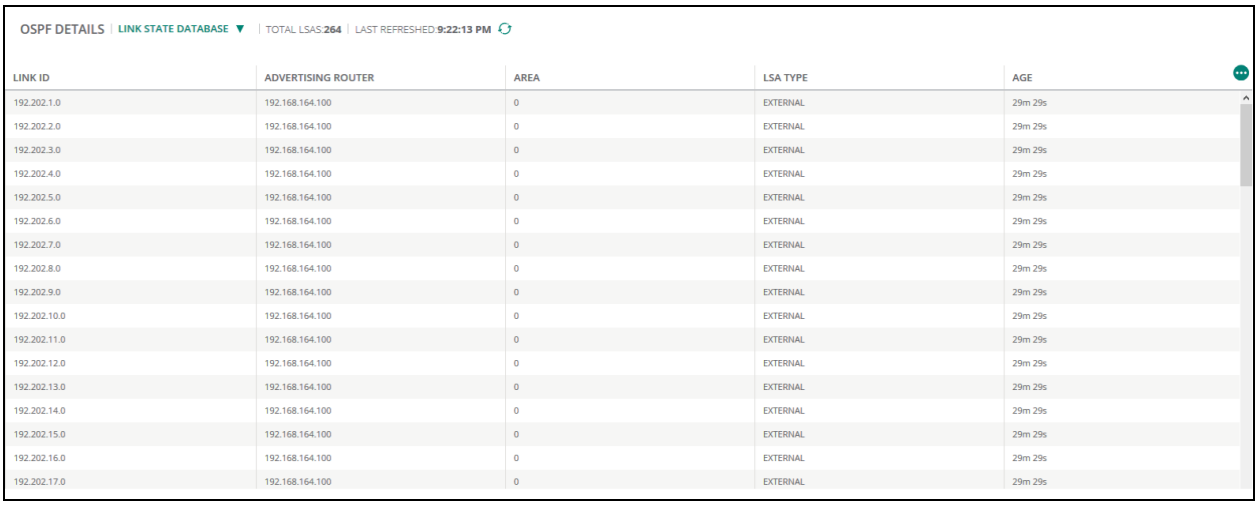
NOTE

Click the Settings icon to reset or set the default columns that are displayed.

- **Total Link State Database**—The total number of Link State Databases.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Link ID**—Displays the router ID of the originating router.
- **Advertising Router**—Displays the routes that is advertising the link-state.
- **Area**—Displays the logical collection of devices that share the same area.

- **LSA Type**—Displays the aggregation type.
- **Age**—Displays the age of the OSPF LSA.
- **State**—Displays the state of the connection.
- **Seq No.**—Displays the 32-bit OSPF Sequence number.
- **Checksum**—Displays the 16-bit checksum for the OSPF packet.

Figure 446 *OSPF—Link State Databases details*



- **LSA types**—There are various LSA types available and they are listed here:
  - **Router**—The Router page displays the following details:
    - Flags
    - Link ID
    - Link Data
    - Link Type
    - Metric
  - **Network**—The Network page displays the following details:
    - Mask
    - Attached router
  - **Network Summary**—The Network Summary page displays the following details:
    - Address
    - Mask
    - Metric
  - **ASBR Summary**—The ASBR Summary page displays the following details:
    - ASBR
    - Metric
  - **External**—The External page displays the following details:
    - Mask
    - Metric
    - Type

- Route Tag
- Forwarding Address

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Overview > Routing > Overlay

The **Overlay** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- Overlay Summary
- Overlay Details

Viewing the Overview > Routing > Overlay Tab

To navigate to the **Overlay** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **Overlay**.

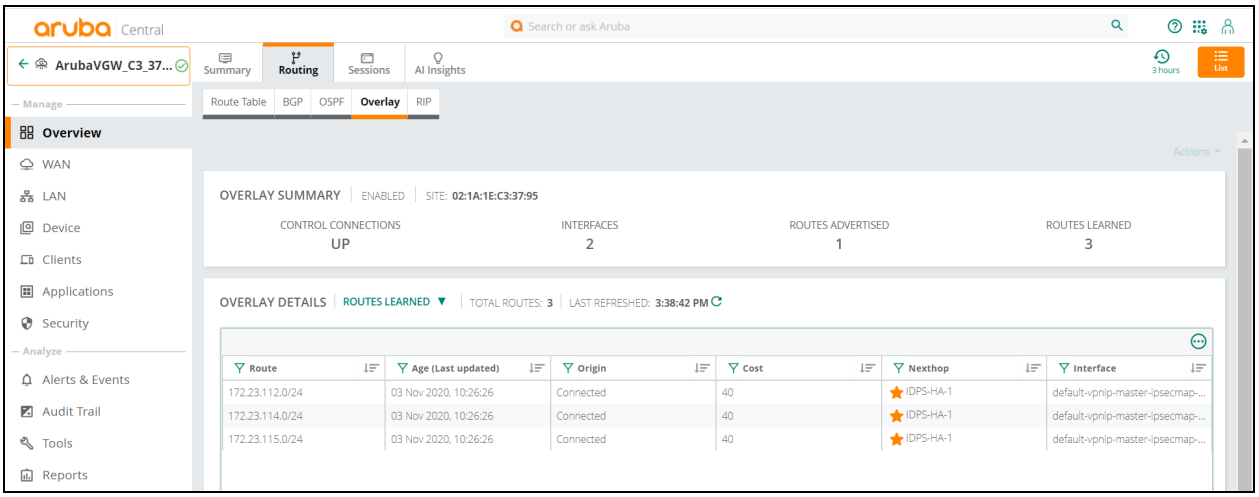
   To exit the gateway dashboard, click the back arrow on the filter.

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

Overlay Summary

- **Status**—Status is either Enabled or Disabled.
- **Site**—Displays the site location.
- **Control Connections**—Displays the control connection as either **Up** or **Down**.
- **Interfaces**—Displays the number of active interfaces.
- **Routes Advertised**—Displays the number of routes that are advertised.
- **Routes Learned**—Displays the number of routes that are learned.

Figure 447 *Overlay—Summary*



Overlay Details

- Displays the information categorized by **Control Connections**, **Interfaces**, **Routes Advertised**, and **Routes Learned**.

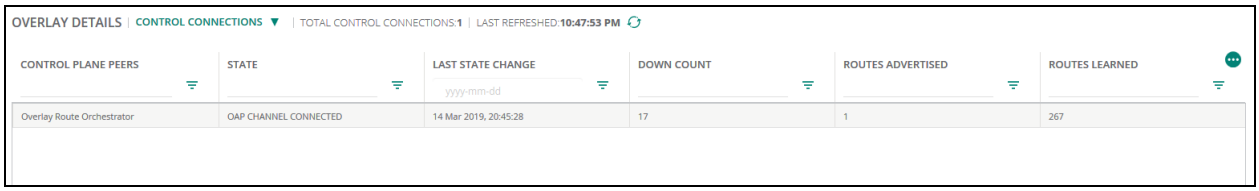
- **Control Connections**

NOTE

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

  - **Total Control Connections**—Displays the total number of control connections.
  - **Last Refreshed**—Indicates when the last refresh was completed.
  - **Control Plane Peers**—Displays the Control Plane Peers.
  - **State**—Displays the state of the connection.
  - **Last State Change**—Indicates the Last State Change.
  - **Down Count**—Displays the Down Count.
  - **Routes Advertised**—Displays the advertised routes.
  - **Routes Learned**—Displays the number of routes that are learned.

Figure 448 *Overlay Details —Control Connections*



- **Interfaces**

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

- **Total Interfaces**—Displays the total number of interfaces.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Interfaces**—Displays the number of active interfaces.
- **State**—Displays the state of the interface.
- **Tunnel Destination**—Displays the destination address.
- **Uptime**—Amount of time the tunnel has been active since it was last reset.
- **Routes Learned**—Displays the number of routes that are learned.

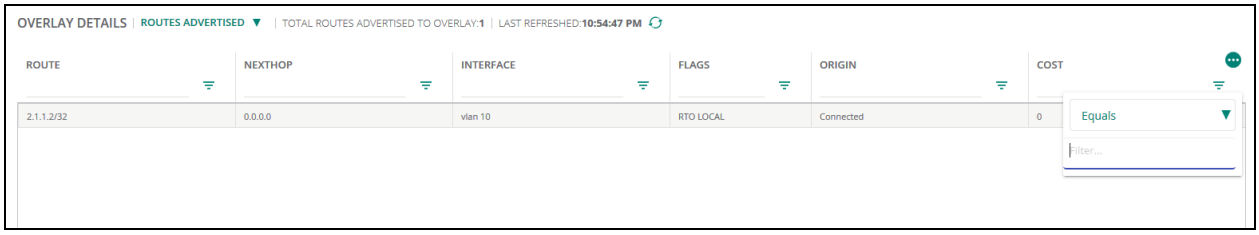
Figure 449 *Overlay Details —Interfaces*

- **Routes Advertised**

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the filter icon on each column header row to filter the displayed information.

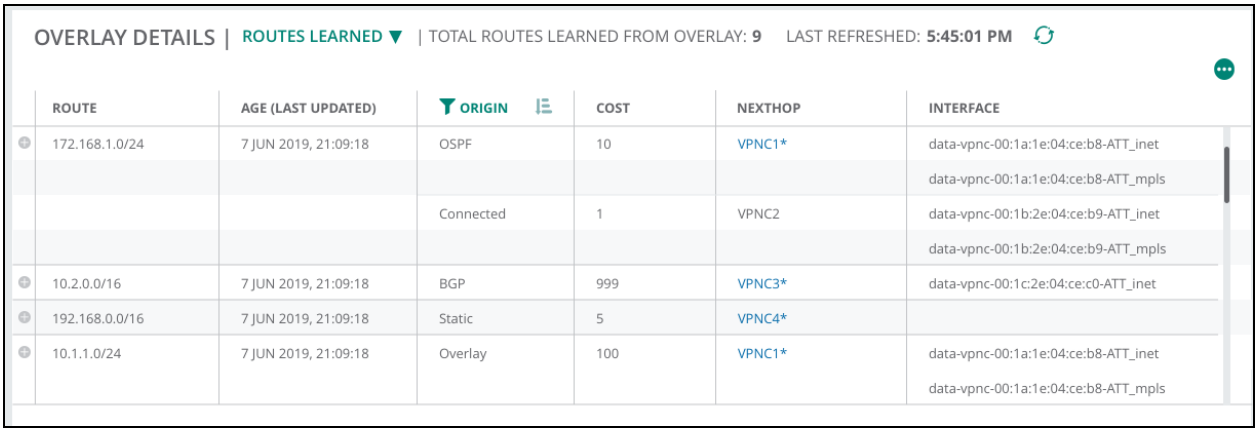
- **Route**—Displays the route name.
- **Nexthop**—Displays information about the next hop.
- **Interface**—Displays the number of active interfaces.
- **Flags**—Lists the number of active flags.
- **Origin**—Origin of the route.
- **Cost**—Cost associated with the route.

Figure 450 *Overlay Details—Routes Advertised*



- **Routes Learned**
- **Total Routes Learned**—Displays the total number of routes that are learned.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Route**—The route IP address aand subnet.
- **Age (Last Updated)**—Last updated date.
- **Origin**—Orging of the connection, for example, Connected or Overlay.
- **Flags**—Lists the number of active flags.
- **Nexthop**—Displays information about the next hop.
- **Interface**—Displays the number of active interfaces.

Figure 451 *Overlay Details—Routes Learned*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Overview > Routing > RIP

The **RIP** tab under **Manage** > **Overview** > **Routing** in the gateway dashboard displays the following sections:

- RIP Summary
- RIP Details

Viewing the Overview > Routing > RIP Tab

To navigate to the **RIP** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Routing** > **RIP**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **RIP** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

RIP Summary

The **RIP Summary** section displays the following information:

- **Enabled**—Implies that RIPv2 is enabled on the gateway device.
- **Version**—Displays the RIP version, RIPv1 or RIPv2. Currently, Arubasupports only RIPv2.
- **Interfaces**—Displays the number of interfaces that participates in the routing process.
- **Neighbors**—Displays the number of neighboring connections.
- **Routes**—Displays the number of routes advertised.
- **ECMP**—Displays the number of ECMPs available.
- **Infinity**—The hop count (16) assigned to unreachable devices (typically, any route that requires more than 15 hops).
- **Timers**—RIP uses timers to regulate its performance:
  - **Update** timer displays the interval between periodic routing updates. By default this is set to 30 seconds.
  - **Invalid** timer displays the time in seconds after which the route is marked invalid but is still available in the table. By default this is set to 180 seconds.
  - **Flush** timer displays the time duration after which the route is flushed out or removed from the table. By default this is set to 120 seconds.

Figure 452 *RIP—Summary*

RIP Details

Displays the information categorized by **Interfaces**, **Neighbors**, and **Routes**.

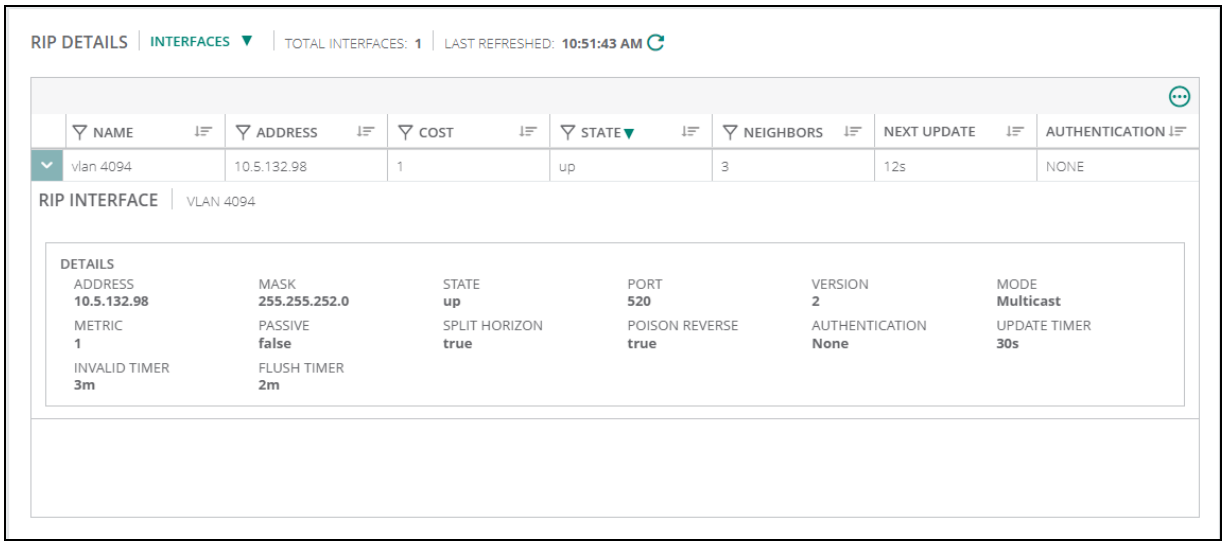
- **Interfaces**
  - **Name**—Displays the name of the interface.
  - **Address**—Displays the IP Address of the interface.
  - **Cost**—Displays the cost associated.

- **State**—Displays the state of the connection (Up pr Down).
- **Neighbors**—Displays the number of neighbors.
- **Authentication**—Displays the status of this option that is used for enabling RIP authentication mode for MD5.
- **Next Update**—Time in seconds for the next update

Click on an interface listed in the table to view the following details:

- **RIP Interface**—Displays the name of the interface.
- **Address**—Displays the IP Address of the interface.
- **Mask**—Displays the subnet mask.
- **State**—Displays the state of the connection (Up or Down).
- **Port**—Displays the port number of the interface.
- **Version**—Displays the RIP protocol version.
- **Mode**—Displays the interface configuration mode.
- **Metric**—Displays the number of hop counts.
- **Passive**—Indicates whether the interface is operating in passive mode.
- **Split Horizon**—Indicates whether Split Horizon is implemented.
- **Poison Reverse**—Indicates whether Poison Reverse is implemented.
- **Authentication**—Displays the status of this option that is used for enabling RIP authentication mode for MD5.
- **Update Timer**—Displays the interval between periodic routing updates, by default this is set to 30 seconds.
- **Invalid Timer**—Displays the time in seconds after which the route is marked invalid but is still available in the table.
- **Flush Timer**—Displays the time duration after which the route is flushed out or removed from the table.

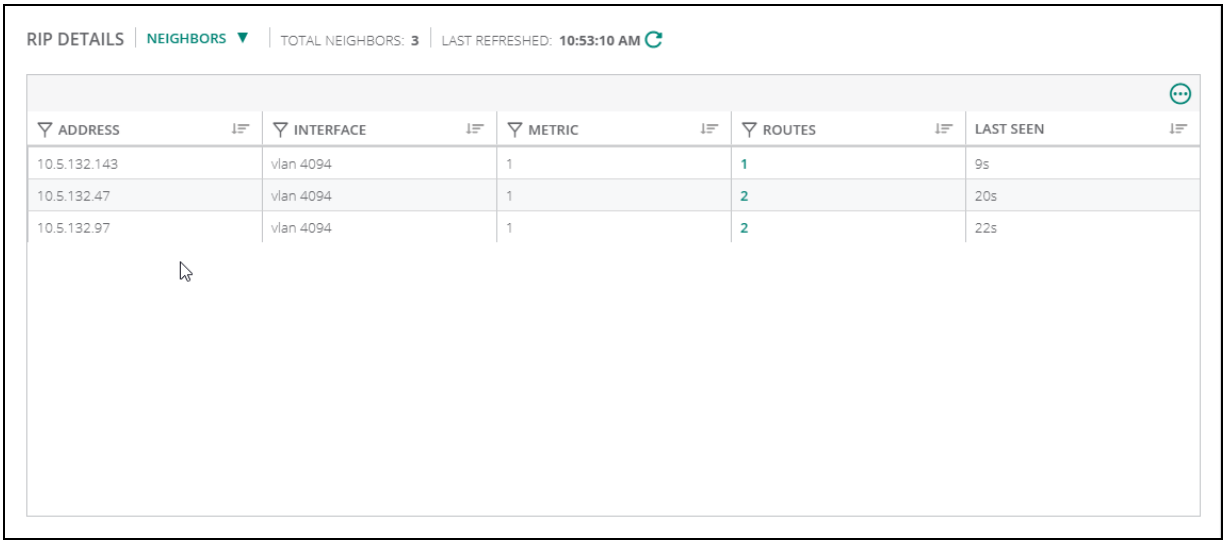
Figure 453 *RIP—Interfaces Details*



- **Neighbors**
  - **Address**—Displays the IP address of the neighbor.
  - **Interface**—Displays the name of the interface.

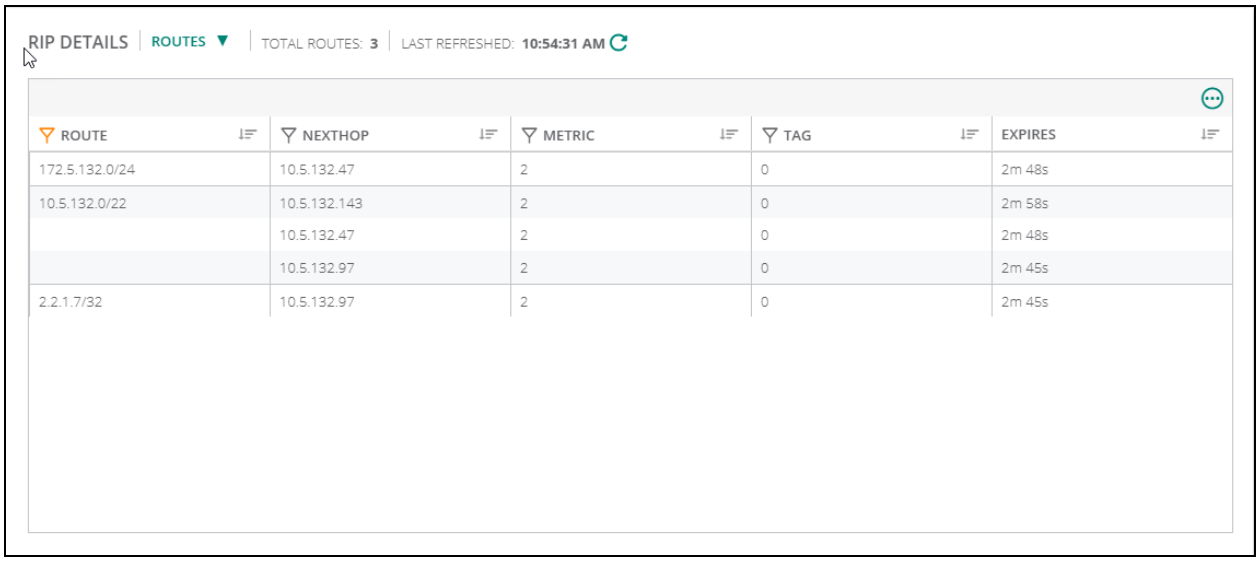
- **Metric**—Displays the number of hop counts.
- **Routes**— Displays the number of routes learned. Click the number for details of the routes learned.
- **Last Seen**— Displays the last seen time duration in *nD nH nM nS* format.

Figure 454 *RIP—Neighbors Details*



- **Routes**
  - **Route**—Displays the route.
  - **Next Hop**—Displays information about the next hop.
  - **Metric**— Displays the number of hop counts.
  - **Tag**—Displays the tag number associated with the route attribute that is set.
  - **Expires**—Displays the time in *nD nH nM nS* format after which the route expires.

Figure 455 *RIP—Routes Details*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Overview > Sessions

The **Sessions** tab under **Manage** > **Overview** in the gateway dashboard displays the following sections:

- Session Summary
- Sessions

Viewing the Overview > Sessions Tab

To navigate to the **Sessions** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Overview** > **Sessions**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Sessions** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Session Summary

Displays a summary of all the running sessions.

The following details are displayed in the **Session Summary** section:

- **Current entries**—Displays the number of current and active entries.
- **Max entries**—Displays the total entries made with the time period.
- **High watermark**—Displays the highest number of active entries.
- **Allocation failures**—Displays the number of failed allocations.
- **Denied entries**—Displays the number of entries that were denied.

Sessions

The **Sessions** section displays information filtered by the **IP Address** entered in the text box.

- Click the Settings icon to reset or set the default columns that are displayed.
- Click the Filter icon and enter the keyword or ip address to filter the information.

The **Sessions** table displays information about:

- **Application**—Displays the list of applications.
- **Protocol**—Displays the communication protocol used.
- **Source port** —Displays the source port number.
- **Dest port** —Displays the destination port number used by the application.
- **Action**—Displays the application specific action.
- **DSCP**—Displays the Differentiated Services Codepoint (DSCP) value.
- **Flags**—Displays the applied flags. Hover over the information icon to see the Legend for the flag description.
- **Packets**—Displays the number of packets.
- **Bytes**—Displays the amount of data (in bytes and mega bytes) consumed by the application.
- **State**—Displays the connection state of the application. The state can either be Active, Inactive, or Denied.
- **Start Time**—Displays the start time.
- **Receive Time**—Displays the receive time.
- **WEBCC Category**—Displays the WEBCC category.
- **WEBCC Reputation**—Displays the WEBCC reputation.
- **WEBCC Score**—Displays the WEBCC score.
- **Application Category**—Displays the application category.
- **Priority**—Displays the priority value.

To view additional information of individual sessions, click the drop down icon to expand and display session specific information.

The following information is displayed:

- **Details**
  - **User role**—Displays the user role name.
  - **User policy rule (ACE)**—Displays the user policy rule.
  - **Start time**—Displays the session start time.
  - **Receive time**—Displays the session receive time.
  - **WebCC category**—Displays the WebCC categorization.
  - **WebCC reputation**—Displays the site reputation.
  - **Application category**—Displays the application category.
  - **DSCP**—Displays the Differentiated Services Codepoint (DSCP) value.
  - **Priority**—Displays the priority value.

- **Nexthop**
  - **Uplink interface**—Displays the uplink interface details.
  - **Uplink VLAN**—Displays the uplink VLAN details.
  - **Tunnel**—Displays the tunnel details.
- **Matching PBR**
  - **Policy Name (RACL)**—Displays the policy name.
  - **Policy Rule (RACE)**—Displays the policy rule.
- **Dynamic Path Selection (DPS)**
  - **Policy name**—Displays the policy name.
  - **Path preference**—Displays the path interface details.
  - **Compliance**—Displays the compliance details.
  - **Matching Policy Rule**—Displays the matching policy rule.

NOTE

Matching PBR and Dynamic Path Selection (DPS) tables require SD-WAN version 2.0.0.1 or higher.

Figure 456 *Session Summary and Session Information*

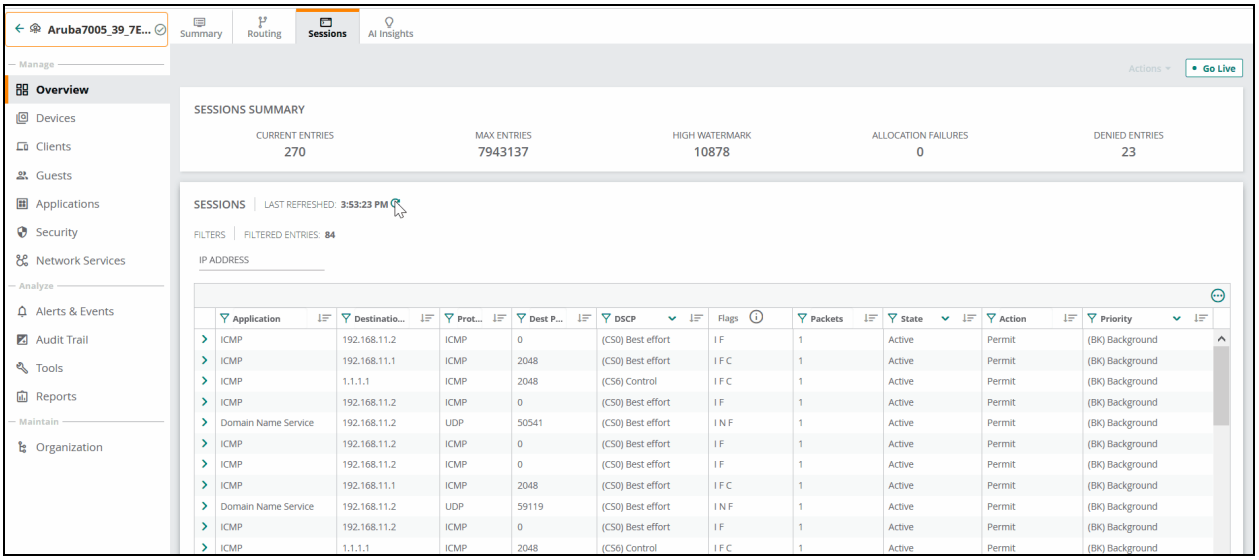
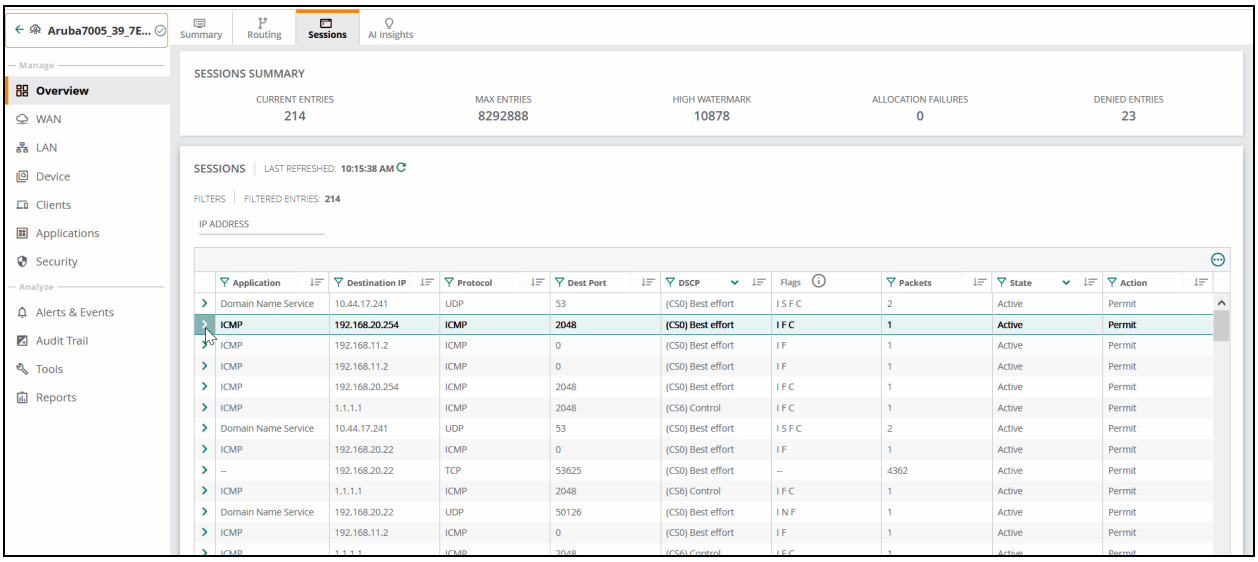


Figure 457 *Session Details*



Gateway > Overview > AI Insights

In the gateway dashboard, the **AI Insights** tab displays information on gateway performance issues such as tunnel up, tunnel down, airtime utilization, and memory utilization.

Viewing Gateways > AI Insights

To navigate to the **AI Insights** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**. Ensure that the filter selected contains at least one active gateway.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.

   The dashboard context for the gateway is displayed.
4. In the gateway dashboard context, click the **AI Insights** tab.

   The **Insights** page is displayed.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **AI Insights** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

NOTE

AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** ( ) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

- Red—High priority
- Orange—Medium priority
- Yellow—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. Each insight report provides specific details on the occurrences of these events for ease in debugging.

Gateway > WAN > Summary

The **Summary** tab under **Manage** > **WAN** page in the gateway dashboard displays the following sections:

- Port Status
- WAN Interfaces
- Go Live

You can view and monitor your WAN interfaces, the tunnels configured, and the path steering data for all the DPS policies configured.

Viewing the WAN > Summary Tab

To navigate to the **WAN > Summary** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Summary**.

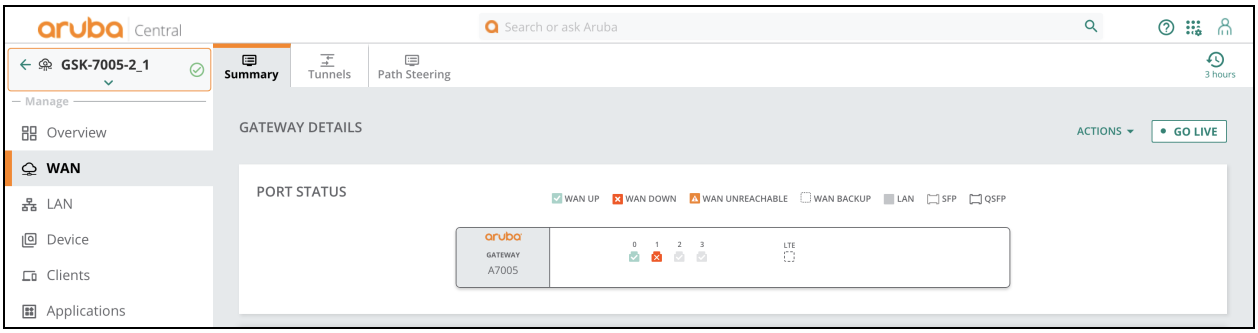
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Port Status

- Displays the WAN port status. Click a WAN port for more details.

Figure 458 *Port Status*

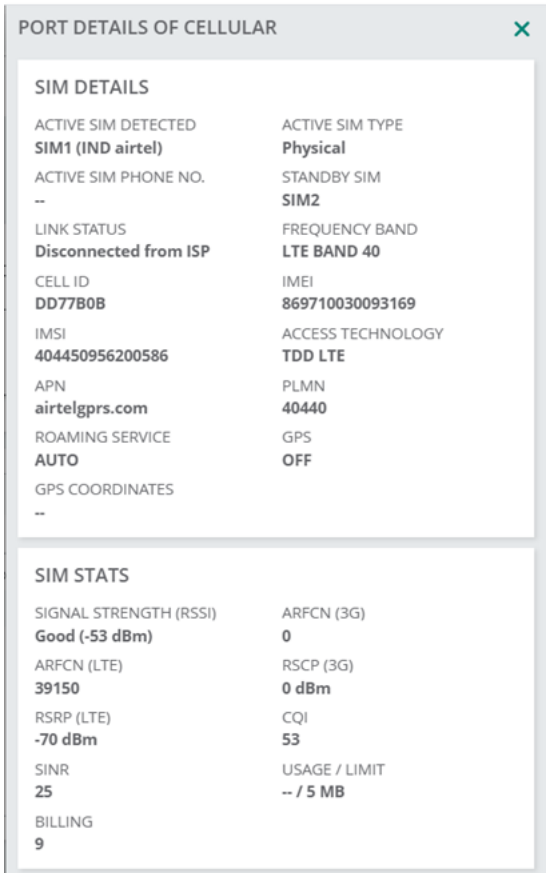


For a 9004-LTE Branch Gateway, the **Port Status** displays the LTE uplink details and when you hover over **Internal LTE**, you can view details about the active SIM, the name of the service provider, and the signal strength.

Figure 459 *Port Status of a 9004-LTE Gateway*

You can click on the active SIM to view the port details of cellular.

Figure 460 *Port Details*



WAN Interfaces

- Lists the WAN interfaces and provides the total number of WAN interfaces. Displays the summary of WAN uplinks. The following details are displayed for the port:

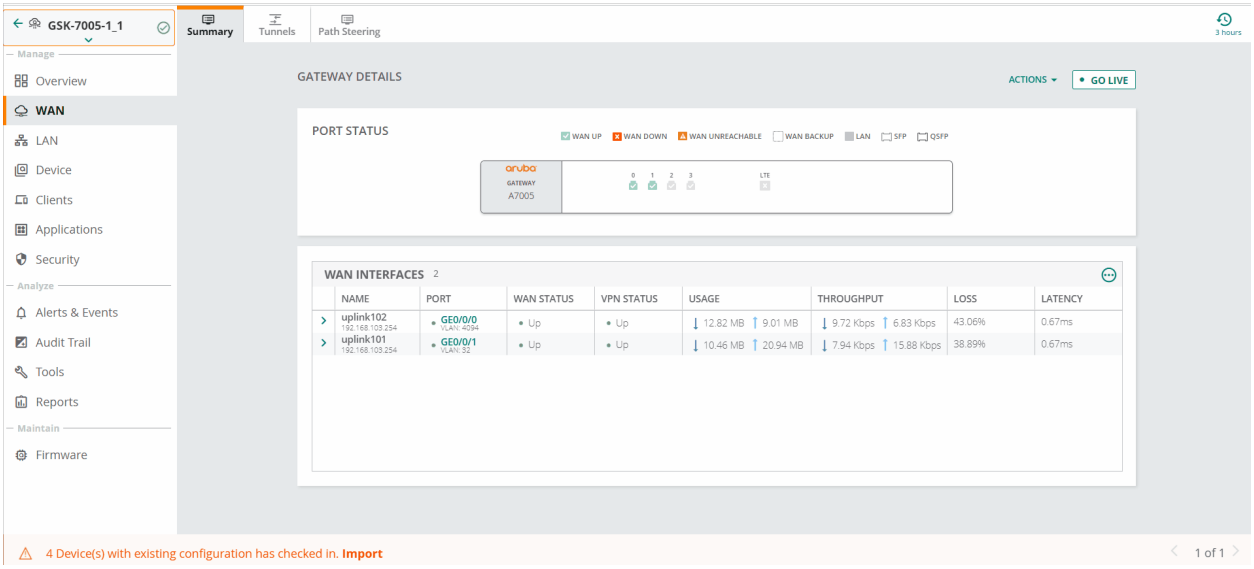
NOTE

Click the Settings icon to reset or set the default columns that are displayed.

  - **Total WAN Interfaces**—Total number of WAN interfaces available.
  - **Name**—Name of the WAN interface.
  - **Port**— Port number along with the associated VLAN ID.
  - **WAN Status**—WAN reachability status.
  - **VPN Status**—VPNC reachability status.
  - **Usage**—WAN interface usage (Sent and Received).
  - **Throughput**—WAN interface transmit and receive performance in Kbps.
  - **Loss**—Loss percentage.
  - **Latency**—The latency in milliseconds.

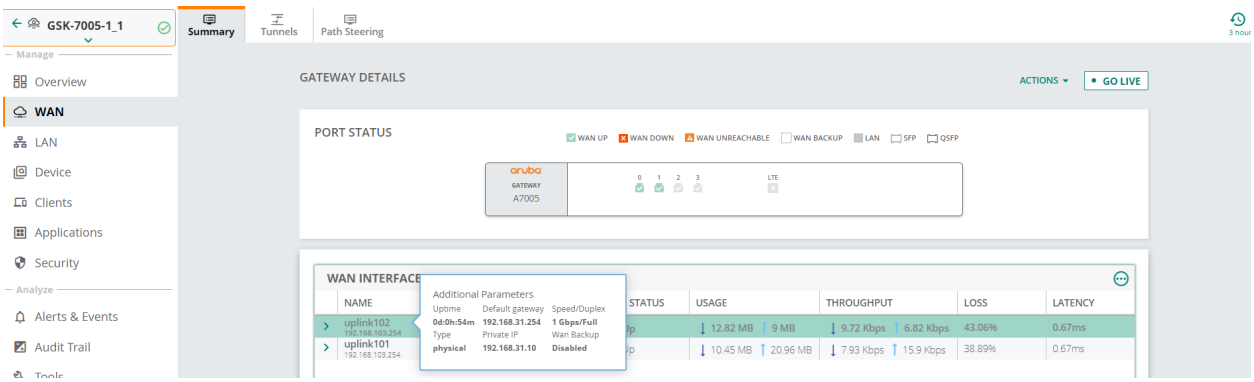
In the **WAN Interfaces** table, click a port number to display the **Packets** and **Errors** details.

Figure 461 *WAN Interfaces Packets and Errors*



- The following graphs are displayed under the **Packets** tab:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.
- The following graphs are displayed under the **Errors** tab:
  - **CRC Errors**—The number of cyclic redundancy errors logged.
  - **Error Frames**—The number of error frames logged.
  - **Collisions**—The number of collisions encountered.
- **Additional Parameters**—In the **WAN Interfaces** table, hover on the WAN interface name to view the additional parameter for the WAN interface.

  Figure 462 *Additional Parameters*



  The following additional parameters are displayed for the WAN interface:
  - **Uptime**—Uptime of the uplink (DD-HH-MM).
  - **Default Gateway**—Default gateway.
  - **Speed/Duplex**—Port speed.
  - **Type**—Service provider uplink type (Physical / Virtual).

- **Private IP**—Private IP address.
- **WAN Backup**—Backup of WAN interface (Enabled or Disabled).

Expand the **WAN Interface** name to see the following details.

- **WAN Availability**—Provides an overall graphical representation of the selected interface's WAN availability based on reachability. The graph shows the selected WAN port's ability to reach its default gateway and health check IP.
- **VPN Availability**—Provides an overall graphical representation of the selected interface's VPN availability based on reachability.
- **Usage**—Provides a snapshot of the WAN usage and is available for **All Traffic**, **Internet**, and **VPN** specific information. You can see the incoming and outgoing traffic for the gateways with time plotted on the x-axis. Hover over the chart to see the incoming and outgoing traffic for a particular time frame.
  - **Top Applications**—Displays application level WAN usage per-uplink for top ten applications. Click the **Go to Applications** link to view details in the **Applications** tab.
    The WAN visibility is available only for 3 hours time range.

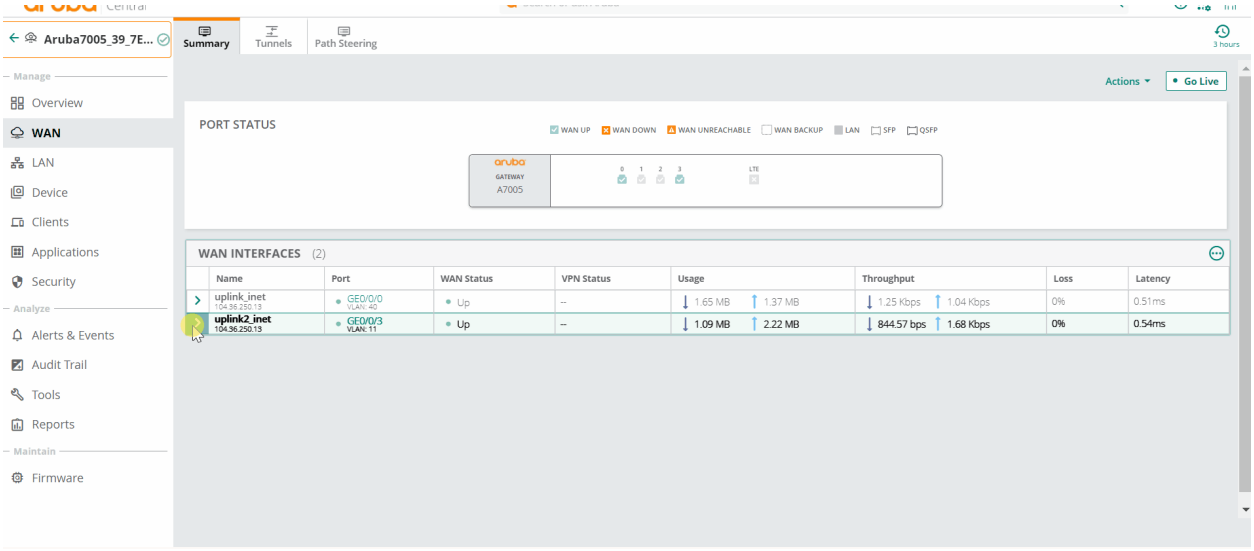
  Click the following icons to see the chart in logarithmic scale or linear scale.
  - Logarithmic Scale—Click this icon to view chart in logarithmic scale.
  - Linear Scale—Click this icon to view chart in linear scale.

  Click Received or Sent at the bottom of the chart to view or hide the usage chart for received or sent data.
- **Throughput**—Provides a graphical representation of the selected WAN interface's throughput. The graph displays the WAN interface's transmit and receive performance in bps.

  Click the following icons to see the chart in logarithmic scale or linear scale.
  - Logarithmic Scale—Click this icon to view chart in logarithmic scale.
  - Linear Scale—Click this icon to view chart in linear scale.

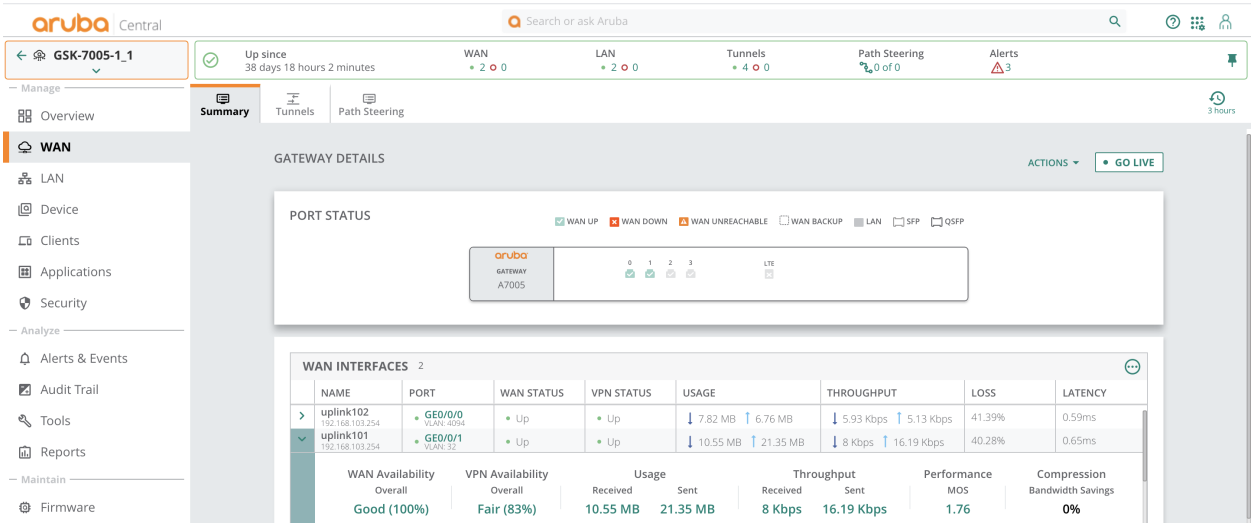
  Click Received or Sent at the bottom of the chart to view or hide the usage chart for received or sent data.
- **Performance**—The Performance section displays the MOS score of interface and the following graphs based on the probe that is selected. For a health check probe, only Latency and Packet Loss graphs are displayed.
  - **Latency**—The latency in milliseconds.
  - **Packet Loss**—Displays the packet loss in percentage.
  - **Jitter**—Displays the jitter in milliseconds.
  - **MOS Score**—Displays the MOS score.
- **WAN Compression**—Provides bandwidth savings of WAN compression uplink, along with optimized and non optimized packets and the average bandwidth saved in percentage.

Figure 463 *WAN Interfaces Availability*



Live Monitoring for Device State is enabled for **Status Header Tile**, **Port Status** and **WAN Interfaces**.

Figure 464 *WAN_Live Monitoring*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** option allows you to view the WAN interface data in real-time. The details about individual WAN interfaces are updated every five minutes in the normal WAN page view, whereas the details displayed in Live mode are updated every five seconds. This feature allows you to compare the statistics of two WAN interfaces. By default, the first two are displayed. You can select the uplinks for which you want to view the data. This feature is especially useful to troubleshoot issues.

The **Downstream** graph displays data on download speed and the **Upstream** graph provides data on upload speed. The X-axis in the graph indicates the time and the Y-axis indicates the throughput in Bytes per second (bps).

The Live session is active for 15 minutes and automatically returns to normal view at the end of 15 minutes. A timer displays the number of minutes since the live session started.

To view the live statistics of the WAN interfaces, click the **GO LIVE** button. To go back to normal view, click the **STOP LIVE** button.

Figure 465 *GO LIVE page*

Gateway > WAN > Tunnels

The **Tunnels** tab under **Manage** > **WAN** page in the gateway dashboard displays the following sections:

- Tunnels Summary
- Tunnels
- Tunnel Info

The Tunnels tab displays the status and health details for Branch Gateway tunnels and IAP-VPN tunnel.

Viewing the WAN > Tunnels Tab

To navigate to the **Tunnels** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Tunnels**.

   To exit the gateway dashboard, click the back arrow on the filter.

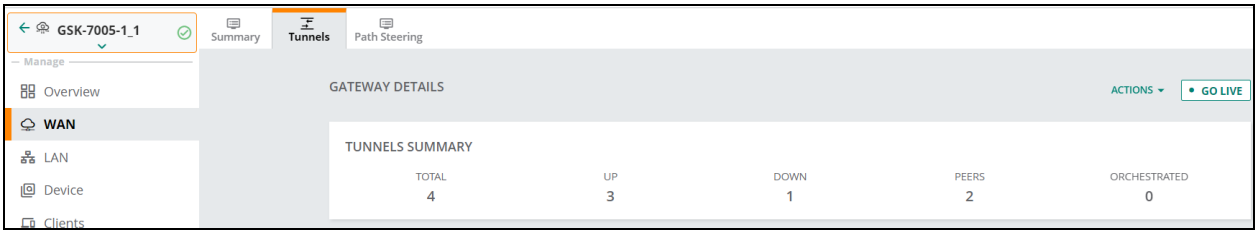
   You can change the time range for the **Tunnels** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Tunnels Summary

The following details are displayed in the **Tunnels Summary** table:

- **Total**—Total number of VPN tunnels.
- **Up**—Number of VPN tunnels in UP state.
- **Down**—Number of VPN tunnels in DOWN state.
- **Peers**—Total number of VPN peers.
- **Orchestrated**—Total number of VPN tunnels running in orchestrated mode.

Figure 466 *Tunnels Summary*



Tunnels

The following details are displayed in the **Tunnels** table:

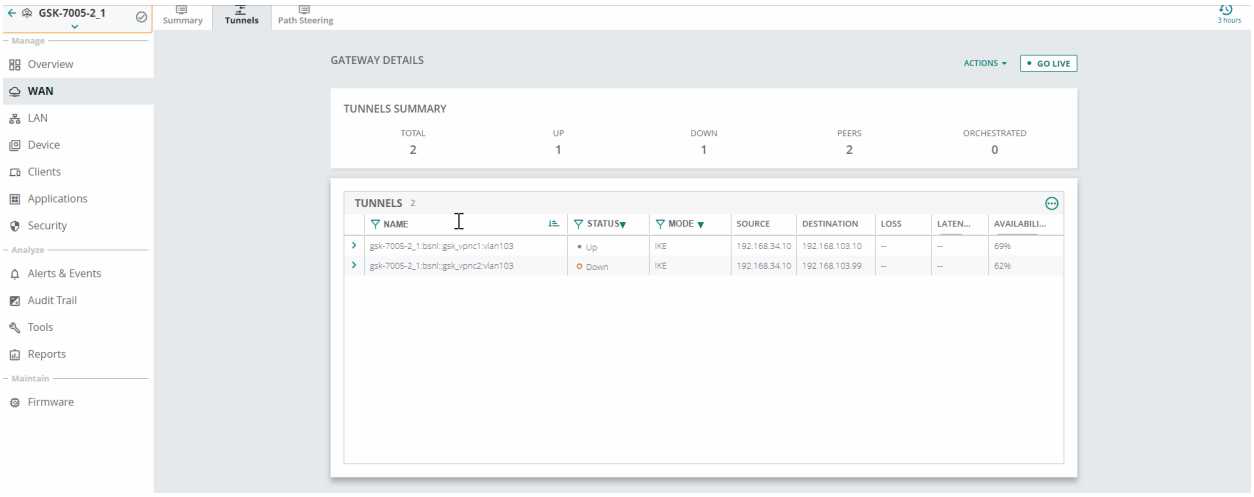
- **Name**—Tunnel name.
- **Status**—Status of the tunnel (Up or Down).
- **Mode**—Displays the type of tunnel. The tunnel configurations displayed are:
  - **Orch**—Identifies tunnels that have been orchestrated.
  - **Orch-Srv**—Identifies the orchestrated tunnels that are in survivability state.
  - **Orch-IKE**—Orchestrated tunnels which use the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite with 3rd party devices such as Zscaler.
  - **IKE**—Identifies tunnels created manually using the IKE protocol.

- **Source**—Source IP address of the tunnel.
- **Destination**—Destination IP address of the tunnel.
- **Loss**—Percentage of packet loss.
- **Latency**—The latency in microseconds.
- **Last Change Reason**—Reason for the last status change of the tunnel.
- **Availability**—Availability graph of the tunnel. Displays the percentage of time the tunnel was in UP state.

NOTE

The default view of gateways table shows only a few columns. To view the hidden columns, click the settings icon at the right side of the table. To reset the columns, click **Reset to default**.

Figure 467 *Tunnels Details*



Tunnel Info

- Expand a tunnel name to view the following details:
  - **Uptime**—Amount of time the tunnel has been active since it was last reset.
  - **Link**—Tunnel link.
  - **WAN IP**—WAN IP address.
  - **Uplink Port**—Uplink port details.
  - **Last Change Reason**—Reason for the last status change of the tunnel.
  - **Peer IP**—Peer IP address.
  - **VLAN**—VLAN ID.
  - **Source MAC**—Source MAC address.
  - **Next Rekey**—Next Rekey time.

- **Auth**—Authentication methods such as SHA1, DES, and 3DES.

From SD-Branch 2.3.0.0 version, Overlay Tunnel Orchestration supports the SHA2-256 authentication method. The Tunnel Orchestration creates IPSec tunnels with SHA2-256 authentication algorithm, only when both the tunnel endpoints (Initiator and Responder) support SHA2-256 authentication (that is, both the tunnel endpoints are running on SD-Branch 2.3.0.0). Else, the Tunnel Orchestration triggers the default authentication (SHA1).

- **In SPI**—Inbound Security Parameter Index (SPI).
- **Out SPI**—Outbound Security Parameter Index (SPI).
- **Encryption**—Encryption.

- **Availability**—Availability information of the tunnel.
  - **Tunnel Status**—Provides an overall graphical representation of the selected tunnel's availability based on VPNC reachability.
  - **Usage**—Displays the tunnel's traffic usage.
  - **Throughput**—Displays the inbound and outbound traffic rates for the selected tunnel. The graph displays the tunnel's performance in Kbps. The graph also displays information that is sent and received.
  - **Performance**—The Performance section displays the details based on the interface that is selected.

  Live monitoring is enabled for sections that display the status, such as:
- The **Tunnels Summary**
- Status of the **Tunnels Details**

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

- **Utilization**—Displays the utilization in percentage terms. The average, minimum, and maximum packet utilization is displayed.
- **SLA Policy Compliance**—Displays the SLA policy compliance details.

Gateway > WAN > Path Steering

In the **Path Steering** tab, you can view traffic path steering details for the Dynamic Path Steering policies configured on the Branch Gateway. This tab also displays the number of policies that are compliant along with the total number of policies configured on the Branch Gateway.

From the list of Dynamic Path Steering polices, select the policy for which you want to view the path steering details.

The **Pathsteering** tab under **Manage** > **WAN** page in the gateway dashboard displays the following sections:

- Path Steering Summary
- Path Steering Details

Viewing the WAN > Path Steering Tab

To navigate to the **Path Steering** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **WAN** > **Path Steering**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Path Steering** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Path Steering Summary

Displays the following information.

- **State**—Displays whether the path steering feature is enabled.
- **Policy Compliance**—Displays the compliance status of all the configured policies.

Path Steering Details

Displays the following information.

- **Expected Threshold Values**
  - **Policy Name**—The name of the Dynamic Path Steering policy
  - **Bandwidth**— The threshold percentage set for bandwidth utilization
  - **Latency**—The threshold value set for a round-trip ping time in milliseconds
  - **Jitter**—The threshold value set for jitters in packet transmission in milliseconds
  - **Packet Loss**—The percentage of packet loss allowed for the traffic type
  - **Path Preference**—The path preference in the primary, secondary, and tertiary order
  - **Status**—The compliance status of the uplinks
  - **Overall Compliance**—Overall compliance (%) of the policy

Figure 468 *Path Steering Details*

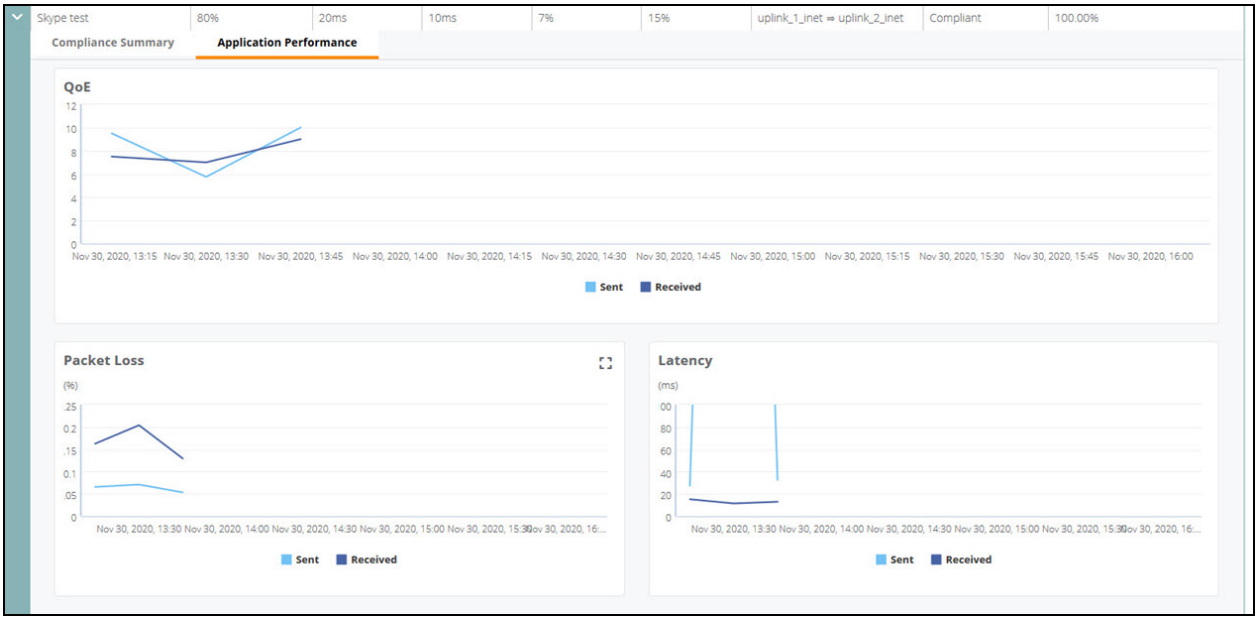
Click a policy to view the **Compliance Summary** that consists of the **Status** and **Session** information and the **Application Performance**.

- **Status**—Provides a graphical representation of the configured uplink statuses. The following details are displayed:
  - Overall status
  - The status of each of the uplinks configured for the Dynamic Path Steering policy on that gateway. Hover over the status bar to view the compliance status details of all the configured uplinks. You can view the compliance status of the uplinks and the probe IPs. If the probe IPs are non-compliant, it displays the reason for non-compliance such as latency, jitter, or packet loss. The following list contains the various colors and the corresponding compliance status:
    - **Green**—An uplink is **Compliant** when all of the associated probe IPs meet the set SLAs and threshold settings.
    - **Orange**—An uplink is **Partially Compliant** when you have multiple probe IPs and not all of them are compliant.
    - **Red**—An uplink is **Non-Compliant** when all of the probe IPs are non-compliant.
    - **Yellow**—This is the **Hold Period** when an uplink changes it's status from Non-compliant to Compliant (usually the first 3 minutes of the transition phase).
    - **Grey**—Uplink status is **Unknown** when the Dynamic Path Steering feature does not send any compliance information to the cloud.
    - **Purple**—The uplink is compliant and **FEC Protected** because of the redundant packets sent by FEC even though the packet loss percentage has exceeded the configured SLA.
- **Sessions**—Provides a graphical representation of the total number of sessions. The following details are displayed:
  - Overview
  - The sessions count on each of the uplinks configured for the Dynamic Path Steering policy on that gateway

Figure 469 *Path Steering Details—Compliance Summary*

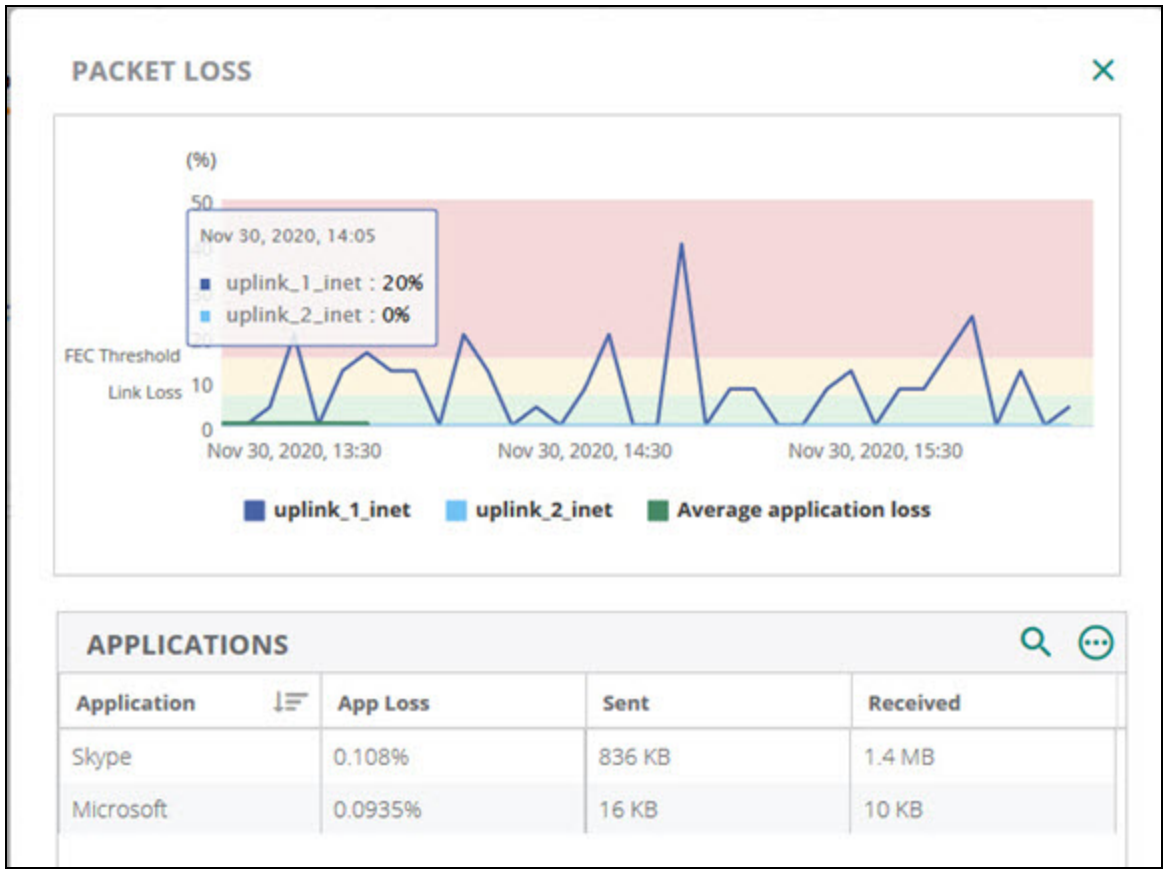
- **Application Performance**—Provides a graphical representation of the performance of the application for QoE, Packet Loss, and Latency. The passive application monitoring data is tagged with the DPS policy ID and the scores for both Sent and Received traffic are displayed in this chart. QoE is the average of the Packet Loss and Latency scores.

Figure 470 *Application Performance*



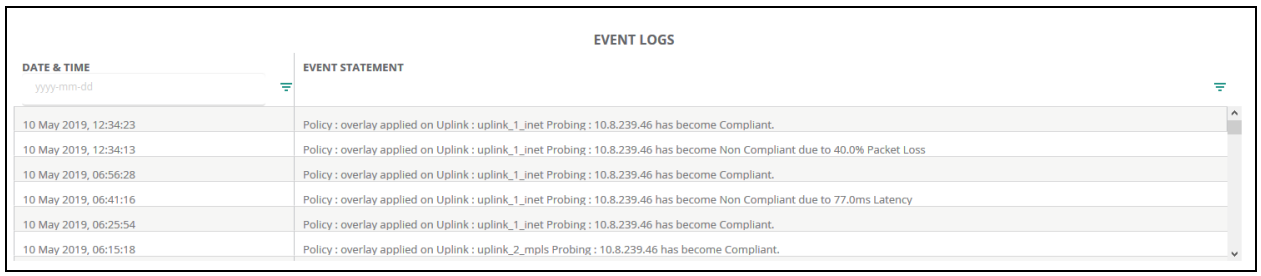
Click the Expand icon to drill down the packet loss data. The following image displays the Packet Loss data with respect to the configured FEC threshold. The uplink_1_inet has reached the FEC threshold which is 20% in this case, beyond which the uplink becomes non-compliant.

Figure 471 *Packet Loss*



- **Event Logs**—When an uplink becomes non-compliant, an event is recorded. When the same uplink becomes compliant adhering to the set SLAs, another event is recorded. The **Event Logs** table provides information about all such events. It displays the timestamp and a detailed event statement that contains the policy name, the uplink name, the probe IP, and the reason for non-compliance, if it is a non-compliance event.

Figure 472 *Event Logs*



Live monitoring is enabled for sections that display status, such as:

- The **path Steering Summary**
- Real time state of the **Event Logs**
- **Path Steering Summary**—Path steering summary of the primary, secondary, and standby uplinks.
- **Path Steering Details**—Displays the following path steering details:
- **Traffic Path**—Displays traffic path steering status for each link associated with the WAN policy.

- **Status**—Provides a graphical representation of the status of uplinks.
- **MPLS (Primary)**
- **Comcast (Secondary)**
- **LTE (Standby)**
- **Traffic Steer**
- **Traffic Classification**—Displays charts showing client traffic trends to application, application categories, website categories, and websites of a specific security reputation score. The **Traffic Classification** section also shows application with the highest security threat score. To view the traffic classification based on application, application category, and website category, you must enable **Deep Packet Inspection** on the Branch Gateways.

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > LAN > Summary

The **Summary** tab under **Manage** > **LAN** page in the gateway dashboard displays the following sections:

- Port Status
- LAN Interfaces Summary
- VLAN Interfaces Summary

Viewing the LAN > Summary Tab

To navigate to the **LAN > Summary** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.

4. Under **Manage**, click **LAN** > **Summary**.

   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Port Status

Provides a graphical representation of the LAN link availability of the Branch Gateway. Also provides a quick view of the LAN port status. Click a LAN port to view the **Port Details** pop-up page.

Figure 473 *LAN port status*

LAN Interfaces Summary

The table displays the summary of LAN interfaces and total number of LAN interfaces. The following details are displayed for the port:

- **Port**—Port number. Click on the Port to open the **Port Details** pop-up page.
- **Admin State**—Administrative state of the LAN interface. Values are **Enabled** or **Disabled**.
- **Operational State**—Operational state of the LAN interface. Values are **Up** or **Down**.
- **Port Speed**—Port speed.
- **VLANs**—Range of VLANs.
- **MTU**—MTU value.

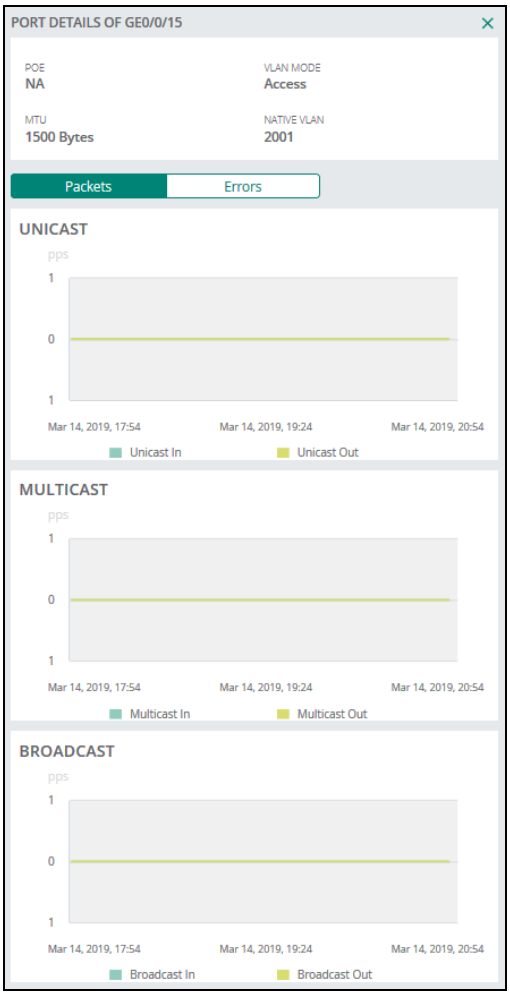
Port Details Pop-Up page

Click on a port in the **Port Status** or **LAN Interfaces Summary** page to display the **Port Details** pop-up page. The page has two tabs, **Packets** and **Errors**.

- The following graphs are displayed under the **Port Details > Packets** tab:
  - **Unicast**—The number of unicast packets per second.
  - **Multicast**—The number of multicast packets per second.
  - **Broadcast**—The number of broadcast packets per second.

  Hover over any point of time on the x-axis to get data about packets for that instant of time.

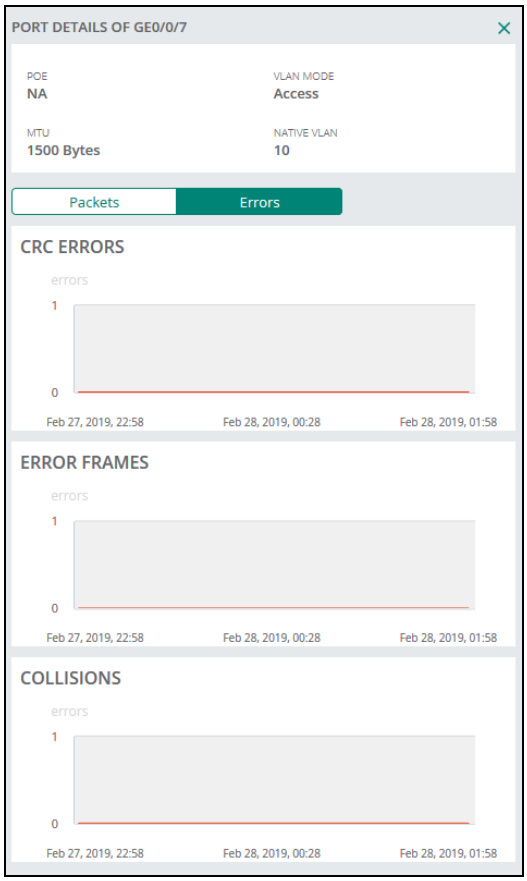
Figure 474 *Port Details—Packets*



- The following graphs are displayed under the **Port Details** > **Errors** tab:
  - **CRC Errors**—The number of cyclic redundancy errors logged.
  - **Error Frames**—The number of error frames logged.
  - **Collisions**—The number of collisions encountered.

Hover over any point of time on the x-axis to get data about packets for that instant of time.

Figure 475 *Port Details—Errors*

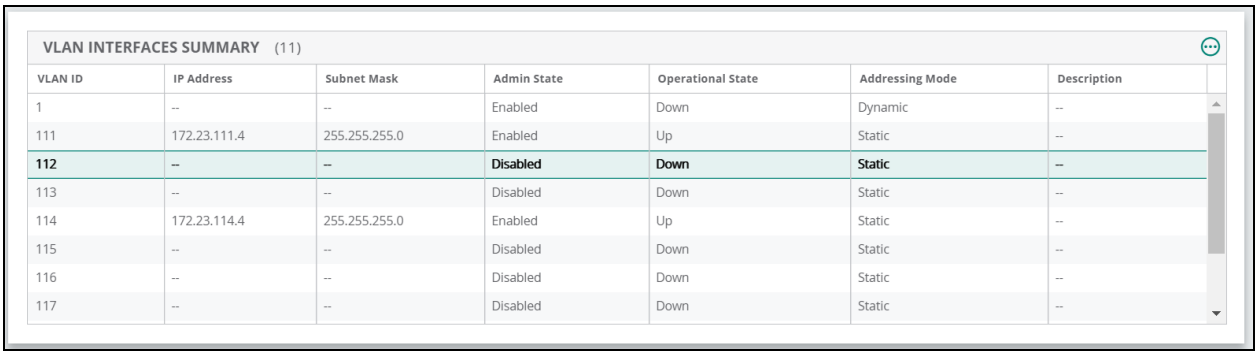


VLAN Interfaces Summary

The table displays the summary of VLAN interfaces and total number of VLAN interfaces. The following details are displayed:

- **VLAN ID**—VLAN ID number.
- **IP Address**—IP address.
- **Subnet Mask**—Subnet mask of the IP address.
- **Admin State**—Administrative state of the VLAN interface.
- **Operational State**—Operational state of the VLAN interface.
- **Addressing Mode**—Type of addressing mode.
- **Description**—Description of the VLAN.

Figure 476 *VLAN Interfaces Summary*



VLAN INTERFACES SUMMARY (11)

VLAN ID	IP Address	Subnet Mask	Admin State	Operational State	Addressing Mode	Description
1	--	--	Enabled	Down	Dynamic	--
111	172.23.111.4	255.255.255.0	Enabled	Up	Static	--
112	**--**	**--**	**Disabled**	**Down**	**Static**	**--**
113	--	--	Disabled	Down	Static	--
114	172.23.114.4	255.255.255.0	Enabled	Up	Static	--
115	--	--	Disabled	Down	Static	--
116	--	--	Disabled	Down	Static	--
117	--	--	Disabled	Down	Static	--

Live monitoring is available for the following:

- **Port Status**
- Operational state of the LAN interface in **LAN Interfaces Summary** table

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > LAN > DHCP

The **DHCP** tab under **Manage** > **LAN** page in the gateway dashboard displays the following sections:

- DHCP Pools
- Active Leases

Viewing the LAN > DHCP Tab

To navigate to the **WAN > DHCP** tab in the gateway dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in **List** view.

3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.

4. Under **Manage**, click **LAN** > **DHCP**.

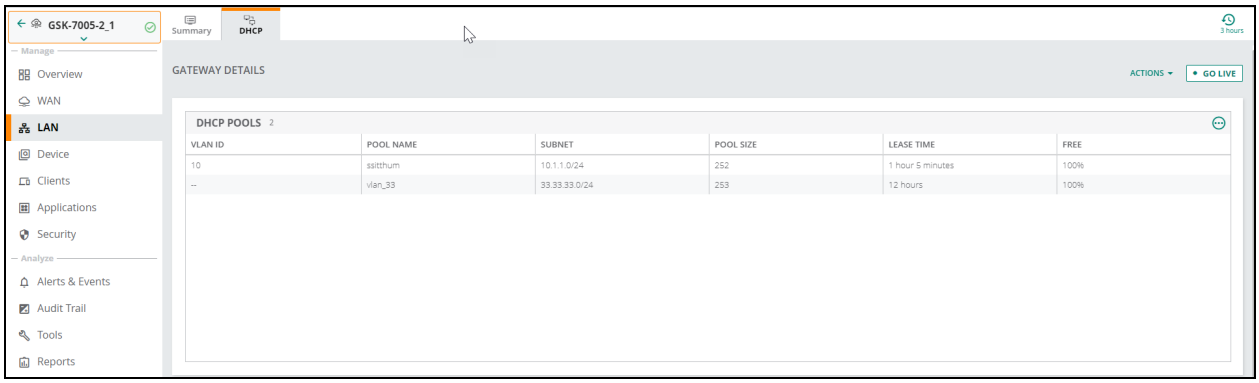
   To exit the gateway dashboard, click the back arrow on the filter.

   You can change the time range for the **DHCP** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

DHCP Pools

- The table displays the summary of DHCP pools and total number of DHCP pools. The following details are displayed:
  - **VLAN ID**—VLAN ID number.
  - **Pool Name**—Name of the DHCP pools.
  - **Subnet**—IP address of the client subnet.
  - **Pool size**—Size of the pool.
  - **Lease time**—Lease time of the pool.
  - **Free**—Number of addresses available.

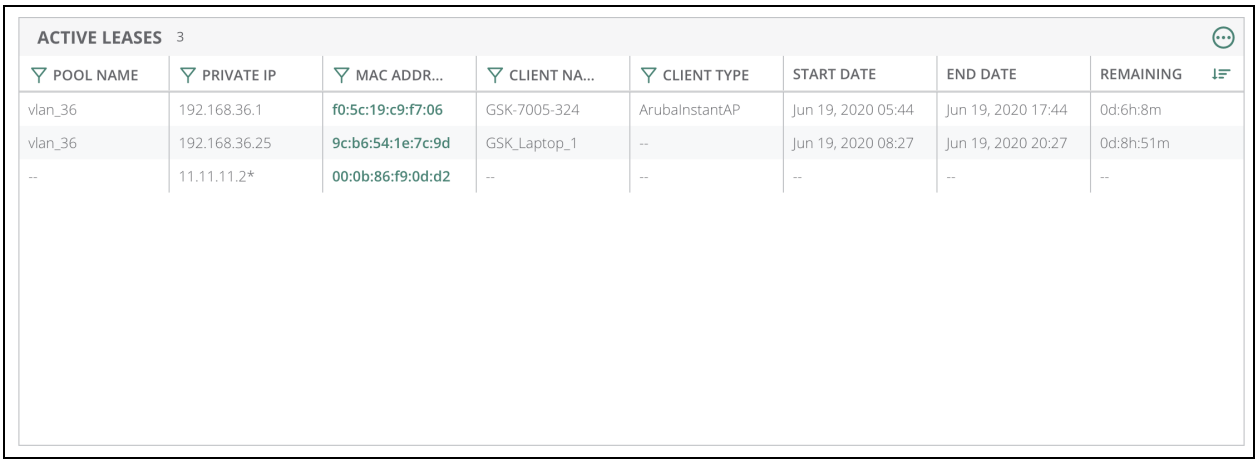
Figure 477 *DHCP Pools*



Active Leases

- The table displays the summary of active leases total number of active leases. The following details are displayed:
  - **Pool Name**—Name of the DHCP pools.
  - **Private IP**—IP address of the client subnet. The IP address with asterisk symbol (*) indicates it is a reserved IP address.
  - **MAC Address**—MAC address of the client. Clicking on the address takes you to the Client page.
  - **Client Name**—Client name.
  - **Client Type**—Client type.
  - **Start Date**—Start date and time of the lease.
  - **End Date**—End date and time of the lease.
  - **Remaining**—Remaining time for the lease to expire.

Figure 478 *Active Leases*



Live monitoring is available for the following:

- **Port Status**
- Operational state of the LAN interface in **LAN Interfaces Summary** table

Actions

The **Actions** drop-down list contains the following options (the **Clear IPSec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway. See Rebooting a Gateway
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. See Opening a Remote Console
- **Clear IPSec SA**—Clears the IPSec Security Associations (SA). See Clearing IPSec SA
- **Clear ISAKMP SA**—Clears the ISAKMP SA. See Clearing ISAKMP SA

Go Live

The **Go Live** link redirects to the **Manage** > **WAN** > **Summary** tab in the gateway dashboard. See the **Go Live** section in the Gateway > WAN > Summary page.

Gateway > Applications > Visibility

The **Visibility** tab under **Manage** > **Applications** in the gateway dashboard displays the following tabs:

- Applications Tab in List View
- Websites Tab in List View

The **Visibility** dashboard displays charts showing client traffic trends with respect to application, application categories, website categories, and websites of a specific security reputation score. To view the traffic classification based on application, application category, and website category, you must enable **Application Visibility** service on Branch Gateways.

To view the application usage metrics for gateways, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one Branch Gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view.
3. Click a gateway under **Device Name**.

   The dashboard context for the specific gateway is displayed.
4. Under **Manage**, click **Applications** > **Visibility** .

   The Visibility dashboard is displayed with two second-level tabs, **Applications** and **Websites**.

   You can change the time range for the **Visibility** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

NOTE

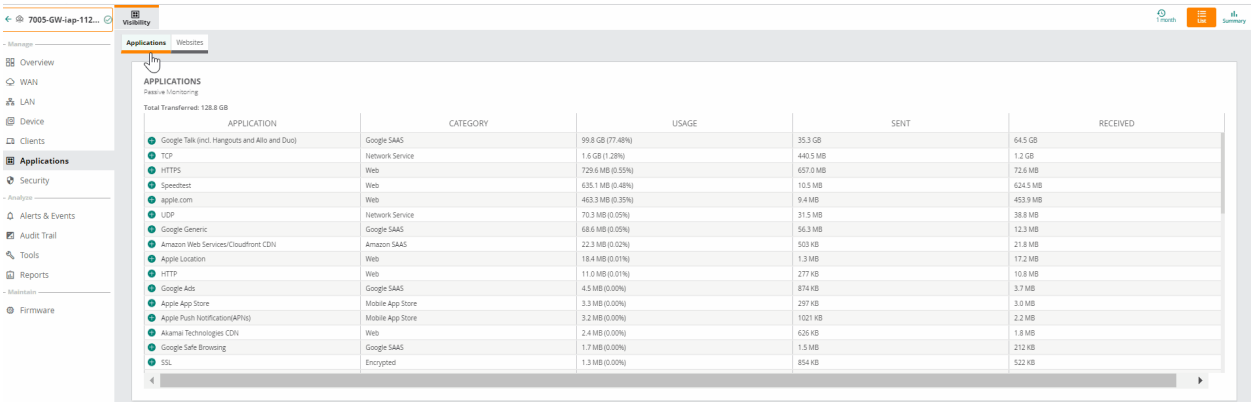
Click the **List** and the **Summary** icons on the **Application** and **Websites** sections to toggle between the dashboard views.

Applications Tab in List View

The **Visibility** > **Applications** tab in **List** view displays the following:

- **Application**—Displays the top N applications based on total bandwidth usage. Apart from the top N, the rest of the applications are grouped under the **Unclassified** category. Click the **+** sign next to the service name to expand an application in List view. A graph is displayed with date and time on the x-axis and usage on the y-axis. The graph displays the amount of data sent and received by the application over a period of time. To get the data sent and data received information for a specific day, hover over a point on the x-axis.
- **Category**—Displays the top N web categories based on total bandwidth usage. Apart from the top N, the rest of the web categories are grouped under the **Unclassified** category.
- **Usage**—Displays the bandwidth usage of each application.
- **Sent**—Displays the amount of data sent by the application.
- **Received**—Displays the amount of data received by the application.

Figure 479 *Visibility > Applications in List View*

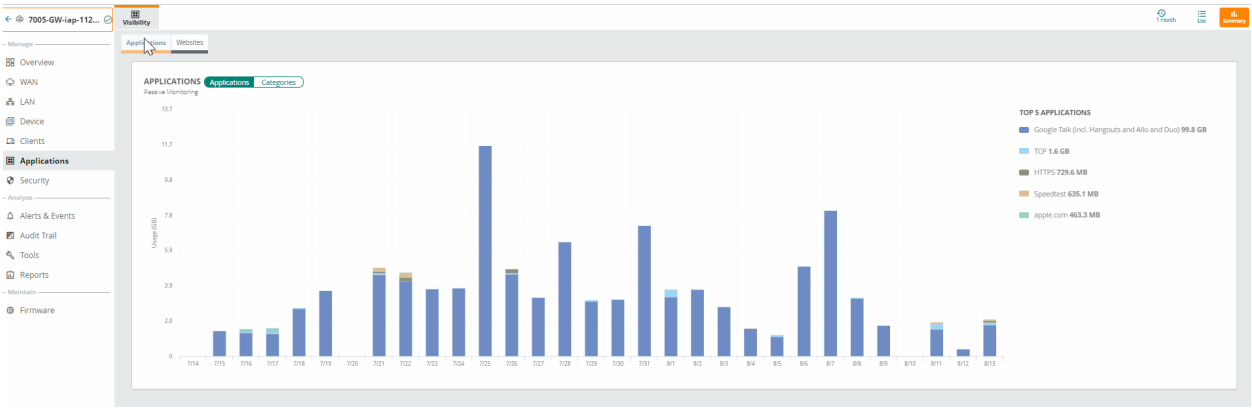


Applications Tab in Summary View

The **Visibility** > **Applications** tab in **Summary** view displays the following:

- **Applications**—Displays the graph top 5 applications based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover over a bar on the x-axis.
- **Categories**—Displays the top 5 web categories based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover over a bar on the x-axis

Figure 480 *Visibility > Applications in Summary View*

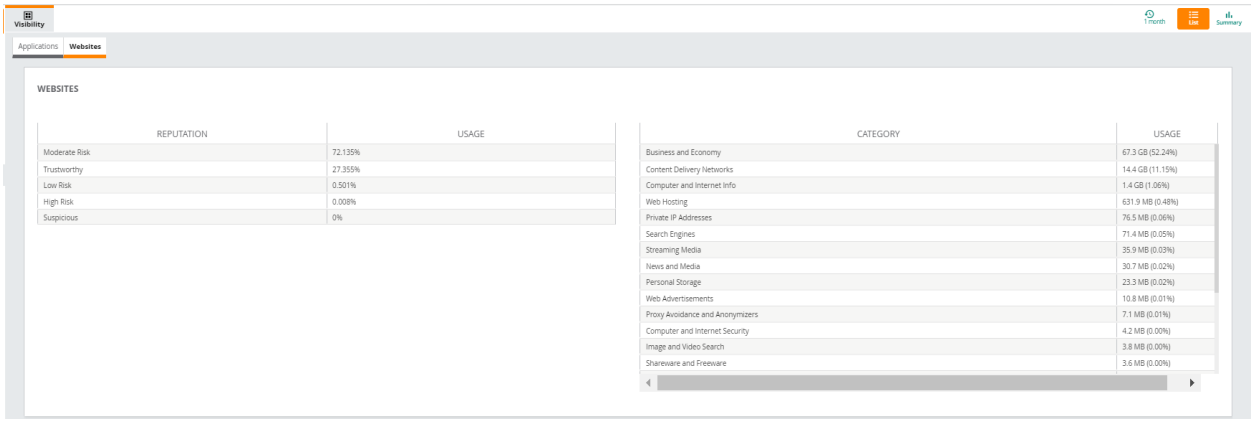


Websites Tab in List View

The **Visibility** > **Websites** tab in **List** view displays the following:

- **Reputation and Usage**—Displays the reputation and usage percentage.
- **Category and Usage**—Displays the WebCC category and the usage percentage.

Figure 481 *Visibility > Websites in List View*



Websites Tab in Summary View

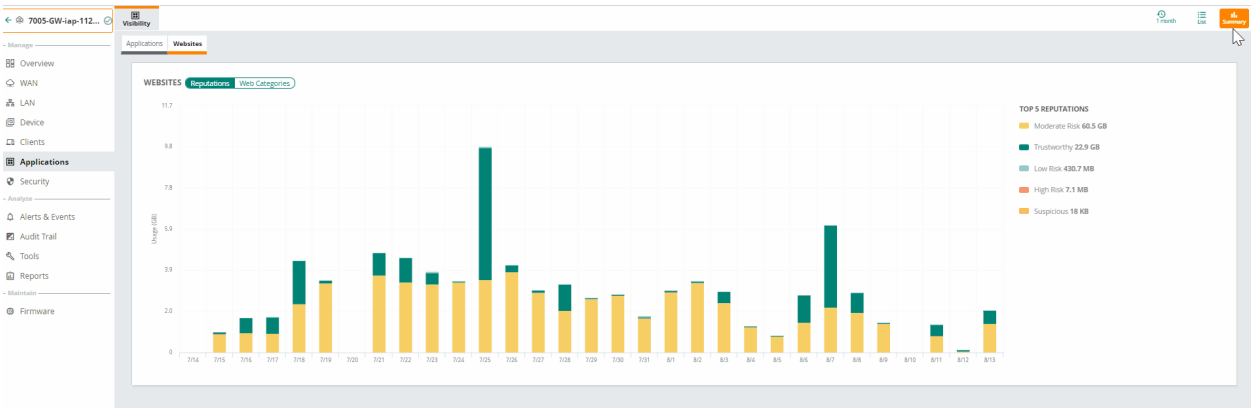
The **Visibility** > **Websites** tab in **Summary** view displays the following:

- **Reputations**—Displays the top 5 reputations based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover

over a bar on the x-axis.

- **Web Categories**—Displays the top 5 WebCC categories based on total bandwidth usage. The graph displays date on the x-axis and usage on the y-axis. To get the total data usage information for a specific day, hover over a bar on the x-axis.

Figure 482 *Visibility > Websites in Summary View*



Downloading Gateway Details

You can download the gateway details as a .csv file.

To download the gateway details, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. In the **Gateways** table, click the download icon to download the gateways details as a .csv file.

   A .csv file is downloaded.

Related links:

Deleting a Gateway

Rebooting a Gateway

Deleting a Gateway

Aruba Central allows you to delete a gateway only when the device is offline. To delete an offline gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

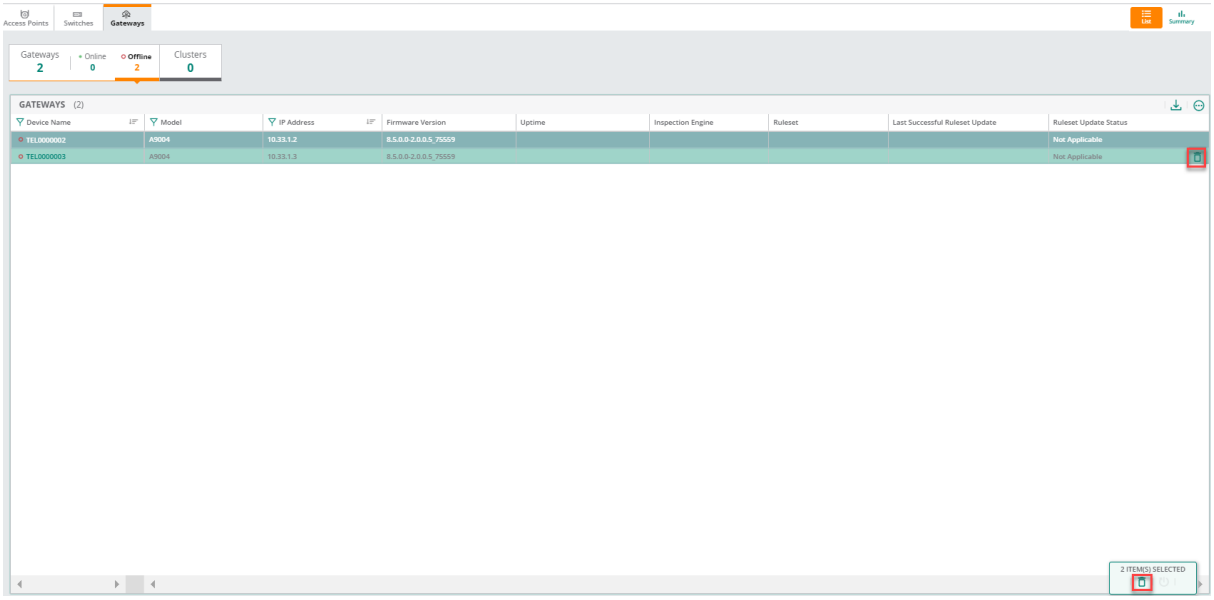
   A list of gateways is displayed in **List** view under the second-level **Gateways** tab.

3. Click **Offline** to display a table with the list of offline gateways.
4. From the **Gateways** table, select the gateway(s) that you want to delete. To select a gateway, click on any column except **Device Name**.

NOTE

Clicking on a device name in the Device Name column opens the gateway dashboard.

5. Click the **Delete** button at the bottom of the page to delete all the selected gateways. To delete a particular gateway, click the **Delete** button available at the end of the row for that gateway.



6. Confirm deletion.

The offline gateway is deleted. However, the device still can be found in Aruba Central database, as the device entry remains in the **Device Inventory** page.

Rebooting a Gateway

Aruba Central allows you to reboot a gateway. The **Reboot Gateway** option is available under the **Actions** drop-down for many gateway pages. The following procedure explains how to reboot a gateway in the **Manage** > **Overview** > **Summary** page for a gateway.

NOTE

The **Reboot Gateway** option is only available for online gateways.

To reboot a gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the Gateways table, click the gateway to reboot.

5. You can delete the gateway in multiple ways. Perform one of the following steps:
   - In the **Actions** drop-down list, click **Reboot Gateway**.
   - Click the **Reboot** button available at the end of the row for that gateway.
   - Click the **Reboot** button at the bottom of the page.

   A **Reboot** dialog box is displayed.
6. Click **Yes** to reboot the gateway.

   All clients connected to this gateway are disconnected and gateway reboots.

The **Gateway Details** page takes less than a minute to update the interface status after the gateway is rebooted and reconnected to Aruba Central.

Opening a Remote Console

Aruba Central allows you to open the remote console for a CLI session through SSH for a gateway. Ensure that you allow SSH over port 443.

To open the remote console for a gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the Gateways table, click the gateway for which you want to open the remote console.

   The **Overview** > **Summary** page corresponding to the gateway is displayed.
5. In the **Actions** drop-down list, click **Open Remote Console**.

   A CLI session dialog box is displayed. The default user ID is **Admin**, but you can edit and customize the user ID. Ensure that the custom user ID is mapped to the device.

Clearing IPSec SA

Aruba Central allows you to clear the IPsec Security Association (SA) for a gateway. The **Clear IPSec SA** option is available under the **Actions** drop-down for many gateway pages. The following procedure explains how to clear **IPSec SA** in the **Manage** > **Overview** > **Summary** page for a gateway.

The **Clear IPSec SA** option is only available for online gateways.

To clear IPSec SA for a gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.

3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the **Gateways** table, click the gateway for which you want to clear the **IPSec SA** option.

   The **Overview** > **Summary** page corresponding to the gateway is displayed.
5. In the **Actions** drop-down list, click **Clear IPSec SA**.

Clearing ISAKMP SA

Aruba Central allows you to clear the ISAKMP Security Association (SA) for a gateway. The **Clear ISAKMP SA** option is available under the **Actions** drop-down for many gateway pages. The following procedure explains how to clear **ISAKMP SA** in the **Manage** > **Overview** > **Summary** page for a gateway.

The **Clear IPSec SA** option is only available for online gateways.

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view under the second-level **Gateways** tab.
3. Click the second-level **Online** tab to display a table with the list of online gateways.
4. In the Gateways table, click the gateway for which you want to clear the **ISAKMP SA** option.

   The **Overview** > **Summary** page corresponding to the gateway is displayed.
5. In the **Actions** drop-down list, click **Clear ISAKMP SA**.

   The clear command is sent successfully and a success message is displayed.

Chapter 34
Monitoring Your Network

This chapter describes the various options available for viewing the device, client, and network details:

Network Overview

In the **Network Operations** app, perform the following steps to access the overall network summary page:

1. Set the filter to **Global**.

   The Global dashboard is displayed.
2. Under **Manage** > **Overview**, the network summary page displays the following tabs:
   - **Network Health**—Displays vital information of the network sorted by site. For more information, see Network Health Dashboard.
   - **WAN Health**—Displays information on WAN Healths.
   - **Summary**—Displays details such as the bandwidth usage in the network, client counts, and cluster-specific details. For more information, see Global—Summary.
   - **WiFi Connectivity**—Displays connection details of all the clients connected to an AP. For more information, see Wi-Fi Connectivity.
   - **AI Insights**—Displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization at AP. For more information, see The AI Insights Dashboard.

Network Health Dashboard

The Network Health dashboard displays information of the network sorted by site. This dashboard displays information on network devices and WAN connectivity of individual sites.

To launch the **Network Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Overview > Network Health** to launch the **Network Health** dashboard.

The **Network Health** dashboard has two views, you can toggle between them by clicking on the view icons.

- **Summary**— This view displays the vital network information of individual sites on cards mapped by geographical location. Sites are marked with location pins—green pin for a site with no issues and red pin for a site with potential issues. Hover over a pin to view more details about a site in a card view. When there are multiple sites in a region and cannot be displayed as individual pins on the map view, they appear as numbers on a round pin in the condensed view. The pin color is red if it has one site in the Down status and green if all the sites are Up. Click the pin to zoom in and view the sites on the map.

The pin on the map changes to red when the value in one of the following parameters in the **List** view is greater than zero for the **Down** status:

- **Number of devices**
  - **Status**
  - **High Mem Usage**
  - **High CPU Usage**
  - **High CH Utilization**
  - **High Noise**
- **Uplink Status**
- **Tunnels Status**

The following table lists the information displayed in a Network health card:

Table 299: *Network Health Card*

Item	Description
User experience	Displays the user experience of the devices in the site. This information is displayed when there is at least one UXI sensor deployed in a site. Clicking on the **User experience** redirects you to the UXI dashboard for further troubleshooting. The UXI Dashboard allows you to configure and manage UXI sensors. For more information, see User Experience Insight Sensors Integration.
Insights	Displays the number of AI Insight reports available for the site. The reports are organized by degree- **High**, **Medium,** and **Low** depending on the number of events in the network.
Devices	Displays the number of connected and Offline APs for the site. Clicking on one of the numbers redirects you to the **Devices** dashboard page of the site.
Clients	Displays the number of connected and failed clients for the last three hours. Clicking on one of the numbers redirects you to the **Clients** dashboard page of the site.
RF Coverage	Provides a link to view or configure the floorplan for the site. Clicking on the **Floorplan** redirects you to the floor plans page of the site
Uplinks	Displays the uplink connectivity status of devices in the site. This information is displayed when there is at least one uplink in the site.
Tunnels	Displays the connectivity status of tunnels in the site. This information is displayed when there is at least one tunnel in the site.
High Mem usage	Displays the number of devices with high memory utilization in the site. This information is displayed when there is at least one device with high memory utilization in the site.

Table 299: *Network Health Card*

Item	Description
High CPU usage	Displays the number of devices with high CPU usage in the site. This information is displayed when there is at least one device with high CPU usage in the site.
High CH utilization	Displays the number of APs with a higher channel utilization in the 5 GHz and 2.4 GHz radio bands. This information is displayed when there is at least one AP with a higher channel utilization in the 5 GHz or 2.4 GHz radio bands in the site.
High noise utilization	Displays the number of APs with high RF noise in the 5 GHz and 2.4 GHz bands. This information is displayed when there is at least one AP with a higher noise utilization in the 5 GHz or 2.4 GHz radio bands in the site.

- **List**—This view displays the global network report in a list sorted according to individual sites. Clicking on the site name will take you to the **Site Health** dashboard page. The data columns listed in the page can be managed by clicking on the hamburger icon (☰) on the right of the column header. The report can be filtered by clicking on the filter labels below the column name. Selecting a filter label filters the results based on the field values of the column is ascending or descending order, sites with zero issues will not be displayed. The order of the results displayed can be toggled by clicking the or icon beside the filter.

  The **Network Health** dashboard displays the information listed in the table below.

Table 300: *Network Health Dashboard*

Header	Description
Site Name	The name of the site. Clicking on the site name will take you to the **Site Health** dashboard page (**Site > Overview > Site Health** tab). To search for a site by name, click on the **Site Name** label and enter the name of the site.
AI Insights	Displays the number of AI Insight reports available for the site. The reports are organized by degree- **High**, **Medium,** and **Low** depending on the number of events in the network.
Number of Devices	
Status	The number of devices that are in Up or Down state in a site. Click the **List** icon and hover your mouse over a field in the column to view the following details: ▪ WLAN Devices Down ▪ Wired Devices Down ▪ Branch Devices Down
High Memory Usage	The number of devices with high memory utilization in the site. Click the **List** icon and hover your mouse over a field in the column to view the following details: ▪ WLAN High Memory ▪ Wired High Memory ▪ Branch High Memory
High CPU Usage	The number of devices with high CPU usage in the site. Click the **List** icon and hover your mouse over a field in the column to view the following details: ▪ WLAN CPU High ▪ Wired CPU High

Table 300: *Network Health Dashboard*

Header	Description
	▪ Branch CPU High
High CH Utilization	The number of APs with a higher channel utilization in the 5 GHz and 2.4 GHz radio bands.
Clients	Displays the number of connected and failed clients for the site.
High Noise	The number of APs with high RF noise in the 5 GHz and 2.4 GHz bands.
WAN	
Uplink Status	Displays the uplink connectivity status of devices in the site. The data is classified into two columns: devices with no issues and devices with no uplink connectivity.
Tunnel Status	Displays the connectivity status of tunnels in the site. The data is classified into two columns: tunnels with no issues and tunnels with no connectivity.

WAN Health—Global

The **WAN Health** tab provides detailed information of the network health status and usage for the sites in which Branch Gateways and VPNCs are configured in your setup.

To navigate to this page:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Overview** > **WAN Health**.
3. Click the **List** icon to navigate to the list view of **Transport** and **Site** pages.

Page Views

The **WAN Health** page offers the following views:

- **Summary**—This view provides a pictorial view of the network across various sites. The sites are color coded; red indicates potential issues and green indicates that there are no issues. To change the zoom level, click the zoom icons. You can click the different site on the map to view details.
- **List**—Primarily provides numerical representation of data under **Transport** and **Site** tabs.
  - **Transport**—The columns categorized under **Uplink** and **Performance** provide textual values. You can select a device from the **Name** column to view the details about that device's health.
  - **Site**—The **Site Type** and **Connectivity Status** columns provide textual values. You can select the site from the **Site Name** column to view details about that site's health.

This page uses the following indicators to present information on status of the network health:

- Grey ● bullet icon—Indicates no issues.
- Red ● bullet icon—Indicates potential issues.

WAN Health

Table 301: *Gateways Network Health Page*

Header	Totals	Description
Site Name	Displays the total number of sites.	Name of the site. Use the column filter bar to search for a particular site. Click the site name to open the **Site Health** page. For more information, see the *Site Health* section in the *Aruba Central Help Center*.
Site Type	Displays the total number of sites for each site type.	Displays whether the device is deployed as a hub or spoke. ■ To filter gateways provisioned as a hub, click **Hub**. ■ To filter gateways provisioned as a spoke, click **Spoke**. ■ To filter gateways deployed as cloud instances, click **Cloud**. Only hubs can be deployed as cloud instances, so if a hub is deployed as a cloud instance, the site type is **Cloud**.
Device Status	Displays the total number of devices in Up and Down state.	Displays the total count of devices in the UP and DOWN states. ■ To filter devices in UP sate, click **Up**. ■ To filter devices in DOWN sate, click **Down**.
Connectivity	Displays the total number of links.	Displays the following information: ■ **Status**—Displays the overall connectivity status. One of the following statuses is displayed: ◦ Up ◦ Partial ◦ Down Hover over the column to view the circuit status, tunnel status, overlay status, and underlay status separately.
Performance	Displays the average value for site availability.	Displays the following metrics: ■ **Site Availability**—Displays the site availability. The range is from 0 to 100 percent. To filter site availability, click the column filter bar and enter values in the **Min** and **Max** text boxes. Hover your mouse over the column to view site availability on a per provider basis.

For information about a particular site, see WAN Health—Site.

WAN Health—Transport

The **WAN Health—Transport** page displays the transport health of all uplinks belonging to an end-user. This page helps in monitoring network health of all uplinks based on active monitoring probes.

To launch the **WAN Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Overview** and select the **WAN Health** tab.
3. Click **List** view to launch the **Transport** page.

You can change the time range for the **Transport** tab by clicking the time range filter and selecting one of the available options: 3 hours, 1 day, and 1 week.

The **Transport** page displays the following information :

Table 302: *WAN Health—Transport*

Content	Description
Name	Displays the name of the device. **Search Options**: ■ The icon allows you to search a particular gateway by its name. Clicking on the gateway name redirects you to the Device overview dashboard. ■ The and icons allow you to sort the gateways in ascending or descending order.
Site	Displays the name of the site. Type the name of a site in the filter field to display the list of gateways from a particular site. **Search Options**: ■ The icon allows you to search a particular site by its name and display the list of gateways belonging to the site. ■ The and icons allow you to sort the sites in ascending or descending order.
Status	Displays the gateways whose uplinks are in Up or Down state. **Search Options**: ■ Select **Up** or **Down**from the drop-down filter to display the gateways of a particular state. ■ The and icons allow you to sort the status in ascending or descending order.
Transport	Displays the transport type used by the uplink. Supported transport types are: ■ MPLS ■ LTE ■ Internet ■ Metro-Ethernet Select one of the transport types from the drop-down filter to display the uplinks of a particular transport type. The and icons allow you to sort the transport type in ascending or descending order.
Carrier	Displays the uplink carrier. **Search Options**: ■ The icon allows you to search a particular carrier by its name. Clicking on the carrier name redirects you to the **WAN Summary** dashboard > **WAN Availability** tab. ■ The and icons allow you to sort the carrier names in ascending or descending order.
Type	Displays whether the uplink is Primary or Backup. **Search Options**: ■ Select **Primary** or **Backup** from the drop-down filter to display the gateways of a particular type. ■ The and icons allow you to sort the type in ascending or descending order.
Availability	Displays whether the uplink availability is good, fair, or poor based on the availability percentage. ■ Good > 90% ■ Fair > 70% ■ Poor < 70% Select one of the availability options from the drop-down filter to display the gateways of a particular availability percentage.

Table 302: *WAN Health—Transport*

Content	Description
	The  and  icons allow you to sort the availability in ascending or descending order.
Usage	Displays the uplink usage in gigabytes. The  and  icons allow you to sort the usage in ascending or descending order.
Throughput	Displays the uplink throughput. The  and  icons allow you to sort the throughput in ascending or descending order.
Loss	Displays the uplink packet loss is good, fair, or poor. ■ Good < 0.5% ■ Fair < 2% ■ Poor > 2% Select either **Good**, **Fair**, or **Poor** from the drop-down filter to display the uplinks with a particular packet loss percentage. The  and  icons allow you to sort the loss in ascending or descending order.
Latency	Displays whether the uplink latency is good, fair, or poor. ■ Good < 200ms ■ Fair < 400ms ■ Poor > 400ms Select either **Good**, **Fair**, or **Poor** from the drop-down filter to display the uplinks with a particular latency calculation. The  and  icons allow you to sort the latency in ascending or descending order.
Jitter	Displays whether the uplink jitter is good, fair, or poor. ■ Good < 200ms ■ Fair < 400ms ■ Poor > 400ms Select either **Good**, **Fair**, or **Poor** from the drop-down filter to display the uplinks with a particular jitter calculation. The  and  icons allow you to sort the jitter in ascending or descending order.
MOS	Displays the uplink quality based on the Mean Opinion Score (MOS) calculated using loss, latency, and jitter. The  and  icons allow you to sort the MOS in ascending or descending order.

WAN Health—Site

The **WAN Health** page displays details for the wired, wireless, and gateway devices deployed on the site.

To launch the **WAN Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to a site.
2. Under **Manage**, click **Overview > WAN Health** to launch the **WAN Health** dashboard.
3. Click the **Site** tab.

   The site health information is displayed in the **List** view.

The following indicators are used for the status of the site health:

- Grey ● bullet icon—Indicates no issues.
- Red ● bullet icon—Indicates potential issues.

The **WAN Health** dashboard for the site displays the following information:

Table 303: *Gateways Network Health Page*

Header	Totals	Description
Site Name	Displays the total number of sites.	Name of the site. Use the column filter bar to search for a particular site. Click the site name to open the **Site Health** page. For more information, see Site Health.
Site Type	Displays the number of sites for each site type.	Displays whether the device is deployed as a hub or spoke. Only hubs can be deployed as cloud instances, so if a hub is deployed as a cloud instance, the site type is **Cloud**.
Device Status	Displays the number of devices in **Up** and **Down** state.	Displays the total count of devices in the Up and Down states for each site.
Connectivity	Displays the number of links.	Displays the overall connectivity status and it can be one of the following: ■ Up ■ Partial ■ Down Hover over the value to view the circuit status, tunnel status, overlay status, or underlay status in a text box.
Performance	Displays the average value for site availability.	Displays the site availability. The range is from 0 to 100 percent. To filter site availability, click the column filter bar and enter the **Min** and **Max** values in the text boxes. Hover over the value to view site availability for each provider.

Site Health Dashboard

The **Site Health** dashboard displays details of wired and wireless devices deployed on the site. This page includes information on client connectivity statistics, change logs, health of devices, and RF health of the site.

To launch the **Site Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, set the filter to a site.
2. Under **Manage**, click **Overview > Site Health** to launch the **Site Health** dashboard.

Alternatively, the **Site Health** dashboard can be accessed by selecting a site from the **Network Health** dashboard page. The **Site Health** dashboard displays the information listed in the table below:

Table 304: *Site Health Dashboard*

Content	
Name	Name of the site.
Location	Location of the site.

Table 304: *Site Health Dashboard*

Content	
APs	Number of APs deployed on the site.
Switches	Number of switches deployed on the site.
Gateways	Number of gateways deployed on the site.
Summary Statistics	A graphical representation of the number of clients (wired and wireless) and their bandwidth usage for the selected time range.
Change Log	A visual representation of change logs for configuration, firmware, and reboot changes in the selected time range. Select a column in the graph and click on the **Config Log**, **Firmware Log** and **Reboot Log** button to view detailed information logs on the corresponding events in the site.
System Health Indicators	
Down Devices	This graph shows the count of devices with DOWN status. The graph displays the following information: ■ Total number of devices ■ Number of unique devices that were DOWN ■ Minimum and maximum device downtime. To view more details, select a time range in the graph and click on **See Devices**. A pop-up window displays the details of devices with DOWN status and their Up and Down time in percentage. You can also add other metrics such as CPU, Memory, 5 GHz and 2.4 GHz Channel Utilization, and 5 GHz and 2.4 GHz Noise Floor by clicking on the **Add Metric** button. A particular device can be filtered from the list by clicking on the filter icon ( )and entering the name of the device.
High CPU & High Memory	This graph shows the total count or percentage of devices with high CPU utilization and high memory utilization. ■ **High CPU Utilization**—This graph displays the total number of devices, number of unique devices with high CPU utilization, and minimum and maximum number of devices with high CPU utilization. You can also view the total count or percentage of maximum and minimum number of devices with high CPU utilization for a specific time when you hover your mouse over the graph. ■ **High Memory Utilization**—This graph displays the total number of devices, number of unique devices, the minimum and maximum number of devices with high memory utilization. You can also view the total count or percentage of maximum and minimum number of devices with high memory utilization for specific time when you hover your mouse over the graph. ■ **Threshold Setting Widget**—You can also choose to view the graph details based one of the following criteria by clicking the ( ) icon and selecting any of the following options: ◦ >70% CPU utilization ◦ >80% CPU utilization ◦ >90% CPU utilization ◦ >70% memory utilization ◦ >80% memory utilization ◦ >90% memory utilization

Table 304: *Site Health Dashboard*

Content	
	To view more details, select a time range in the graph and click on **See Devices**. A pop-up window displays the details of devices with high CPU utilization and memory utilization with their individual minimum and maximum values. You can add other metrics such as 5 GHz and 2.4 GHz Channel Utilization , 5 GHz and 2.4 GHz Noise Floor, and Device Down time for the devices by clicking on the **Add Metric** button. A particular device can be filtered from the list by clicking on the filter icon ( ) and entering the name of the device.
RF Health Indicators	
5 GHz Utilization and Noise	This graph displays the total count or percentage of devices with high channel utilization and high noise floor levels for 5 GHz band. ■ **Device Details**—The graph displays total number of devices, number of unique devices with high 5 GHz channel utilization and high noise floor levels, and the minimum and maximum number of devices with high channel utilization. You can also view the total count of maximum and minimum number of devices with high 5 GHz channel utilization and noise for a specific time when you hover your mouse over the graph. ■ **Threshold setting**—You can also choose to view the graph details based one of the following criteria by clicking the ( ) icon and selecting any of the following options: ◦ >60% 5 GHz Utilization ◦ >70% 5 GHz Utilization ◦ >80% 5 GHz Utilization ◦ >-75 dBm 5 GHz Noise ◦ >-80 dBm 5 GHz Noise ◦ >-85 dBm 5 GHz Noise To view more details, select a time range in the graph and click on **See Devices**. A pop-up window displays the details of devices with high CPU utilization and memory utilization with their individual minimum and maximum CPU utilization values. You can add other metrics such as CPU, Memory, 2.4 GHz Channel Utilization, 2.4 GHz Noise Floor, and Device Down time for the devices by clicking on the **Add Metric** button. A particular device can be filtered from the list by clicking on the filter icon ( ) and entering the name of the device.
2.4 GHz Utilization and Noise	This graph displays the total count or percentage of devices with a higher channel utilization and high noise floor levels for 2.4 GHz channel. ■ **Device Details**—The graph displays the total number of devices, number of unique devices with high 2.4 GHz channel utilization and noise floor levels, minimum and maximum number of devices with high channel utilization and noise levels. You can also view the total count of maximum and minimum number of devices with high 2.4 GHz Utilization and Noise for a specific time when you hover your mouse over the graph. ■ **Threshold Setting widget** —You can also choose to view the graph details based one of the following criteria by clicking the ( ) icon and selecting any of the following options: ◦ >60% 2.4 GHz Utilization ◦ >70% 2.4 GHz Utilization ◦ >80% 2.4 GHz Utilization ◦ >-75 dBm 2.4 GHz Noise ◦ >-80 dBm 2.4 GHz Noise ◦ >-85 dBm 2.4 GHz Noise

Table 304: *Site Health Dashboard*

Content	
	To view more details, select a time range in the graph and click on **See Devices**. A pop-up window displays the details of devices with 2.4 GHz channel utilization and 2.4 GHz noise floor with their individual minimum and maximum values. You can add other metrics such as CPU, Memory, 5 GHz Channel Utilization, 5 GHz Noise Floor, and Device Down time for the devices by clicking on the **Add Metric** button. A particular device can be filtered from the list by clicking on the filter icon ( ) and entering the name of the device.
NOTE: The threshold setting widget ( ) is visible only when you bring the mouse pointer closer to its position slightly above the right-hand side of each graph.	

User Experience Insight Sensors Integration

The integration of User Experience Insight (UXI) sensors in Aruba Central enables monitoring the network health of a site from end-user perspective, as seen by the UXI sensors deployed in a site. Once integrated with Aruba Central, the high-level summary of UXI sensor alerts are displayed in the UXI field of the Network Health card in Map view.

UXI Field in Network Health Card

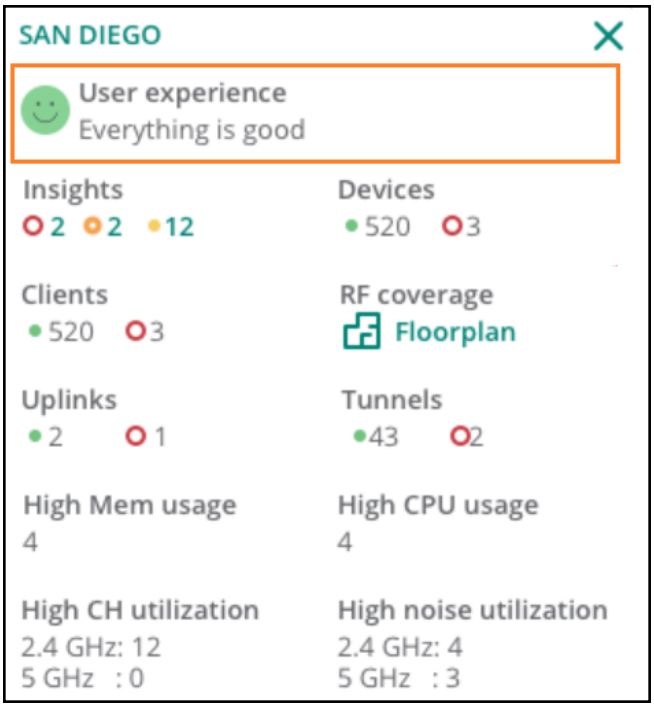
The UXI field in the Network Health card displays the top alert coming from UXI sensors at a site. This information is displayed when there is at least one UXI sensor deployed in the site. Ensure that the UXI sensor is connected to an AP or an SSID broadcasted by the AP in the site.

To display the UXI field of the Network Health card in the Network Health dashboard, complete the following steps:

1. Ensure that the AP that connects to the UXI sensor is mapped to a site in Aruba Central. To create sites, see Managing Sites.
2. Generate an API token and enable UXI integration in Aruba Central. For more information, see UXI Sensors Integration in Aruba Central.
3. Configure UXI integration using the generated API token in UXI Dashboard. For more information, see Aruba Central Integration in UXI Dashboard.

Clicking on the UXI field leads to the UXI Dashboard for further troubleshooting. The following image displays the Network Health card for a test site called San Diego. The highlighted part of the Network Health card displays the UXI field.

For more information about each field in the Network health card, see Network Health Dashboard.



NOTE

The UXI integration with Aruba Central is achieved through APIs to monitor end-user experience at a given site.

UXI Sensors Integration in Aruba Central

To generate an API token and enable UXI integration, complete the following steps:

1. Log in to Aruba Central.
2. In the **Accounts Home**, navigate to **API Gateway** > **System Apps & Tokens**.
3. Click the **+ Add Apps and Tokens**.
4. Configure the name of the application that will use the new token in the **Application Name** field of the **New Token** table.
5. Click the **Applications** drop-down and select **Network Operations** in the **New Token** table.
6. Click **Generate**.
7. When the token is generated, make a note of the displayed **Client ID** and **Client Secret**.

NOTE

The **Client ID** and **Client Secret** are required for Aruba Central integration in the UXI dashboard.

8. Click **Download Token** to save the token in JSON file format.
9. Navigate to **Accounts Home** > **API Gateway** > **APIs**.
10. Make a note of the URL listed under **Documentation** Column.

NOTE

The URL is required for Aruba Central integration in the UXI dashboard.

Aruba Central Integration in UXI Dashboard

To configure UXI integration using the generated API token, complete the following steps:

1. Log in to UXI dashboard.
2. Navigate to **Settings** > **Account** > **Integrations**.
3. Click **Link Central Account**.
4. Configure the following parameters with information generated from Aruba Central:

   a. Central Client ID—Configure the **Client ID** generated from Aruba Central.
   b. Cluster URL—Configure the API **URL** collected from Aruba Central.
   c. Secret—Configure the **Client Secret** generated from Aruba Central.
   d. Token—Upload the JSON file downloaded from Aruba Central.

5. Click **Add**.

When the Aruba Central integration is completed, the UXI field of the Network Health card is displayed in the Map view of the Network Health dashboard, within the range of 5-10 minutes. Clicking the UXI field redirects you to the UXI dashboard for further troubleshooting.

Global—Summary

In the **Global** dashboard, the **Summary** tab displays the **Usage**, **Clients**, **Bandwidth Usage Per Network**, **Client Count Per Network**, **Top APs By Usage**, **Top Clients By Usage**, **Top IAP Clusters By Usage**, **Top IAP Clusters By Clients**, and **WLAN** network details.

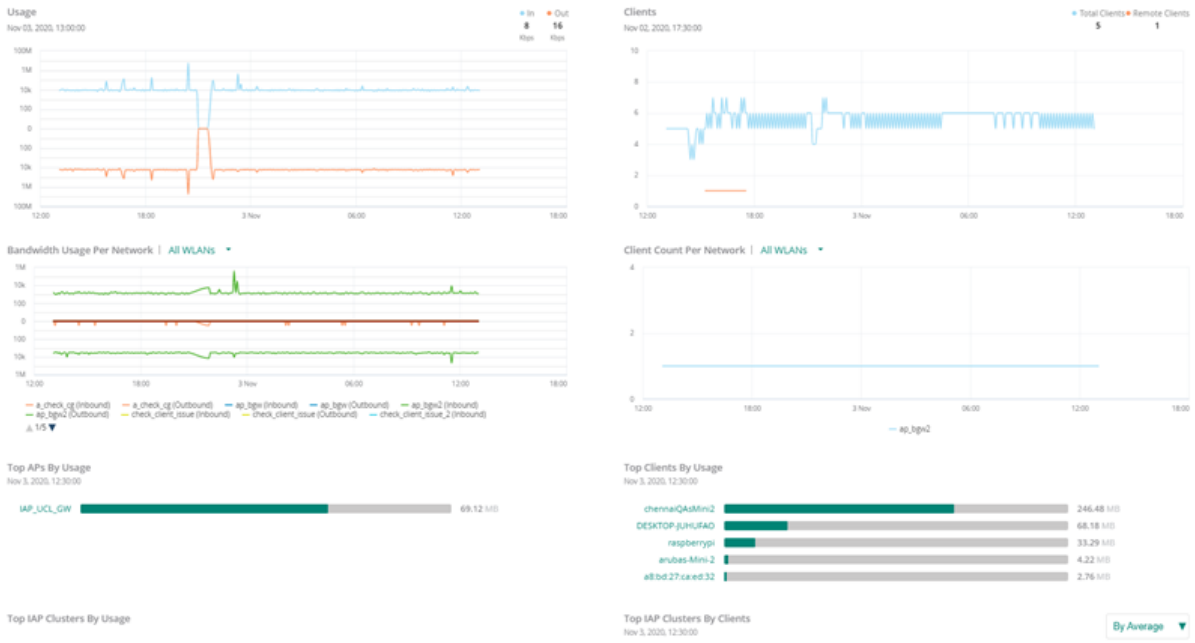
You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

Viewing the Global Summary Page

To navigate to the Global Summary page, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Overview** > **Summary**.
   The Global Summary page is displayed.

Figure 483 *Overview Summary*



The Global Summary page displays the following information.

Table 305: *Global Summary Page Parameters*

Data Pane Item	Description
Usage	Displays the incoming and outgoing data traffic detected on the APs.
Clients	Displays the **Total Clients** that are connected to an AP and **Remote Clients** that are connected to VPN over a specific time period.
Bandwidth Usage Per Network	Displays the incoming and outgoing traffic for all APs per SSID over a specific duration.
Client Count Per Network	Displays the number of clients connected to an AP per SSID over a specific time period.
Top APs By Usage	Displays the list of top APs that utilize the maximum bandwidth in the network. Bandwidth usage includes the sum total of data transmitted and received on the radio interfaces and wired clients connected to the AP.
Top Clients By Usage	Displays the list of top clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network.
Top IAP Clusters By Usage	Displays the list of top AP clusters that utilize the maximum bandwidth in the network.
Top IAP Clusters By Clients	Displays the list of top AP clusters connected to the client that utilize the maximum bandwidth in the network.
WLAN	Displays the list of SSIDs configured. The WLANs table displays the SSID details such the **Name**, **Clients**, **Type**, and **Security**.

Wi-Fi Connectivity

The **Wi-Fi Connectivity** page displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase. The connection phases include **Association**, **Authentication**, **DHCP**, and **DNS**.

To view the connectivity details page, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, site, or all devices in the filter, set the filter to one of the options under **Group** or **Site**.
   - For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Overview**, click **Wi-Fi Connectivity**.

By default, the graphs on the **Wi-Fi Connectivity** page is plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** icon. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month.

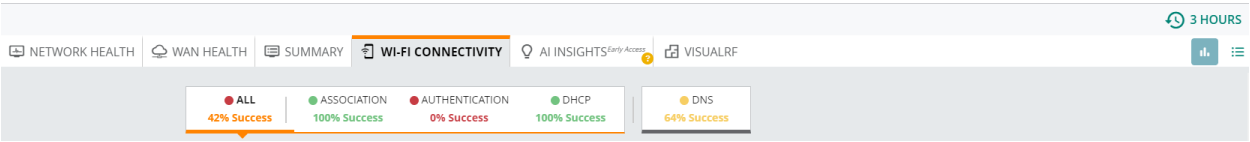
This section includes the following topics:

- Connectivity Summary Bar
- Connection Experience
- AI Insights
- Connection Problems
- Connection Events

Connectivity Summary Bar

The connectivity summary bar displays the details of all clients in percentage. It displays the percentage success rate of each stage for the users to know the network performance.

Figure 484 *Connectivity Summary Bar*



The following table describes the information displayed in each section:

Table 306: *Connectivity Summary Bar*

Field	Description
All	Displays the aggregated success percentage of Association, Authentication, and DHCP for all clients connected to the network.
Association	Displays the percentage of successful attempts made by a client to connect to the network.
Authentication	Displays the percentage of successful attempts of client authentication.

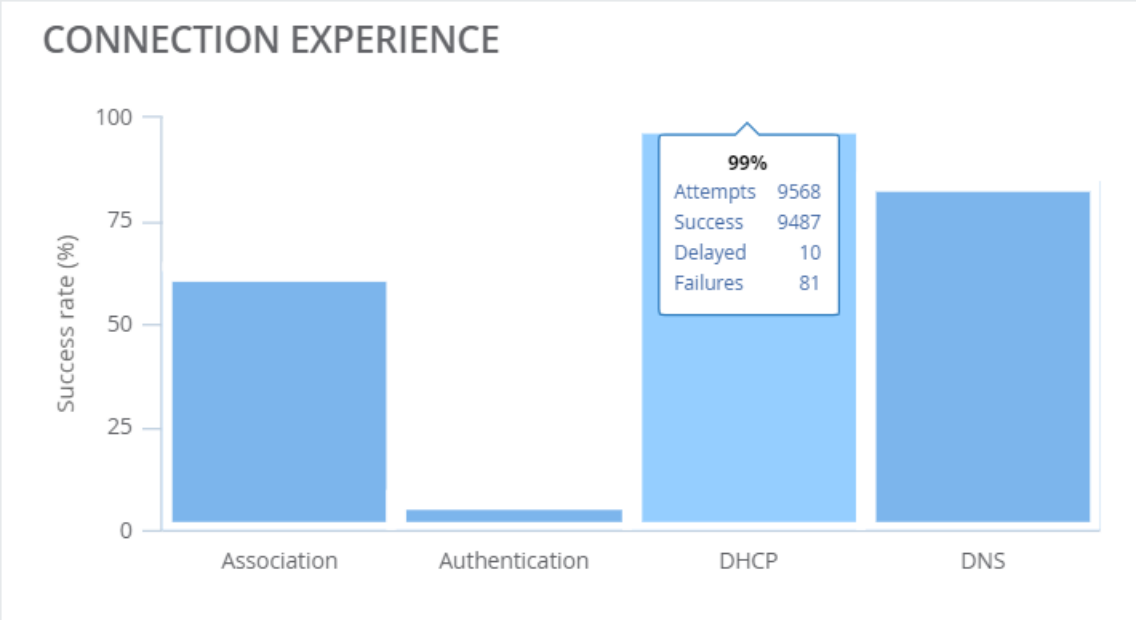
Table 306: *Connectivity Summary Bar*

Field	Description
DHCP	Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client.
DNS	Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network.

Connection Experience

The **Connection Experience** tile displays the overall success percentage, total number of attempts, number of successful attempts, total delays, and the total failures for each of the stages based on the selected time range filter. To view the connection experience for each individual stage, select the stage type from the **Connectivity Summary** bar, the **Connection Experience** gets charted for the selected stage.

Figure 485 *Connection Experience Tile*



AI Insights

The **AI Insights** tile provides a list of AI Insights generated for a selected time range. To view the details, click on a selected **AI Insight**. The page gets redirected to the AI Insights under the **AI Insights** page. Click each of the listed AI Insight for a detailed analysis based on the impact on the network. For more information on AI Insights, see The AI Insights Dashboard.

NOTE

AI-Insights is not implemented for **Association** and **DNS**. AI Insights is not implemented at a Group level also. The page displays **No AI Insights observed**.

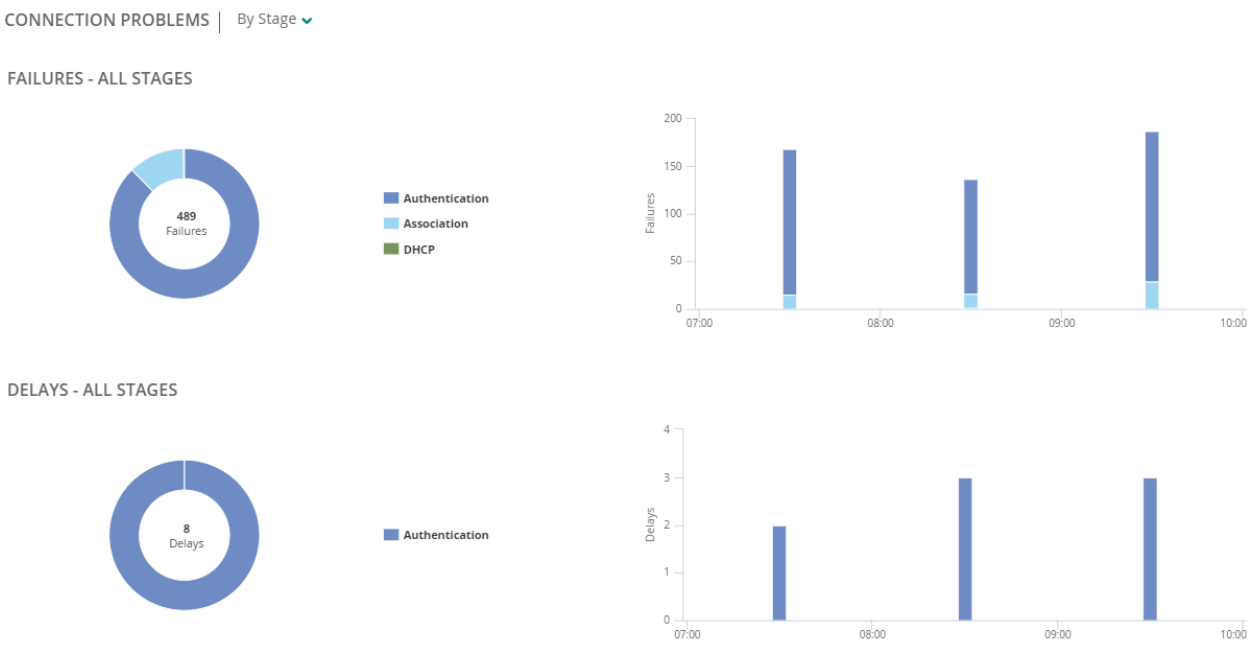
NOTE

For a visual representation of viewing an AI Insight, click here.

Connection Problems

The **Connection Problems** tile displays the details of **Failures** and **Delays** graphically for each of the categories from the drop-down list. Each graph displays the top five MAC addresses or SSID based on the selected category. Each category in the **Connection Problems** drop-down lists changes based on the selected stage in the **Connectivity Summary** bar. Selecting the required category from the drop-down displays the failures and delays in a pie chart with percentage, and a bar graph with the number of failures and delays. Hover the cursor over each graph to view the number of failures or delays for each stage.

Figure 486 *Connection Problems Tile*



The following table describes the information displayed in each connection category based on the selected stage:

Table 307: *Connection Problems Rolls-ups*

Data Pane Content	Description
All	Displays the details of the failures and delays that occurred during a client connection. The chart displays the failure details of Association, Authentication, and DHCP for each client. The Connection Problems drop-down list includes the following categories: ▪ **By Stage** ▪ **By Clients** ▪ **By Access Points** ▪ **By Band** ▪ **By SSID**
Association	Charts the details of the failures and delays that occurred during a client association. The **Connection Problems** drop-down list includes the following categories: ▪ **By Clients** ▪ **By Access Points** ▪ **By Band** ▪ **By SSID**

Data Pane Content	Description
	▪ **By Reason**
Authentication	Charts the details of the failures and delays that occurred during a client authentication. The **Connection Problems** drop-down list includes the following categories: ▪ **By Type** ▪ **By Clients** ▪ **By Access Points** ▪ **By Band** ▪ **By SSID** ▪ **By Server**
DHCP	Charts the details of the failures and delays that occurred during the attempts of DHCP requests and responses by a client. The **Connection Problems** drop-down list includes the following categories: ▪ **By Clients** ▪ **By Access Points** ▪ **By Reason**
DNS	Charts the details of the failures and delays that occurred during the attempts in detected DNS resolutions when a client is connected to the network. The **Connection Problems** drop-down list includes the following categories: ▪ **By Access Points** ▪ **By Reason** ▪ **By Server**

Connection Events

Connection Events table details out the list of delays and failures for each client based on the client MAC addresses. Click the List icon to view the connection events table. Click the **Connection Events** drop down to filter the events **By Clients** or **By Access Points**. The **Connection Events** table displays the following information:

Table 308: *Connection Events*

Data Pane Content	Description
MAC Address	Displays the MAC address of the client.
Name	Displays the name of the access point.
Delays	Displays the delays that occurred during the event.
Failures	Displays the failure details that occurred during the event.

Monitoring SaaS Express

The **SaaS Express** monitoring dashboards are used for viewing the SaaS-related information. It displays charts with Quality of Experience (QoE) scores for all the SaaS applications that are being monitored or optimized. Branch Gateways measure the network performance in terms of packet loss, latency, jitter, and

MOS, and sends that data to Aruba Central. Then, these Key Performance Indicators (KPI) and the Quality of Experience are displayed in Aruba Central. The QoE value is calculated based on the discrete data obtained in every measurement along with their trend. This allows Aruba Central to highlight how one-off events like sudden latency or packet loss spikes could be seen as a drop in performance. The insights gained from the monitoring dashboards identify applications that are not performing well and help correlate this information with the geographical region, the ISP, and so on to root-cause the potential problem.

To view the performance of the SaaS applications, you must have configured the required SaaS applications in the corresponding Branch Gateway groups. For more information, see Configuring SaaS Express .

You can monitor SaaS Express from the following dashboards:

- Global Dashboard
- Site Dashboard
- Gateway Dashboard

Global Dashboard

To view the SaaS Express monitoring dashboard for all sites in the Aruba Central account, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Manage**, click **Applications** > **SaaS Express**.
   By default, the map view of the Saas Express dashboard is displayed.
3. Click **List** to view details in a tabular format.

The following views are available in the Global dashboard:

- Map View
- List View

Map View

The map displays the sites with Branch Gateways in which SaaS Express is configured. The sites in which the QoE scores of all the SaaS applications are good are displayed in green. If one of them is fair or poor, the site is displayed in yellow or red, respectively. The default QoE scores are displayed at the bottom of the table along with the status color. You can view scores based on the performance of the applications only for the last three hours.

The QoE threshold values can be customized. The default QoE scores are classified as follows.

Table 309: *Status and Color for QoE Score*

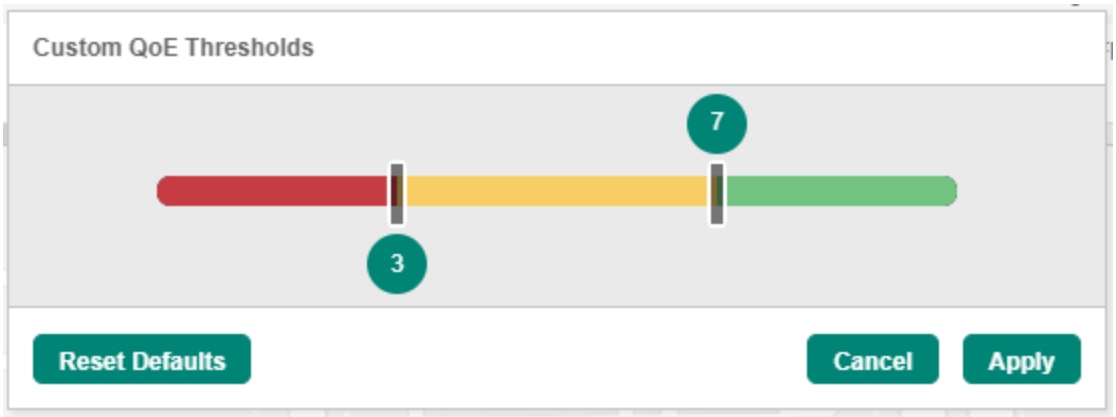
Application Status	Color	QoE score
Good	Green	7 to 10
Fair	Orange	3 to 7
Poor	Red	0 to 3

Customize QoE Thresholds

To customize the QoE threshold values:

1. In the **Application Health** section, click the Edit icon .
   The **Custom QoE Thresholds** pane is displayed.
2. Select and drag the bars left or right to increase or decrease the values.
3. Click **Apply**.
   The threshold values are successfully customized and displayed at the bottom of the table.
4. To reset to the default values, click **Reset Defaults**.

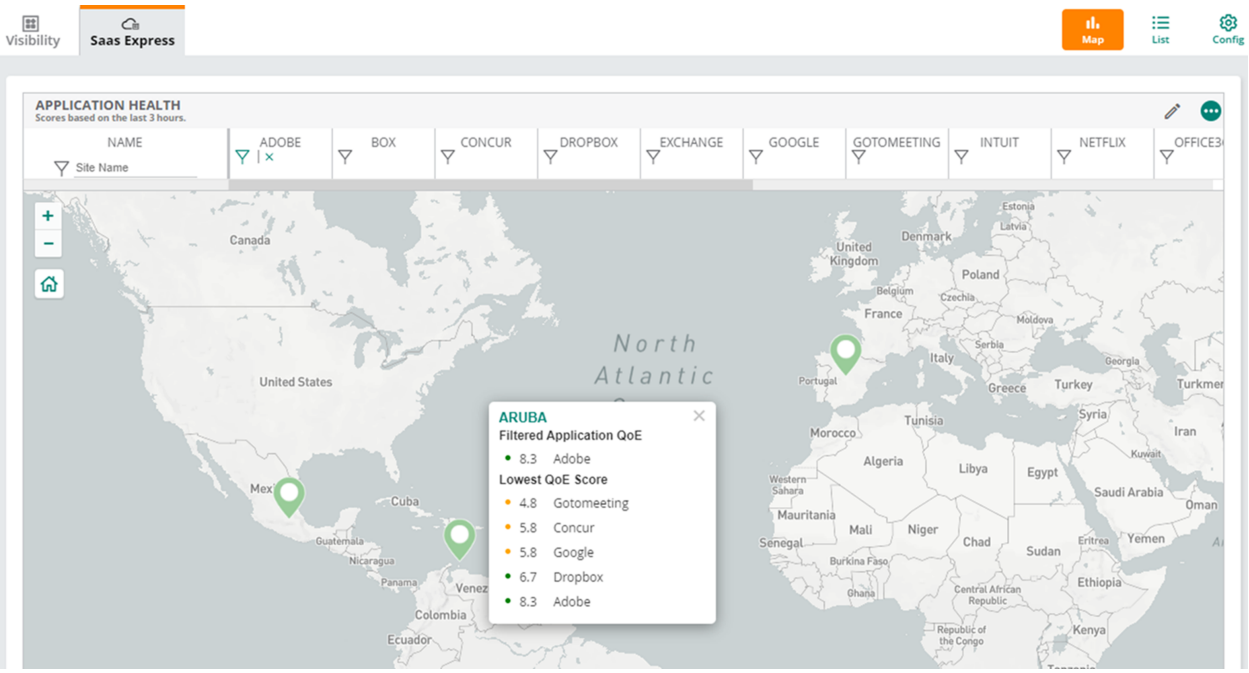
Figure 487 *Custom QoE Thresholds Pane*



The following actions are available in the map view:

- Click the **+** or **-** icons to zoom in or zoom out in the map view.
- Click the Home icon to reset the map view.
- Enter the site name in the **Name** column and click the icon to only view the details of the required site.
- Click the icon in the application name column to view sites where that particular application is running. To clear the selection, click the **x** icon.
- Click the pin (site) to view the site name and five applications with Lowest QoE Score in the pop-up dialog box. Click the site name to navigate to the site dashboard and view the details of all applications. For more information, see Site Dashboard.
- To view the QoE for a particular application on the site, click the icon in that application column. Then, click the pin (site) to view **Filtered Application QoE** in the pop-up dialog box.
- Click the Edit icon to customize the QoE thresholds.
- Click the ellipsis icon to select the required applications to be displayed in the table.

Figure 488 *Map View—SaaS Express Monitoring Dashboard*



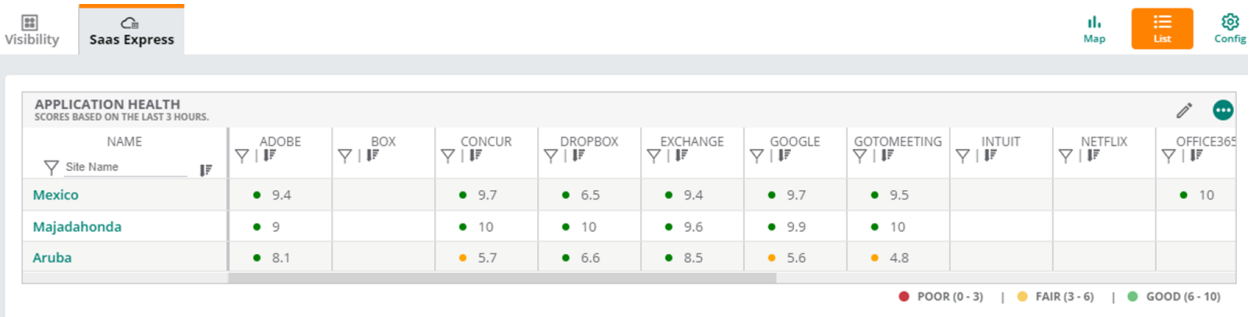
List View

The list view displays the **Application Health** table consisting of the QoE scores of all the sites for all the applications for the last three hours. The default QoE scores are displayed at the bottom of the table along with the status color.

The following actions are available in the list view:

- Enter the site name in the **Name** column and click the icon to only view the details of the required site.
- Click the Filter icon in the application name column and select the **Poor**, **Fair**, or **Good** option to view the corresponding score based on the selection. You can select multiple options.
- Click the and icons in the column to sort the list from **Good** to **Poor** or vice versa.
- Click the Edit icon to customize the QoE thresholds.
- Click the ellipsis icon to select the required applications to be displayed in the table.
- Click the site name in the **Name** column to navigate to the dashboard that displays Site-specific information. For more information, see Site Dashboard.

Figure 489 *List View—SaaS Express Monitoring Dashboard*



Site Dashboard

The details displayed in the site dashboard provide more granular insights into the performance of the SaaS applications.

To view the SaaS Express monitoring dashboard for a specific site, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
2. Under **Manage**, click **Applications** > **SaaS Express**.

   The **Saas Express** monitoring dashboard for that site is displayed.

The following sections are available in the Site dashboard:

- SaaS Express Summary
- SaaS Express Details

By default, the details displayed are for **3 Hours** time range. To change the time, click the **Time Range** filter and select the required option. The available options are:

- **3 Hours**
- **1 Day**
- **1 Week**
- **1 Month**
- **3 Months**

SaaS Express Summary

The **SaaS Express Summary** section displays the following information:

- **Total Apps**—The total number of active applications.
- **Categories Per Exit**—The total number of WAN interfaces for each application category.
- **Avg QoE**—An average of all the three scores: Loss, Latency, and Jitter.
- **Avg Loss**—The average percentage of packet loss during transmission.
- **Avg Latency**—The average time taken to transmit data packets to the destination in milliseconds.
- **Avg Jitter**—The average time delay or jitter in transmitting data packets over the network in milliseconds.

SaaS Express Details

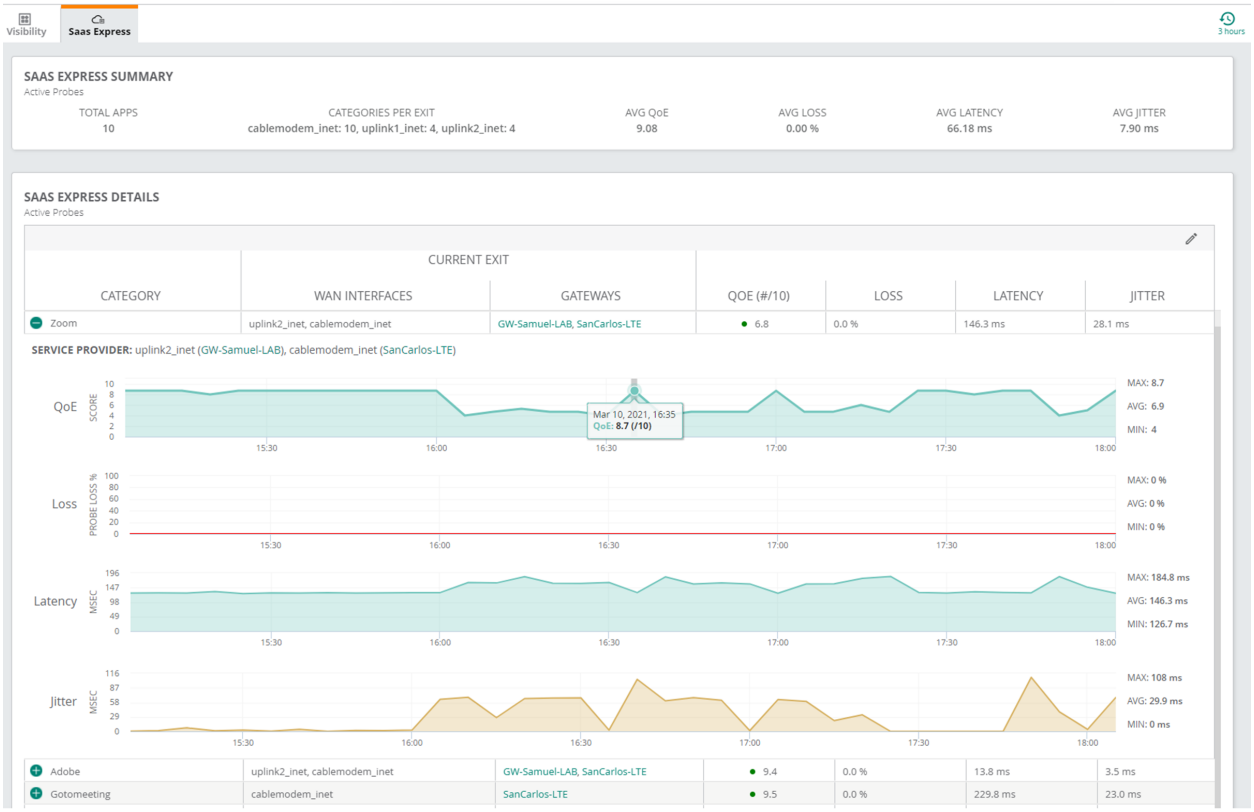
The **SaaS Express Details** table in this section displays the following information for each active SaaS application category:

- **Category**—The name of the SaaS application category.
- **Current Exit**
  - **WAN Interfaces**—The uplink through which the SaaS application traffic traverses.
  - **Gateways**—The Branch Gateway through which the SaaS application traffic traverses.
- **QoE (#/10)**—The average score (out of 10) based on the loss, latency, and jitter values.
- **Loss**—The percentage of packet loss during data transmission.
- **Latency**—The time taken to transmit data packets to the destination that is displayed in milliseconds.
- **Jitter**—The time delay or jitter in transmitting data packets over the network that is displayed in milliseconds.

The following actions are available:

- In the **SaaS Express Details** section, click the Edit icon to customize the QoE thresholds. For information about how to customize, see Customize QoE Thresholds.
- In the **Category** column, click **+** next to the category name to expand the graphical representation of the application performance. To collapse the graph, click **-**.
- Hover over the graph to view the values at a particular time of the day or the day of the week and so on, depending on the time range selected. The maximum, minimum, and average scores for each parameter for the selected time range are displayed next to the QoE, loss, latency, and jitter graph.

Figure 490 *Site View - SaaS Express Monitoring Dashboard*



Gateway Dashboard

The gateway dashboard provides additional information about the SaaS traffic traversing the gateways. The **Measured QoE** values (based on the synthetic probes to the SaaS front -doors) and the **Observed LAN/WAN QoE** values (based on inspecting TCP sessions as they traverse the gateway) can be analyzed. This allows the network administrator to correlate between what is being measured with what is being observed.

To view the SaaS Express monitoring dashboard for a specific gateway, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.

   A list of gateways is displayed in the **List** view.
3. Select the required gateway that is configured for SaaS Express.

   The dashboard context for the selected gateway is displayed.
4. Under **Manage**, click **Applications** > **SaaS Express**.

   The **Saas Express** monitoring dashboard for that gateway is displayed.

The following sections are available in the Gateway dashboard:

- SaaS Express Summary
- SaaS Express Details

By default, the details displayed are for **3 Hours** time range. To change the time, click the **Time Range** filter and select the required option. The available options are:

- **3 Hours**
- **1 Day**
- **1 Week**
- **1 Month**
- **3 Months**

SaaS Express Summary

The **SaaS Express Summary** section displays the following information:

- **Total Apps**—The total number of active applications.
- **Categories Per Exit**—The total number of WAN interfaces for each application category.
- **Avg QoE**—An average of all the three scores: Loss, Latency, and Jitter.
- **Avg Loss**—The average percentage of packet loss during transmission.
- **Avg Latency**—The average time taken to transmit data packets to the destination in milliseconds.
- **Avg Jitter**—The average time delay or jitter in transmitting data packets over the network in milliseconds.

SaaS Express Details

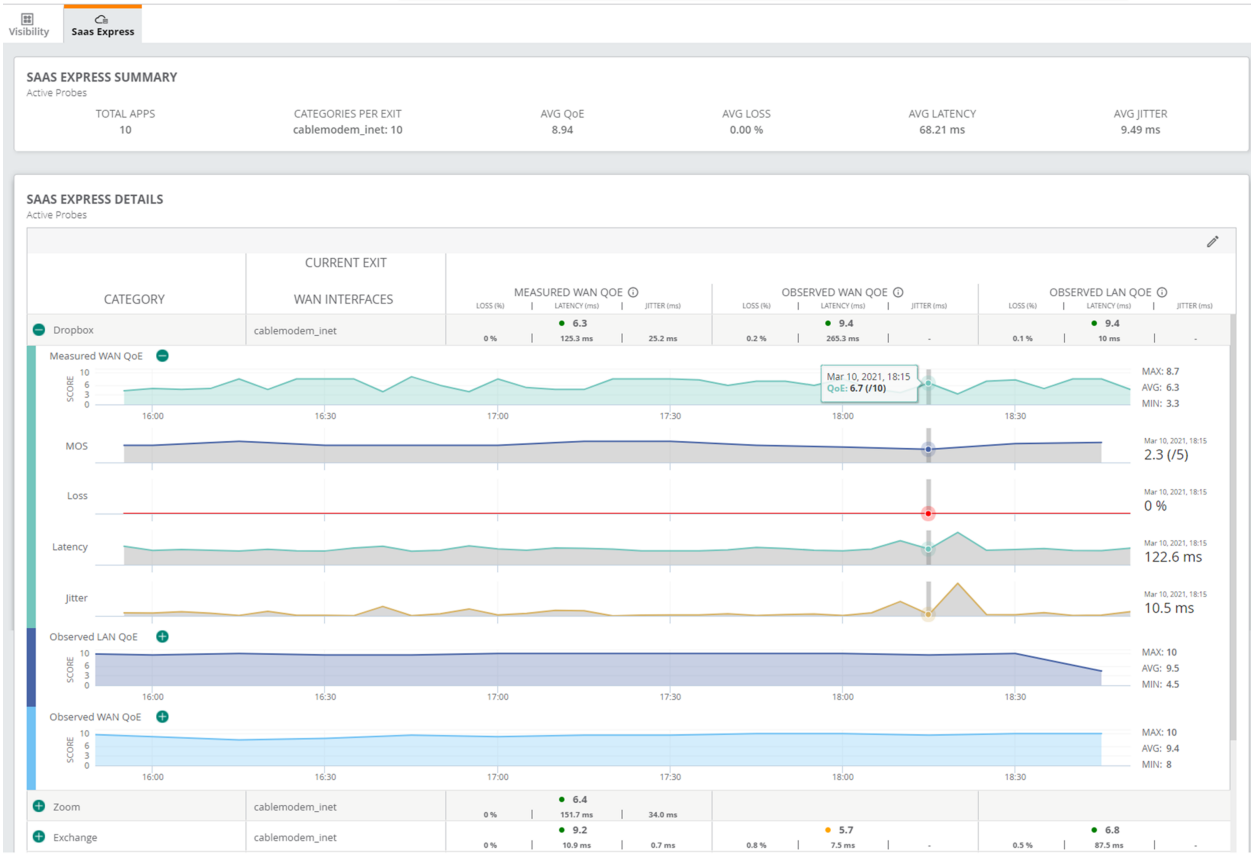
The table in this section displays the following information for each active SaaS application category:

- **Category**—The name of the SaaS application category.
- **Current Exit**
  - **WAN Interfaces**—The uplink through which the SaaS application traffic has traversed.
- **Measured WAN QOE**—The QoE score is based on the active probe and uplink application statistics. The **Loss**, **Latency**, and **Jitter** values are in milliseconds.
- **Observed LAN QOE**—The QoE score is based on analyzing the LAN segment of the communication as downlink SaaS traffic traverses the gateway. The **Loss** and **Round Trip Time (RTT)** values are in milliseconds.
- **Observed WAN QOE**—The QoE score is based on observing the WAN segment of the communication as uplink SaaS traffic traverses the gateway.

The following actions are available:

- In the **SaaS Express Details** section, click the Edit icon to customize the QoE thresholds. For information about how to customize, see Customize QoE Thresholds.
- In the **Category** column, click **+** next to the category name to expand the graphical representation of the application performance. To collapse the graph, click **-**.
  - Hover over the graph to view the values at a particular time of the day or the day of the week and so on, depending on the selected time range. The maximum, minimum, and average scores for each parameter for the selected time range are displayed next to the **Measured WAN QoE**, **Observed LAN QoE**, and **Observed WAN QoE** graphs.
- In the graphical representation, click **+** next to the **Measured** or **Observed QoE** to expand and view the **Mean Opinion Score (MOS)**, **Loss**, **Latency**, and **Jitter** values. To collapse the graph, click **-**.
  - Hover over the graph to view the values at a particular time of the day or the day of the week and so on, depending on the time range selected. The maximum, minimum, and average scores for each parameter for the selected time range are also displayed.

Figure 491 *Gateway—SaaS Express Monitoring Dashboard*



Monitoring Sites in the Topology Tab

In Aruba Central, the **Topology** tab in the site dashboard provides a graphical representation of the site including the network layout, details of the devices deployed, and the health of the WAN uplinks and tunnels.

The Topology feature is available for Foundation and Advanced licenses for APs, switches, and gateways.

This section includes the following topics:

- Before You Begin
- Viewing the Topology Tab
  - Parts of the Topology Tab User Interface
  - Pop-Up Details
  - Details Pane
  - Unreachable Devices
  - VLAN Overlay Details

Before You Begin

The following types of devices are displayed as part of the **Topology** tab:

- Access Point (AP)
- Gateway

- Switch—AOS-Switch, AOS-CX switch
- Stack—AOS-Switch stack, AOS-CX VSF stack
- AOS-CX VSX Switch

In the topology map, Aruba Central only supports third-party routers, switches, gateways, and APs from the vendors listed below:

- Cisco
- Procurve
- Juniper
- HPE Comware
- Meraki
- Cumulus
- Huawei
- Mikrotik
- Extreme
- HPE OfficeConnect Switch
- Arista
- 3Com
- Ruckus
- Mojo
- Mist
- Motorola
- Netgear
- Dell
- Comware
- Hirschmann Railswitch
- Ubiquiti

This section discusses the pre-requisites associated with the devices so that they are displayed correctly in the **Topology** tab:

- The topology map filters devices based on sites. To view the topology map, ensure that you have assigned the devices to sites.
- The minimum required ArubaOS version for access points (APs) and gateways in the topology map is ArubaOS version 8.1.0.0-1.0.1.1.
- To view the topology map, ensure that LLDP is enabled. On switches, LLDP is enabled by default. On Branch Gateways, if the port type is LAN, LLDP is enabled by default.
- To view AOS-CX switches in the topology map, you must create a template configuration for the switch with the password in plaintext.

The guidelines for grouping VPNCs are:

- If the tunnels in the overlay are orchestrated, the VPNCs are grouped according to their hub groups. You can also see the group preference order marked as primary, secondary, or tertiary.

- If the tunnels are configured manually, the VPNCs are grouped according to their sites. If the VPNCs are not associated with any site, they are grouped based on their hub groups. For manual tunnels, the Data Center group preference is not displayed.
- If you have a combination of gateways in a single site, with one gateway configured as a manual tunnel and the other gateway configured as an orchestrated tunnel, both the tunnels are treated as manual and the VPNCs are grouped based on their sites. If there are no associated sites, they are grouped according to their hub groups.

NOTE

Do not install VPNCs with orchestrated tunnels and VPNCs with manual tunnels together in a single site.

Viewing the Topology Tab

To view the topology tab, complete the following steps:

1. In the **Network Operations** app, set the filter to a site for which you want to view the topology map.

   The dashboard context for the site is displayed.
2. Under **Manage**, click **Overview** > **Topology**.

   The Topology map for the selected site is displayed.
3. In the topology map, hover over a device or a link to view the pop-up details. For more information, see Pop-Up Details.
4. In the device or the link pop-up, click the **Show Details** link to view the corresponding **Details** pane. For more information, see Details Pane .

Parts of the Topology Tab User Interface

In the topology tab, the icons provides the following functionality:

Figure 492 *Parts of the Topology Tab*

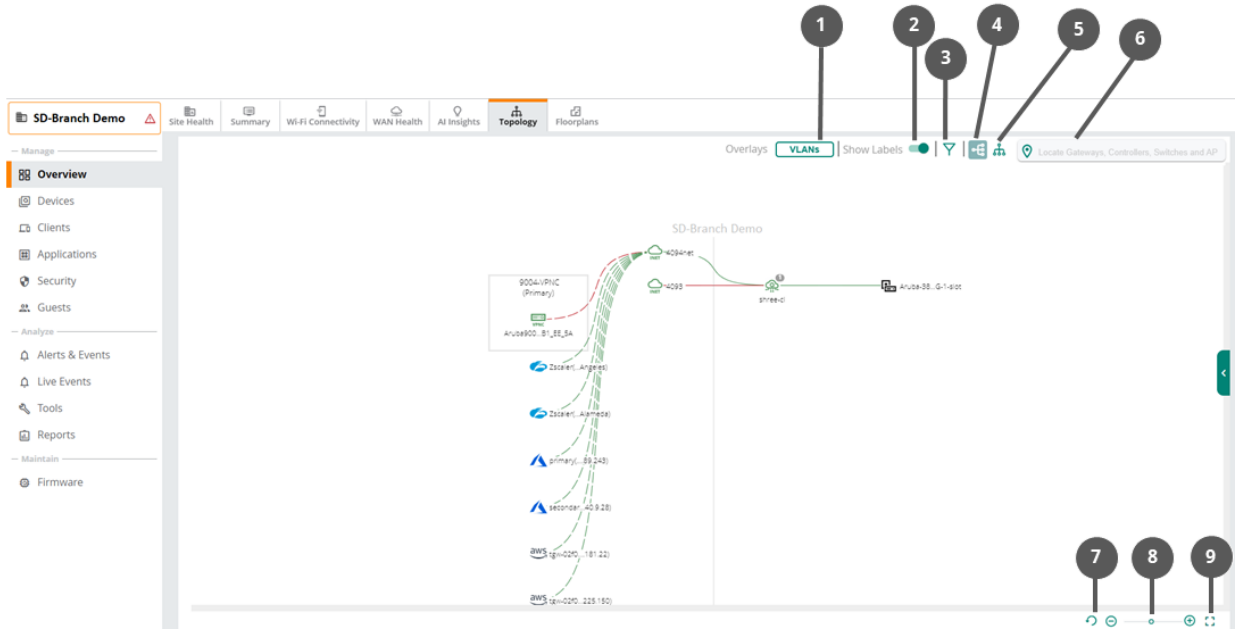


Table 310: *Icon Details*

Callout Number	Description
1	Click the icon to show or hide the **VLANs** pane.
2	Set the toggle icon to show or hide the labels.
3	Click the icon to filter the type of devices to be shown on the map. The following options are available: ■ **Access Points**—Allows you to show or hide the APs from the topology map. ■ **Security Cloud**—Allows you to show or hide the Zscaler and Palo Alto Prisma Access™ Cloud Service from the topology map. ■ **Switch**—Allows you to show or hide the switches from the topology map. ■ **VPNC**—Allows you to show or hide the VPNCs and the virtual gateways from the topology map. ■ **Unmanaged**—Allows you to show or hide the unmanaged devices from the topology map. ■ **Show Devices Without Link**—Allows you to show or hide the devices without link from the topology map.
4	Click the icon to view the topology map in a left to right orientation. The default orientation of the topology map is left to right orientation.
5	Click the icon to view the topology map in a top to down orientation.
6	The search bar allows you to locate a device in the topology map. The search bar field supports exact and partial text search.
7	Click the icon to reset the topology map to the default view.
8	Click the icons to change the zoom level of the topology map. Alternatively, you can drag the slider to set the zoom level of the topology map.
9	Click the icon to view the topology map in full-screen view. In the full-screen view, the pop-up details feature is disabled in the topology map.

When the number of downstream devices connected to a device is less than or equal to 10, the devices are visible in the topology map. When the number of downstream devices connected to a device is more than 10, click the device icon to view the devices in the topology map. A bubble icon on the device represents the number of connected downstream devices.

Table 311: *Icon Types*

Icon	Type
	AP
	Branch Gateway
	Switch

Icon	Type
	Switch Stack
	Unmanaged Device
	Uplink
	VPNC
	Third-party Zscaler VPNC
	Third-party Azure VPNC
	Third-party AWS VPNC

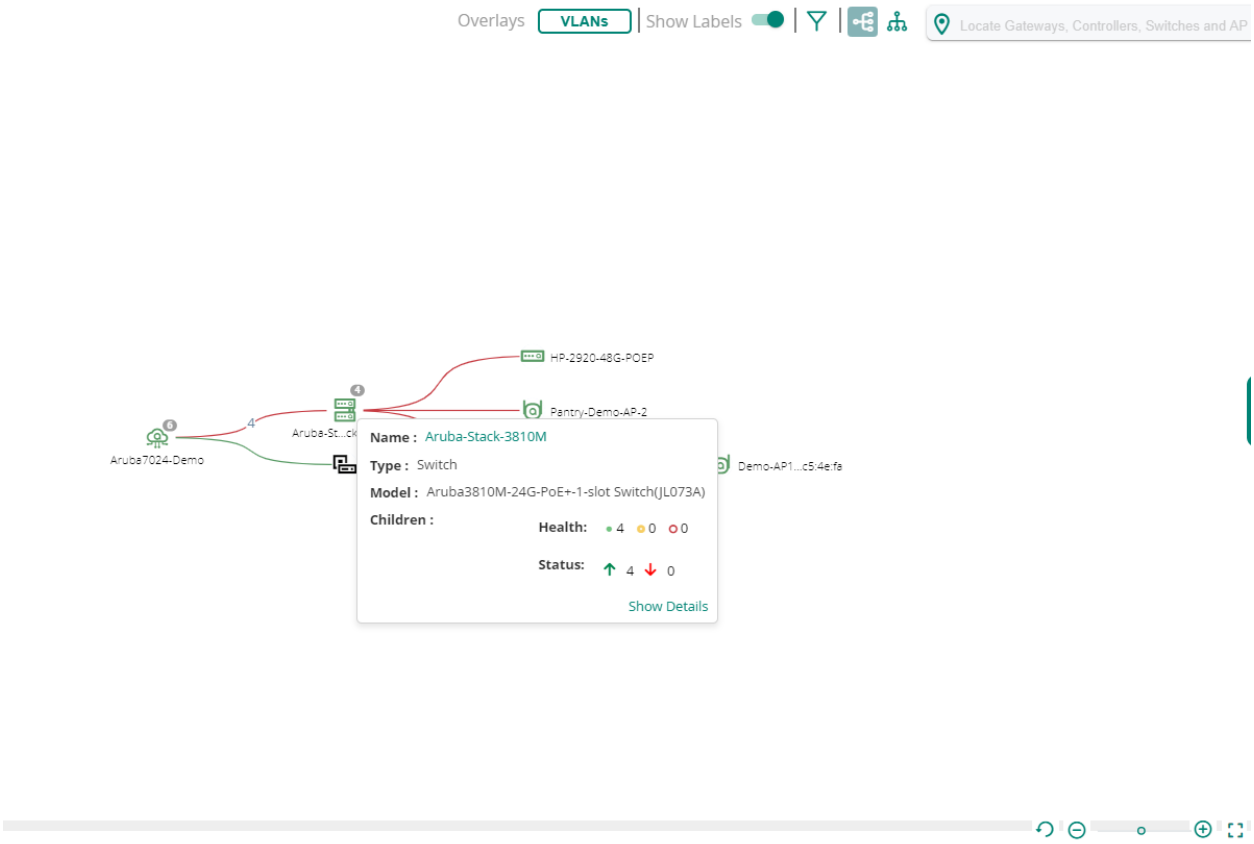
Icon Status

- —Indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
- —Indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%.
- —Indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%.
- —Indicates that the device is online.
- —Indicates that the device is offline.

Pop-Up Details

When you hover over a device or link, a pop-up displays the following details:

Figure 493 *Pop-Up Details*



- Access Point—Displays the following details:
  - **Name**—Hostname of the AP.
  - **Type**—Type of the device.
  - **Model**—Hardware model of the AP.
  - **Health Reason**—The health status of the AP. This parameter is only available when the AP is offline.
  - **Show Details**—Click the link to view the **Details** pane.
- Branch Gateway—Displays the following details:
  - **Name**—Hostname of the Branch Gateway.
  - **Type**—Type of device deployment.
  - **Model**—Hardware model of the device.
  - **Children**—Number of devices connected to the Branch Gateway categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the Branch Gateway based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
    - **Status**—Count of devices connected to the Branch Gateway based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.

- **Show Details**—Click the link to view the **Details** pane.

- VPNC—Displays the following details:
  - **Name**—Hostname of the VPNC.
  - **Type**—Type of device deployment.
  - **Model**—Hardware model of the device.
  - **Show Details**—Click the link to view the **Details** pane.
- Unmanaged—Displays the following details:
  - **Name**—Name of the unmanaged device.
  - **IP Address**—IP address of the unmanaged device.
  - **Show Details**—Click the link to view the **Details** pane.

The value of the **IP Address** parameter is empty if LLDP does not provide the neighbor information.

- Switch—Displays the following details:
  - **Name**—Hostname of the switch.
  - **Type**—Type of the device.
  - **Model**—Hardware model of the switch.
  - **Children**—Number of devices connected to the switch categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the switch based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
    - **Status**—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.
  - **VLANs**—List of VLANs configured on the switch. This field is displayed only when the **VLANs** option is selected under **Overlays**. For more information, see VLAN Overlay Details.
  - **Show Details**—Click the link to view the **Details** pane.
- Switch Stack—Displays the following details:
  - **Name**—Hostname of the switch stack.
  - **Type**—Type of the device.
  - **Model**—Hardware model of the switch.
  - **Children**—Number of devices connected to the switch categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the switch based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.

- **Status**—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.

◦ **VLANs**—List of VLANs configured on the switch. This field is displayed only when the **VLANs** option is selected under **Overlays**. For more information, see VLAN Overlay Details.

◦ **Show Details**—Click the link to view the **Details** pane.

- AOS-CX VSX Switch—Displays the following details:
  - **Name**—Name of the AOS-CX switch that is configured with VSX. The name is displayed in the **VSX_<Device Name>** format. For example, **VSX_8320-switch-primary**. However, in the map, this name is displayed in the **VSX_<first four characters of device name>...<last eight characters of device name>** format. For example, **VSX_8320...-primary**.
  - **Type**—Type of the device.
  - **Model**—Hardware model of the AOS-CX switch.
  - **VSX Role**—Role of the AOS-CX switch in the VSX configuration. Supported values are **Primary** and **Secondary**.
  - **Children**—Number of devices connected to the switch categorized based on the health and status of the devices. The **Children** field displays the following details:
    - **Health**—Count of devices connected to the switch based on the health of the device. A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%.
    - **Status**—Count of devices connected to the switch based on the current status of the devices. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.
  - **VLANs**—List of VLANs configured on the switch. This field is displayed only when the **VLANs** option is selected under **Overlays**. For more information, see VLAN Overlay Details.
  - **Show Details**—Click the link to view the **Details** pane.
- Tunnel—Displays the alias map name of the tunnel configured on the Branch Gateway.

  In the topology map, the tunnels are shown as dotted lines. The tunnel in green color indicates that the tunnel is up. The tunnel in red color indicates that the tunnel is down.

  Click the tunnel link to view the **Details** pane.

In case of High Availability, the redundant gateway tunnel details are also displayed in the **Details** tab under **Virtual Tunnels** when you select the tunnel.

- Uplink—Displays the following information about uplinks configured on the Branch Gateway:
  - **<Name of the Branch Gateway>**—Displays the name of the Branch Gateway.
  - **Uplink**—Type of the uplink.
  - **VLAN**—VLAN ID of the uplink.
  - **Health Reason**—Displays the health status of the uplink. This parameter is only available when the uplink is down. The uplink in green color indicates that the uplink is up. The uplink in red color indicates that the uplink is down.

  Click the uplink to view the **Details** pane.

NOTE

In case of High Availability, the redundant gateway tunnel details are also displayed in the **Details** tab under **Virtual Tunnels** when you select the uplink.

- Edge—Displays the following information about the link:
  - **<Name of the connected device>**—Name of the device connected with the edge link.
  - **<Interface number>**—Interface number of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Alternative links**—Number of the alternative links.

  The edge in green color indicates that the edge is up. The edge in red color indicates that the edge is down.

  Click the uplink to view the **Details** pane.
- Unmanaged edge—Displays the following information about the link:
  - **<Name of the connected device>**—Name of the device connected with the edge link.
  - **<Port Identifier>**—Port number of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Alternative links**—Number of the alternative links.

  The unmanaged edge in green color indicates that the unmanaged edge is up. The unmanaged edge in red color indicates that the unmanaged edge is down.

  Click the unmanaged edge link to view the **Details** pane.
- ISL edge in AOS-CX VSX toplogy map—Displays the following information about the link:
  - **ISL**—Number of inter-switch link (ISL) present between the AOS-CX switches configured with VSX
  - **Other Links**—Number of other links present between the AOS-CX switches configured with VSX.
  - **<Name of the connected device>**—Name of the device connected with the edge link.
  - **<Interface name>**—Interface name where the switches are connected to the devices.

NOTE

Active tunnels are green in color and inactive tunnels are red in color. If there are multiple tunnels connecting to a VPNCs, and even if one of those tunnels is down, the tunnel mapping is displayed in red dotted lines.

Details Pane

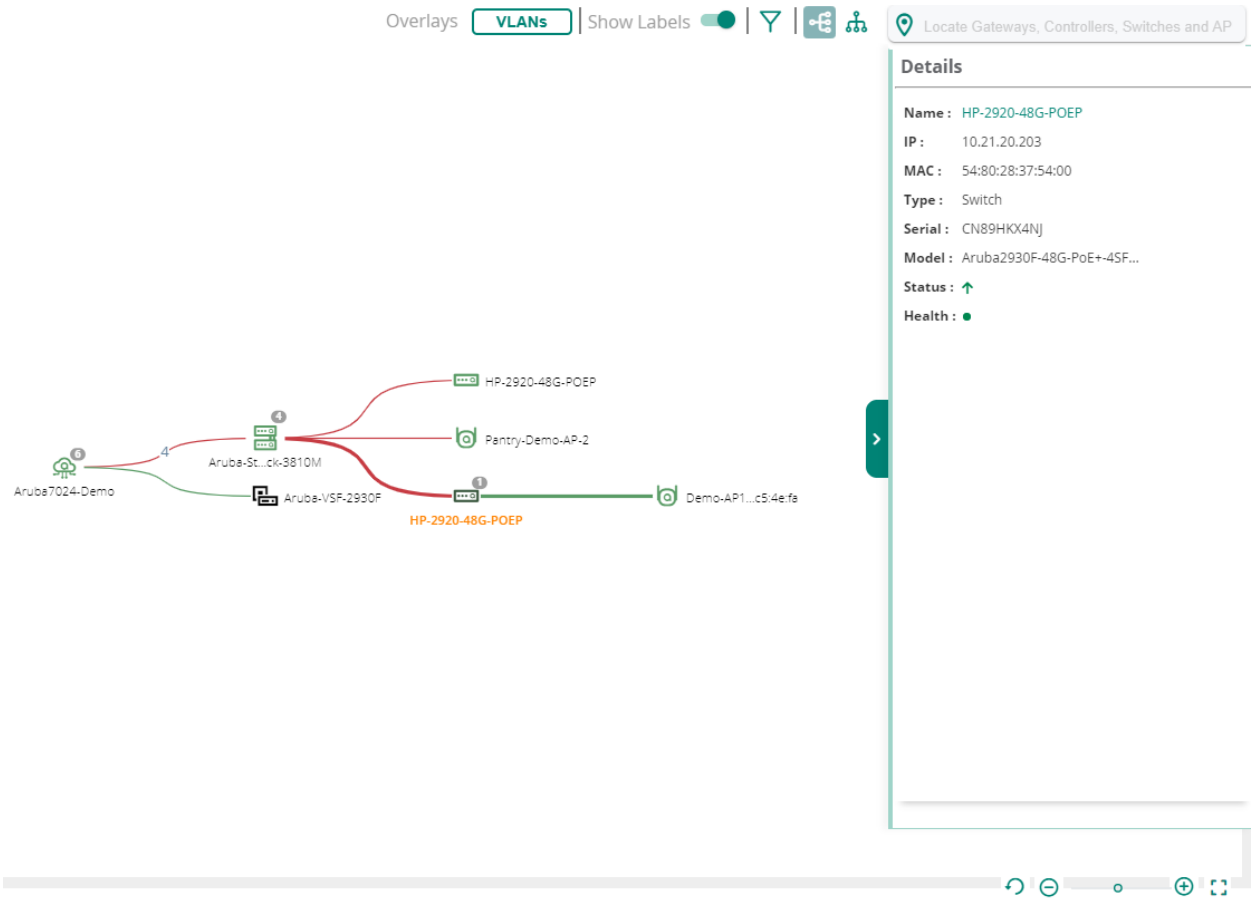
In the topology map, the **Details** pane provides a summary of the devices, uplinks, and tunnel details.

A green bullet icon indicates that the device health is good when the CPU usage is lower than or equal to 75% and the memory usage is lower than or equal to 75%. A yellow bullet icon indicates that the device health is fair when the CPU usage is greater than 75% and the memory usage is greater than 75%. A red bullet icon indicates that the device health is poor when the CPU usage is greater than 90% and the memory usage is greater than 90%. The arrow in green indicates that the device is online. The arrow in red indicates that the device is offline.

In the topology map, select a device and then click the **Show Details** link in the pop-up window to view the **Details** pane. To view the **Details** pane for a tunnel, uplink, or edge, click the link.

The **Details** task pane displays the following information:

Figure 494 *Details Pane*



- Access Point—Displays the following details:
  - **Name**—Hostname of the AP. Click the AP name to view the **Access Point Details** page.
  - **IP**—IP address of the AP.
  - **MAC**—MAC address of the AP.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the AP.
  - **Model**—Hardware model of the AP.
  - **Status**—Operational status of the AP.
  - **Health**—Operational health of the AP.
- Branch Gateway—Displays the following details:
  - **Name**—Hostname of the Branch Gateway. Click the Branch Gateway name to view the **Gateway Details** page.
  - **IP**—IP address of the Branch Gateway.
  - **MAC**—MAC address of the device.
  - **Type**—Type of device deployment.
  - **Serial**—Serial number of the Branch Gateway.
  - **Model**—Hardware model of the device.

- **Status**—Operational status of the device.
- **Health**—Operational health of the device.

- VPNC—Displays the following details:
  - **Name**—Hostname of the VPNC. Click the VPNC name to view the **Gateway Details** page.
  - **IP**—IP address of the VPNC.
  - **MAC**—MAC address of the device.
  - **Type**—Type of device deployment.
  - **Serial**—Serial number of the VPNC.
  - **Model**—Hardware model of the device.
  - **Status**—Operational status of the device.
  - **Health**—Operational health of the device.
- Unmanaged—Displays the following details:
  - **Name**—Name of the unmanaged device.
  - **Description**—Description of the unmanaged device.
  - **IP**—IP address of the unmanaged device.
  - **Capabilities**—Displays the capabilities of the unmanaged device.
    - **Supported**—Lists the supported capabilities of the unmanaged device.
    - **Enabled**—Lists the enabled capabilities of the unmanaged device.

The value of the parameters are empty if LLDP does not provide the neighbor information.

- Switch—Displays the following details:
  - **Name**—Hostname of the switch. Click the switch name to view the **Switch Details** page.
  - **IP**—IP address of the switch.
  - **MAC**—MAC address of the switch.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the switch.
  - **Model**—Hardware model of the switch.
  - **Status**—Operational status of the switch.
  - **Health**—Operational health of the switch.
- Switch Stack—Displays the following details:
  - **Name**—Hostname of the switch. Click the switch name to view the **Switch Details** page.
  - **IP**—IP address of the switch.
  - **MAC**—MAC address of the switch.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the switch.
  - **Stack Role**—Role of the switch in the stack.
  - **Model**—Hardware model of the switch.
  - **Status**—Operational status of the switch.
  - **Health**—Operational health of the switch.
  - **Stack Members**—Provides the **Name**, **Role**, and **State** details of the stack member. Click the stack member name to view the **Switch Details** page.

- AOS-CX VSX—Displays the following details:
  - **Name**—Hostname of the AOS-CX switch with VSX configured. Click the switch name to view the **Switch Details** page.
  - **IP**—IP address of the switch.
  - **MAC**—MAC address of the switch.
  - **Type**—Type of the device.
  - **Serial**—Serial number of the switch.
  - **Model**—Hardware model of the switch.
  - **Status**—Operational status of the switch.
  - **Health**—Operational health of the switch.

  The **VSX** section displays the following details:
  - **ISL State**—State of the ISL connection with the peer AOS-CX switch. Following are the supported values:
    - **WAITING_FOR_PEER**—Waiting for connectivity to the peer.
    - **PEER_ESTABLISHED**—Steady state. VSX LAGs are up when the device is in this state.
    - **SPLIT_SYSTEM_PRIMARY**—Lost ISL connectivity to the peer and the device is operating as primary.
    - **SPLIT_SYSTEM_SECONDARY**—Lost ISL connectivity to the peer and the device is operating as secondary.
    - **SYNC_PRIMARY**—ISL connectivity to the peer restored and the device is syncing states to the peer.
    - **SYNC_SECONDARY**—ISL connectivity to the peer restored and he device is learning states from the peer. VSX LAGs are down when the device is in this state.
    - **SYNC_SECONDARY_LINKUP_DELAY**—Device has learned its states from the peer and monitoring for hardware is to be programmed. VSX LAGs are down when the device is in this state.
  - **ISL Port**—ISL port number of the selected AOS-CX switch. If the ISL is a LAG, then this field displays the LAG name.
  - **ISL Mgmt State**—Management state of the ISL. Following are the supported values:
    - **OPERATIONAL**—ISL management is operational.
    - **INTER_SWITCH_LINK_MGMT_INIT**—ISL management is in initialization state.
    - **CONFLICTING_OR_MISSING_DEVICE_ROLES**—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers.
    - **SW_IMAGE_VERSION_MISMATCH_ERROR**—Software version on the primary device does not match with the software version on the secondary device.
    - **INTER_SWITCH_LINK_DOWN**—ISL is down.
    - **INTERNAL_ERROR**—ISL management has internal errors.
  - **Config Sync Enabled**—Configuration synchronization between the VSX switches are enabled or disabled.
  - **Config Sync Status**—Status of the configuration synchronization between the VSX switches. Following are the supported values:
    - **IN-SYNC**—Configuration synchronization is operational and the VSX switches are in sync.
    - **DISABLED**—Configuration synchronization is disabled.

- **SW_IMAGE_VERSION_MISMATCH_ERROR**—Software image version on the primary device does not match with the software image version on the secondary device.
- **CONFLICTING_OR_MISSING_DEVICE_ROLES**—Either the role is missing on one of the VSX peers or the same role is configured on both VSX peers.
- **PEER_DB_CONNECTION_ERROR**—Error in connecting to peer database. It involves errors due to ISL or ISL management.
- **CONFIGURATION_SYNC_CONFLICT**—Configuration synchronization is operational, but has conflicts synchronizing the configuration. Conflicts can occur if the configuration on the primary device is marked for sync, but the same configuration on the secondary device is not marked for sync.
- **CONFIGURATION_SYNC_MISSING_REFERENCE**—Configuration synchronization is operational, but has missing references in synchronizing the configuration.

◦ **Role**—Role of the AOS-CX switch in the VSX configuration. Supported values are **Primary** and **Secondary**.
◦ **Peer IP**—IPv4 address of the peer switch.
◦ **Peer Serial**—Serial number of the peer switch.
◦ **Peer MAC**—MAC address of the peer switch.
◦ **Peer Name**—Hostname of the peer switch.
◦ **Last Seen**—Date on which the peer switch was last synced.

- Tunnel—Displays the following information about tunnels configured on the Branch Gateway:
  ◦ **Map Name**—Name of the tunnel interface.
  ◦ **Peer MAC**—MAC address of the peer device with which the tunnel was established.
  ◦ **Local MAC**—MAC address of the Branch Gateway.
  ◦ **Source IP**—Source IP address from where the traffic originates.
  ◦ **Destination IP**—IP address to which the traffic is sent.
  ◦ **Established Time**—Timestamp showing when the tunnel was established.
  ◦ **VLAN**—VLAN ID of the tunnel.
  ◦ **Source Serial**—Source Serial of the tunnel.

  The tunnel in green color indicates that the tunnel is up. The tunnel in red color indicates that the tunnel is down.
- Uplink—Displays the following information about uplinks configured on the Branch Gateway:
  ◦ **Uplink Type**—Type of the uplink.
  ◦ **VLAN**—VLAN ID of the uplink.
  ◦ **Link Status**—Uplink status.
  ◦ **Description**—Description of the uplink.
  ◦ **WAN Status**—WAN status.
  ◦ **IP Address**—IP address of the WAN interface.
  ◦ **Public IP Address**—Public IP address.
  ◦ **Device MAC**—MAC address of the device.
  ◦ **Serial**—Serial number of the device.
  ◦ **Port Number**—Port number of the device.
  ◦ **Tunnels**—Displays a list of tunnels mapped to the uplink. Click the drop-down on each tunnel to view the tunnel details.

The uplink in green color indicates that the uplink is up. The uplink in red color indicates that the uplink is down.

- Edge—Displays the following information about the link:
  - **Interface numbers**—Interface numbers of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Interface**—Interface number of the device.
  - **Serial**—Serial number of the device.
  - **Device Name**—Name of the device.
  - **Port Number**—Port number of the device.

In case of Branch Office Controller (BOC) to Switch link, if a peer Branch Gateway link is configured for redundancy, link details are displayed for the peer Branch Gateway to switch link as well.

- Unmanaged edge—Displays the following information about all the links:
  - **Interface numbers**—Interface numbers of the device.
  - **Health Reason**—Displays the health status of the edge link. This parameter is only available when the edge link is down.
  - **Interface**—Interface number of the device.
  - **Serial**—Serial number of the device.
  - **Device Name**—Name of the device.
  - **Port Number**—Port number of the device.
  - **Interface**—Interface number of the unmanaged device.
  - **MAC**—MAC address of the unmanaged device.
  - **Device Name**—Name of the unmanaged device.
  - **Port Identifier**—Displays the port ID, port name, or MAC address of the unmanaged device.
- ISL edge in AOS-CX VSX toplogy map—Displays the following information about the ISL edge:
  - **Inter-Switch Link Status**—Status of the ISL connection with the peer.
  - ***<LAG-name>* - ISL** section displays details about all the interfaces that are part of the LAG. This section also displays the details of the devices connected to these interfaces. It displays the following details:
    - **Serial**—Serial number of the individual device.
    - **Device Name**—Name of the individual device.
    - **Port Number**—Port number of the individual device.
  - **Other**—This section displays details about the other links present between the VSX configured AOS-CX switches. It displays the following details:
    - **Serial**—Serial number of the individual device.
    - **Device Name**—Name of the individual device.
    - **Port Number**—Port number of the individual device.

Unreachable Devices

The **Unreachable Devices** pane provides information about the orphan and the offline unmanaged devices. An unmanaged device is considered to be orphan when all its neighboring Aruba devices get deleted and are only displayed in the **Unreachable Devices** list. An unmanaged device is considered to be offline

when all its neighboring Aruba devices are offline and are displayed both in the **Topology** map and in the **Unreachable Devices** list.

When an unmanaged device is either offline or disconnected, they are only displayed in the **Unreachable Devices** list. The devices listed in the **Unreachable Devices** pane are deleted after 15 days.

To view the **Unreachable Devices** pane, click the **Unreachable Devices** button. The **Unreachable Devices** pane displays the following details:

- **Name**—Name of the unmanaged device.
- **Type**—Type of the unreachable device.
- **MAC**—MAC address of the unmanaged device.
- **Last Seen**—The last active time and date of the unmanaged device.

VLAN Overlay Details

The topology map displays information about the VLANs configured on switches running AOS-Switch and AOS-CX software. To view the VLAN information:

1. Select the **VLANs** option under **Overlays**. The **VLANs** pane is displayed and the network elements in the topology map, such as device icons and edge links, are grayed out.

   The **VLANs** pane displays the first 50 VLANs (unique VLAN ID and name pairs) in the ascending order of VLAN IDs. To search for other VLANs, click the search icon.
2. Select a VLAN from the **VLANs** pane. You can also enter a VLAN name or ID in the search box.
3. The topology map displays the following information:
   - The switches that have the selected VLANs configured are highlighted in a color depending on the status of the switch, green for online and red for offline.
   - The edge link connecting two switches is highlighted in blue, if the following conditions are met:
     - The VLAN IDs are present in both the switches and in the ports associated with the edge link between the switches.
     - The VLAN type (tagged or untagged) configured is the same in both the switches.
4. Hover over the switch to view the list of all VLANs (comma separated) configured on the switch.

   The VLAN IDs are also listed as a range if consecutive VLAN IDs are configured. For example, 100-178, 190, 210.
5. Hover over the edge link connecting the two switches. The pop-up displays the following information:
   - Host name of the switch
   - Serial number of the switch
   - VLAN ID
   - Type of VLAN: **tagged**, **untagged**, or **missing**

Gateway Firewall Logging

The **Firewall** dashboard monitors incoming and outgoing traffic in an Aruba Central-managed network and acts as an investigative resource for users to track blocked sessions within the network. The **Firewall** dashboard provides a detailed summary of all blocked sessions on the gateway, aggregated based on source IP, destination IP, destination port, and protocol. It also logs the blocked sessions which are sent from the gateways connected in the network. It enables you to audit, verify, and analyze the effects of your firewall rules. You can also analyze the sessions by using the chart displayed in the **Blocked Sessions** pane.

The **Firewall** tab is available in the **Global** and **Gateway** dashboards. The historical firewall activity is available only for the **3 hours, 1 day, and 1 week** time range.

Although the firewall logging feature works from Aruba Central version 2.5.2 with minimum image version of ArubaOS 8.6.0.4-2.2.0.0, from Aruba Central 2.5.3 release onwards, Aruba recommends that you upgrade your branch gateways to a recommended image version of ArubaOS 8.7.0.0-2.3.0.0 to benefit from the new features and enhancements.

Enabling Firewall Visibility on Gateways

To view the graphs on the **Blocked Sessions** pane, the **Firewall Visibility** service must be enabled. To enable the **Firewall Visibility** service, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a Branch Gateway group in the filter:
     a. Set the filter to a group. The dashboard context for a group is displayed.
     b. Under **Manage**, click **Devices > Gateways**.
     The dashboard context for the gateway is displayed.
   - To select a Branch Gateway in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices > Gateways**.
     A list of gateways is displayed in the **List** view.
     c. Click a gateway under **Device Name**.
     The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device > Gateway**.
2. Click the **Config** icon. The gateway configuration page is displayed.
3. Click **Advanced Mode**.
4. Click **Security > Applications**. The **Applications** page is displayed.
5. In the **Applications** page, click **Application Visibility** and select the **Firewall visibility** check box to enable the service.
6. Click **Save Settings**.

Firewall Dashboard

The **Global > Security > Firewall > Blocked Sessions** dashboard provides graphical and tabular representation of all the session activities belonging to gateways managed by Aruba Central:

- Graphical view displays a bar graph that represents the session activities of a gateway over time.
- Tabular view represents the in-session activities of a gateway in detail.

The complete session information is summarized at the gateway level and then enriched at Aruba Central before displaying it on the dashboard. Additional details such as client, associated network segment, application details including application category, and policy information are displayed. All session activities are scoped by time and space. From a time perspective, the dashboard displays session activities covering up to 3 hours, 1 day and 1 week of historical data. The **Firewall** tab is only applicable to the **Global** and **Gateway** dashboards.

Session entries that are denied access are displayed in the dashboard to help network administrators understand the reason for a session being denied or blocked due to a policy.

A session can be blocked because one or more of the following policies are configured or enabled:

- IP reputation
- Geographical location-based policies
- Application reputation
- Application classification
- Content in the web site or application
- Missed classifications and the traditional network
- Session and network access control lists

To view blocked session details, ensure that at least one of the configuration settings such as roles, policies, ACLs, DPI, WebCC, IP reputation, or geolocation are configured on the gateway.
For more information, see Creating a Role, Configuring Firewall Policies and ACLs, Filtering URLs Based on Website Content and Reputation, and Using Deep Packet Inspection.

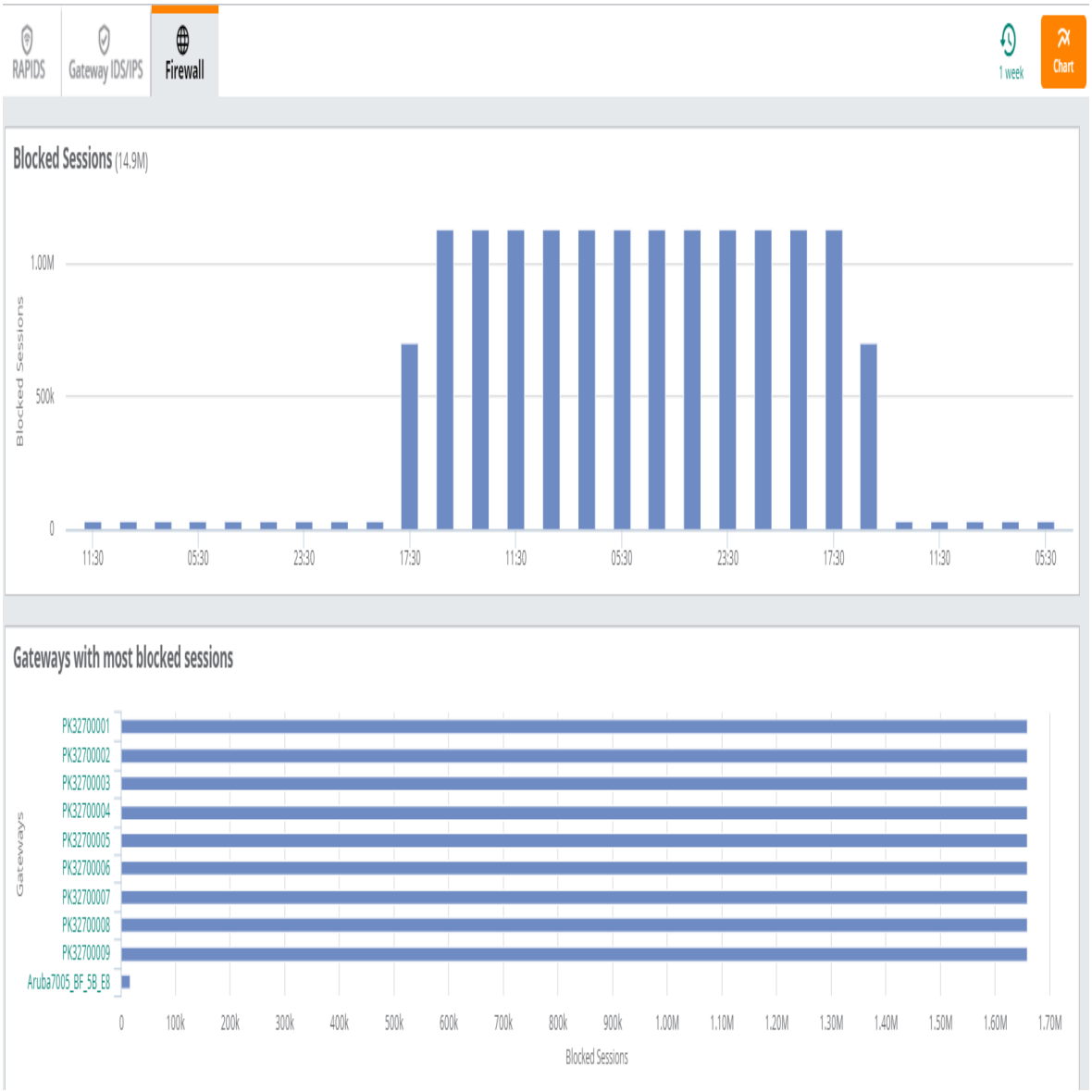
Viewing Blocked Sessions in the Chart View

To view blocked sessions in the chart view, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select all devices, set the filter to **Global**. The dashboard context for the global filter is displayed.
   - To select a Branch Gateway in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices > Gateways**. A list of gateways is displayed in the **List** view.
     c. Click a gateway under **Device Name**. The dashboard context for the gateway is displayed.
2. Under **Manage**, click **Security > Firewall** tab.
   - If the filter is set to **Global**, the **Blocked Sessions** section displays the following charts:
     - **Blocked Sessions Over Time**—Displays the blocked sessions over time. Hover over the histograms to view the number of blocked sessions and the time range (in date, year and duration) for the selected time range in the time filter.
     - **Gateways with Most Blocked Sessions**—Displays the top 10 gateways with most blocked sessions for the selected time range. Hover over any horizontal bar to view the number of blocked sessions for each gateway. Click any gateway to navigate to the corresponding **Blocked Sessions** table or click the host name next to the gateways to navigate to the **Gateway Summary** page.

     The following image displays the **Blocked Sessions** section for the Global Dashboard:

Figure 495 *Firewall Dashboard with Blocked Sessions*



- If the filter is set to a gateway, the **Blocked Sessions** section displays the following charts:
  - **Blocked Sessions Over Time**—Displays blocked sessions over time for a gateway. Hover over the histograms to view the number of blocked sessions and the time range (in date, year and duration) for the selected time range in the time filter. Click any of the histogram bars to navigate to the **Blocked Sessions** table for the selected time range. Based on the selection, the blocked sessions data with the highlighted histogram is displayed.
  - **Blocked Sessions Top Categories**—The horizontal bar graph displays the top application categories with the most number of blocked sessions. Hover over any application to view the blocked sessions count for each application category. The legends in the graph display the number of blocked sessions for the top application categories. Click any application to navigate to the **Blocked Sessions** table for the respective application category. Based on the application selection, the blocked sessions data for the selected application with the highlighted histogram is displayed.

  The following image displays the **Blocked Sessions** section for the gateway dashboard:

Figure 496 *Blocked Sessions Details for the Gateway Dashboard*

Viewing the Blocked Sessions in the Table view

The **Blocked Sessions** page provides a detailed summary of all blocked sessions on the gateways and allows you to view and analyze the sessions by using the histograms and sessions table displayed in the blocked sessions pane. The histogram time interval varies based on the following time range selection:

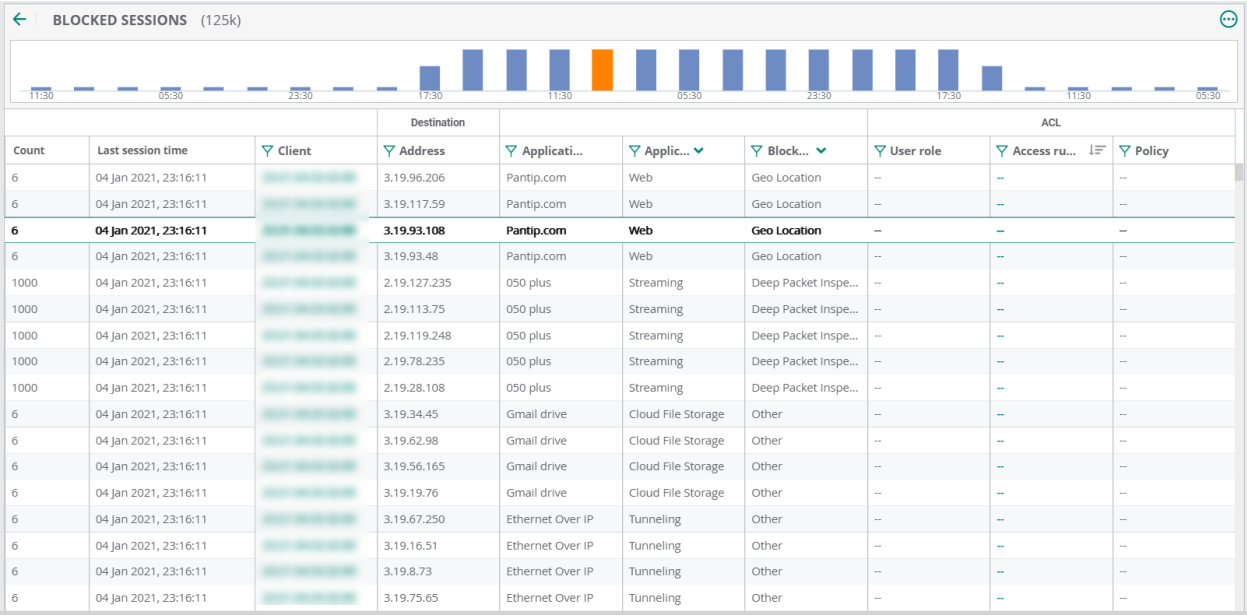
- 3 hours—15 minutes time interval
- 1 day—1 hours time interval
- 1 week—6 hours time interval.

Hover over the histogram to view the number of blocked sessions and the time range (in date, year and duration) for the selected time range in the time filter. To view the sessions data of an application for a specific time range, select the time range and select any of the histogram bars. The sessions data table displays blocked session for the selected histogram bar. To view the sessions table for multiple time range, select either 3 hours or 1 day from the temporal time window, click and drag the histogram either right or

left in the same axis to select and view the multiple time range session data. For 1 week time range, the default interval in the histogram is set to 6 hours. The time range for the histogram can be selected for a minimum of 15 minutes and maximum of 6 hours.

The following image displays the **Blocked Sessions** section for an application with highlighted histogram:

Figure 497 *Blocked Sessions table with Histograms*



To view the **Blocked Sessions** in a tabular view for a gateway, click the **List** icon in the top right corner of the **Firewall** dashboard. The blocked sessions are displayed in a table and contains the following details:

Table 312: *Blocked Sessions in a List View*

Data Pane Item	Description
Count	Displays the number of sessions.
Last session time	Displays last aggregated session's timestamp.
Client	Displays the MAC address of the device. Click the client MAC address hyperlink to view the corresponding **Client Details** page. For more information, see Clients > Wireless Client > Overview.
Source	**Address**—Displays the IP address of the client device that initiated this session.
Destination	▪ **Address**—Displays the destination IP address of this session. ▪ **Port**—Displays the destination port.
Protocol	Displays the communication protocol used.
Application	Displays the application identified for this session. **NOTE:** This column can be empty if the session is denied before classifying the application.

Table 312: *Blocked Sessions in a List View*

Data Pane Item	Description
Domain	Displays the derived domain of the destination application or URL.
Application Category	Displays the application category. **NOTE:** This column can be empty if the session is denied before categorizing the application.
WebCC Category	Displays the WebCC category.
VLAN	Displays the VLAN associated with the initiating client device session.
Blocked Reason	Displays the cause of the blocked session. The cause may be one of the following: ■ **Deep Packet Inspection**—Session blocked due to application classification based on Deep Packet Inspection and associated policies; usually applies to any pre-defined or custom applications. ■ **Web Classification**—Session blocked based on Web Content Classification or Web Reputation and associated policies; usually applies to web sites and web URLs. ■ **IP Reputation**—Session blocked based on IP Reputation policies, usually applies to IP addresses. ■ **Geo Location**—Session blocked based on Geo Location policies, usually applies to geographic location of source or destination IP address. ■ **Others**—Session blocked due to any other reasons not covered above, including session and network ACLs.
ACL	■ **User Role**—Determines the user's network privileges based on the assigned user role. ■ **Access Rule**—Indicates the assigned rule. Hover over the access rule for any session to view the **Role**, **Policy**, and **Rule** applied for that session. ■ **Policy**—Indicates the policies assigned to users.
Autofit columns	Adjusts the column width of the table to fit the page evenly.
Reset to default	Resets the table view to default columns.

About RAPIDS

With Aruba Central, you can identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central sends alerts to the network administrators about the possible threat and provides essential information needed to locate and manage the threat.

This section includes the following topics:

- Generating Alerts for Security Events
- Generating Reports for Security Events

Viewing the RAPIDS Page

To view the RAPIDS page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
2. Under **Manage**, click **Security**. The **RAPIDS > IDS** > **WIDS Events** table is displayed.

Users with the admin role can see all the interfering devices.

Monitoring WIDS Events

The **Manage > Security > RAPIDS > IDS** tab provides a summary of the total number of wireless attacks detected for a given duration.

The **WIDS Events** table displays the following information category:

- **Infrastructure attacks**—Displays the number of infrastructure attacks detected in the network.
- **Client attacks**—Displays the number of client attacks detected in the network.

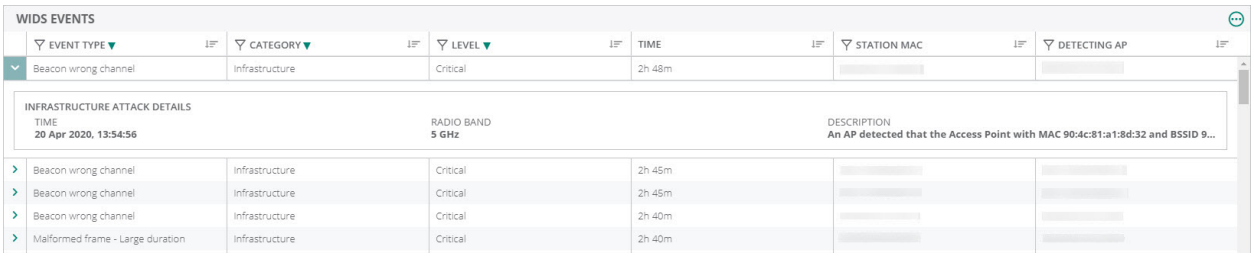
Table 313: *WIDS Events*

Field	Description
Event Type	The type of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the event types based on your requirement.
Category	Category of the intrusion or attack, infrastructure, or client attack. Click the drop-down arrow at the column heading to filter the category that you want to display.
Level	The level of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the attack level.
Time	Time of the intrusion or attack.
Station MAC	MAC address of the station under attack or BSSID of the AP under attack.
Detecting AP	The MAC address of the device that detected the intrusion or attack.
Radio Band	Radio band on which the intrusion was detected. There are two radio band signals available, 2.4 GHZ and 5 GHZ. Click the drop-down arrow at the column heading to filter the radio band where the intrusion was detected.
Description	Details of the attack or the intrusion.

Note the following important points:

- Clicking icon enables you to customize the **WIDS Events** table columns or set it to the default view.
- To view the details of each event that is generated, click the arrow against each row in the table.

Figure 498 *Event Expansion*



- Intrusions are displayed for the time selected in **Time Range Filter**. The **WIDS Events** displays data for a maximum time period of 1 only.

Configuring IDS Parameters

The type and severity of Intrusion Detections raised by an AP is configurable and affects the data that is seen in the **WIDS Events** table. For more information, see Configuring IDS Parameters on APs.

Generating Alerts for Security Events

Aruba Central supports configuring alerts for IDS events. To generate alerts, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
2. Under **Analyze**, click **Alerts & Events**. The **Alerts & Events** page is displayed.
3. In the **Alerts & Events** page, click the **Config** icon.

   The **Alert Severities & Notifications** is displayed.
4. Select **Access Point** tab to display the AP dashboard. Aruba Central supports three alert types for identifying interfering devices:
   - Rogue AP Detected
   - Infrastructure Attacks Detected
   - Client Attack Detected
5. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning.

NOTE

For a few alerts, you can configure threshold value for one or more alert severities. To set the threshold value, select the alert and in the **exceeds** text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

   b. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:
      - **Group**—Select a group to limit the alert to a specific group.
      - **Label**—Select a label to limit the alert to a specific label.
      - **Sites**—Select a site to limit the alert to a specific site.
   c. **Notification Options**
      - **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a

comma.

- **Streaming**—Select the **Streaming** check box to receive the streaming notifications when an alert is generated.
- **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list. For more information, see Webhooks.
- **Syslog**—Select the **Syslog** check box to receive the syslog notifications when an alert is generated.

d. Click **Save**.

For more information on how to configure Alerts, see Configuring Alerts.

Generating Reports for Security Events

Aruba Central supports generating reports for IDS events. To generate reports, complete the following steps:

1. In the **Network Operations** app, use the filter to select **Global**.
2. Under **Analyze**, click **Reports**.
3. In the **Reports** page, click **Create**. Aruba Central supports **Security Compliance** to display the report of all wireless intrusions. For more information on how to create Reports, see Creating a Report.

For creating RAPIDS report, you need not select the **Groups** or **Labels** option. Also, you need not select the device groups name or labels name from the **Device Groups** or **Labels** drop-down lists, respectively.

About Floorplans

Floorplans allow you to plan sites, create and manage floor plans, and provision access points. You can use Floorplans to do basic planning procedures, such as, creating a floor plan and provisioning access points. The **Floorplans** dashboard can be accessed only from a site context.

Floorplans provide a real-time picture of the radio environment of your wireless network and the ability to plan the wireless coverage of new sites. For a better understanding of your wireless network, you must know the location of your devices and users, and the RF environment of your network. Floorplans provide this information at your fingertips through integrated mapping and location data.

Floorplans use sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every wireless device in range. Floorplans does not require dedicated RF sensors or a costly additional location appliance, because it gathers all the necessary information from your existing devices.

- Floorplans is supported only on access points running 6.5.2.0 or a later version.
- Do not use the back or front navigation. Instead, use the breadcrumbs.
- APs are removed from the floorplan and deployed device list based on the device unlicensing. For example, When you unassign a license for an AP, it gets removed from the deployed device list and floorplans, and when you assign back the license for an AP, it gets added back to the deployed device list and to the same co-ordinates of the floorplan location. Also, when your license gets auto expired, the devices gets removed from the list and floorplan location and the same gets added back on license renewal. Make sure that you check the assigned AP device licensing status before adding them to the floorplan. For more information, see Managing License Assignments.

Floorplans offer the following features:

- Create and import floor plans.
- Pictorial navigation that allows you to view the floor plans associated with access points, associated clients, rogues, buildings, and floors.
- Accurate calculation of the location of all associated client devices using RF data from your devices.
- Accurate calculation of the location of all rogue devices (as classified by RAPIDS) using RF data from your devices.
- A map view that shows the location of devices and heatmaps that depict the strength of RF coverage in each location.

Related Topics

- Floorplans Dashboard
- Planning and Provisioning Devices
- Customizing the Floorplans View
- Floorplans APIs

Floorplans Dashboard

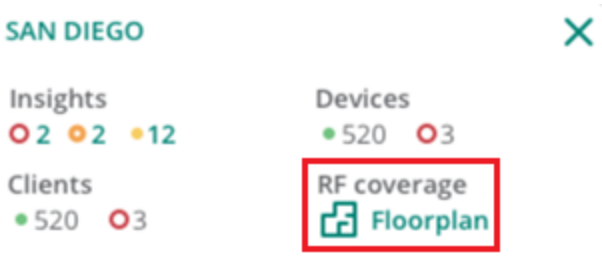
The **Floorplans** dashboard can be accessed from a site context or an access point context. You can either navigate to a specific site to view the floor plan or view a specific site floor plan from the **Network Health** tab in the **Global** context.

To view the **Floorplans** dashboard from the **Network Health** tab in the **Global** context, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the **Global** filter is displayed.
2. Under **Manage** > **Overview**, the **Network Health** page is displayed.

3. Hover over a site to view the following details:

   Figure 499 *Site-level Details with Floorplan Option*



4. Click **Floorplan** under **RF Coverage**. The **Floorplans** dashboard for the selected site is displayed.

To view the **Floorplans** dashboard from a site context, complete the following steps:

1. In the **Network Operations** app, set the filter to a **Site**.
   The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.
   The **Floorplans** dashboard allows you to customize the view by selecting various properties and also allows you to select multiple floors in the same site.

To view the **Floorplans** dashboard from an access point context, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the **Global** filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of access points is displayed in the **List** view.
3. Click the **Access Point** name to view the **Access Point Details** page. If there are many APs connected to the network, click **Online** or **Offline** to filter the online or offline APs.
4. Additionally, enter the access point name in the **Device Name** column and then click the AP name. The AP **Summary** page is displayed.
5. Under **Manage** > **Overview**, click **Floor Plan**. The floor plan details with the highlighted AP is displayed.
6. Click anywhere on the floor plan to navigate to the exact floor for a site with the AP highlighted.

The floor plan details for an AP is only accessible for the devices that are assigned with license.

Planning and Provisioning Devices

Floorplans provide the capability to plan buildings, floors, and location for device provisioning before the actual deployment. You can create a floor plan and add devices to the floor plan.

The planning and provisioning workflow includes the following procedures:

- Creating a Floor Plan
- Importing a Floor Plan
- Modifying Floor Plan Properties
- Adding Devices to the Floor Plan

Creating a Floor Plan

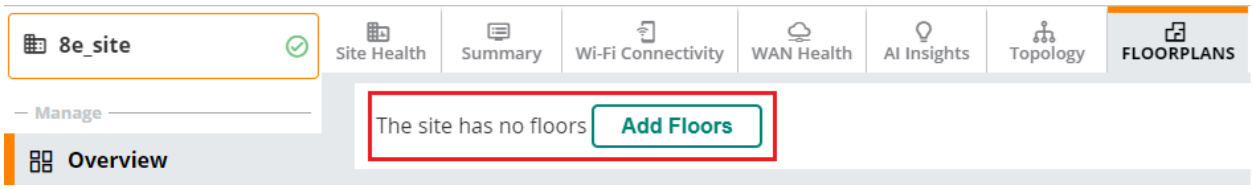
Floorplans allow you to add, modify, and import a floor plan background image file. When importing RF plans ensure that the devices from the device catalog are included.

To create a new floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to a **Site**.

   The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.
3. Click **Add Floors**. The **Floor Plan** tab is displayed.

   Figure 500 *Floorplans Dashboard*



4. Click **Edit** in the slide out pane on the right.
5. Click **New Floorplan**. You can also add the floor plan by right-clicking on the center gray area and click **New Floorplan**. The **New Floorplan** pop-up window is displayed.
6. Click **Choose File** and locate a floor plan image file from your local file system. You can import the floor plan image file in the jpg, jpeg, gif, bmp, pdf, png, dwg, and svg format.
7. Assign a floor name and a floor number in the **Floor name** and **Floor number** text boxes, respectively.
8. Click **Save**.
9. You can define new floor by clicking the **Define New Floor** option on the top right corner.
10. The **Define New Floor** includes the following option:
    a. **Scale**—Shows the dimensions of the floor.
    b. **Region**—Allows you to define floor plan boundary and planning region.
    c. **CAD Layer**—Allows you to import walls from the CAD file.
    d. **Access Points**—Allows you to add the access point's to the floor plan.
11. Click **Next** button after you set the **Scale**, **Region**, and **CAD layer** for the floor.
12. To add a planned access point, under **Access Points** > **Planned APs**, select the device type from the **Type** drop-down menu.
13. In the **Count** field, enter the number of devices to add to the new floor.
14. Click and drag the **Deployment Type** slider bar to adjust data rates for a high density or low density environment.
15. Optionally, click the **Advance** link to configure the advance deployment options:
    a. **Service Level**—Select **Speed** or **Signal** to plan coverage by adjusting the data rate requirements (speed) or AP signal strength settings. Click **Calculate AP Count** to recalculate the suggested number of APs based on these settings.
    b. **Client Density**—In the **Max Clients** field, set the anticipated number of clients that will be stationed in the floor. In the **Clients Per AP** field, enter the maximum number of clients supported by each radio. Click **Calculate AP Count** to recalculate the suggested number of APs based on these settings.
16. Click **Add APs to Floorplan** to add the planned APs to the floor.

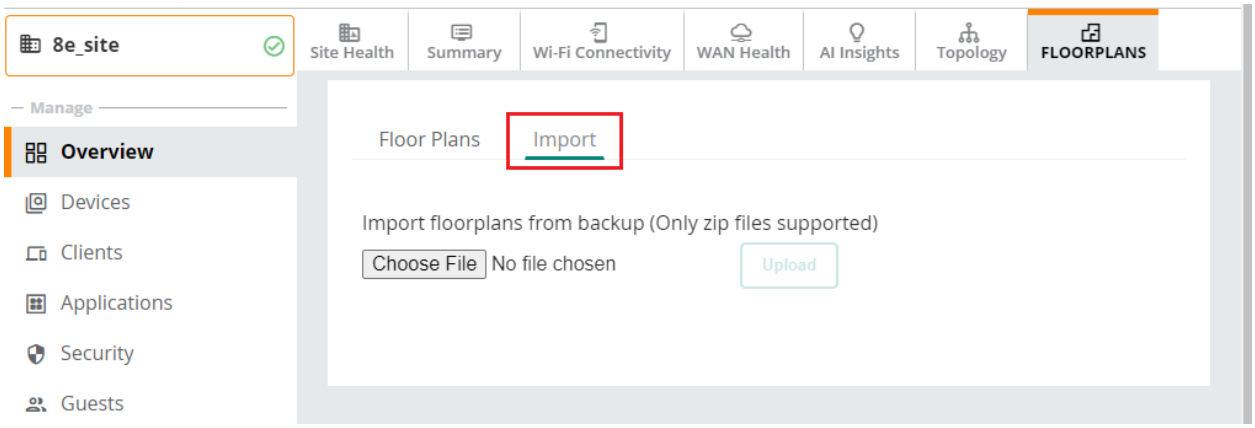
17. Click **Finish**.
18. To remove the planned device from the floor plan, right-click on that device and click **Remove**.

Importing a Floor Plan

To import a floor plan exported from AirWave or Aruba Central, complete the following steps:

1. In the **Network Operations** app, set the filter to a **Site**.
   The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.
3. Click the **Import** menu option.
   Below is an example figure of **Import** menu option:

   Figure 501 *Floorplans Import Option*



4. Click **Choose File** and select the floor plan zip file to import.
5. Click **Upload**. When an import is complete, the UI displays a notification to alert the user.

Modifying Floor Plan Properties

To edit the properties of an existing floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to a **Site**.
   The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.
3. Click **Edit** to modify the properties. In case of multiple floors, select the floor from the drop-down list and click Edit. For more information on edit, see Customizing the Floorplans View.
4. Click **Save**.

Adding Devices to the Floor Plan

You can add planned devices or devices available in Aruba Central, to a floor plan. Planned devices are used to simulate AP behaviors (heatmap coverage) on the floor plan, instead of real devices. You can match and replace planned devices with real devices that are available in Aruba Central.

To add the already deployed devices to the floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to a **Site**.
   The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.

3. Click **Edit**. In case of multiple floors, select the floor from the drop-down list and click **Edit**.
4. Click the **Add Deployed Devices**. A list of devices is displayed.
5. Expand the group containing the APs which need to be provisioned on this floor plan. Note that by default, devices that have already been added to **Floorplans** are hidden. To show them, clear the **Hide APs that are already added** check box at the bottom of the list.
6. Click and drag an AP to its proper location on the floor.
7. To remove a device from the floor plan, right-click that device and then click **Remove.**

To add planned devices when creating a new floor plan, complete the following steps:

1. In the **Network Operations** app, set the filter to a **Site**.
   The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floorplans**. The **Floorplans** dashboard is displayed.
3. Click **Edit**. In case of multiple floors, select the floor from the drop-down list and click **Edit**.
4. Click **Add Planned Devices** and select a device type (model) from the list of available devices.
5. Click and drag the device to the desired location on the floor.
6. To replace a planned AP with an AP that is available in Aruba Central, click **Auto-Match Planned Devices** from the **Action** tab.

To auto-match devices, ensure that you edit the device name or MAC address of the planned AP to match the name or MAC address of the AP added to Aruba Central.

7. To remove a planned device from the floor plan, right-click on that device and then click **Remove**.

Customizing the Floorplans View

To customize your floor plan view, click the **View** tab on the right sliding panel. The **View** tab displays the list of devices.

- Click **APs** to view the details of the access point and the RF environment.
- Click **Clients** to view the client details.
- Click **Rogues** to view the rogue details.

The **Floorplans** navigation menu on the right pane consists of the **Properties**, **View**, and **Edit** tabs. The following table describes the menu options available for a floor:

Table 314: *Floorplan Menu Options*

Tabs	Options
Properties	The **Properties** tab has the following menu options: ■ **APs**—Displays the total number of APs, the planned APs, and the number of APs that are offline. ■ **Floor name**—Displays the floor name. ■ **Floor number**—Displays the floor number. ■ **Width**—Displays the current width of the floor plan. To change these settings, click the **Measure** icon and measure a portion of the floor. ■ **Height**—Displays the current height of the floor plan. To change these settings, click the **Measure** icon and measure a portion of the floor. ■ **Gridsize**—Displays the grid. Decreasing the grid size enables the location to place clients in a small grid which increases accuracy. ■ **Advanced**—Allows you to set the values to indicate if the environment is related to an office

Tabs	Options
	space, cubicles, offices, or concrete.
View	The **View** tab has the following menu options: ■ **Devices**—Displays APs, clients, and rogue devices detected on the floor. ■ **AP Overlays**—Shows the heatmap for the current and adjacent floors. ■ **Floorplan Features**—Displays the following details: ●**Grid Lines**–Allows you to change the grid size and color. ●**Labels**–Shows or hides the labels tagged to the devices on the floor. ●**Origin**–To ensure that multi-floor heatmaps display properly, ensure that your floor plans are vertically aligned. **Floorplans** use the origination point for this alignment. By default, the origin appears in the upper left corner of the floor plan. You can drag and drop the origin point to the correct position. ●**Regions**–Displays the regions defined within a floor plan. For example, you can define two small regions of high density clients within a larger floor plan with lower client density. ●**Walls**–Displays walls drawn on the floor.
Edits	The **Edit** tab has the following menu options: ■ **Drawing**—Allows you to draw a region or wall for the floor. ■ **Devices**—Allows you to add and delete the already deployed or planned devices. ■ **Actions**—Displays the following options: ●**Select All**–Selects all floors. ●**Export Floor Plans**–Exports the floor plan of a specific floor. ●**Undo**–Cancels the previous action. ●**New Floorplan**–Allows you to create a new floor plan. ●**Auto-match Planned Devices**–Automatically matches the devices that are planned for deployment and reloads the page. ●**Go to floor above**–Allows you to navigate to the floor above. ●**Go to floor below**–Allows you to navigate to the floor below. ●**Refresh**–Refreshes the page. ●**Replace Background**–Allows you to replace the current background.

User Interface Elements of the Floorplans Dashboard

The **Floorplans** dashboard provides various options to customize your view. The customizable parameters include:

Table 315: *User Interface Elements*

UI Element	Description
	Click the drop-down to select a specific floor from the site.
	Click **APs** to view the details of the access point and the RF environment.
	Click **Clients** to view the client details.

Table 315: *User Interface Elements*

UI Element	Description
	Click **Rogues** to view the rogue details.
	Click **Heatmaps** to view the strength of RF coverage in each location. You can view heatmaps in monochrome also. Click the monochrome check box in the **Floorplans** dashboard to select either the monochrome display or the colored display of heatmaps.
	Click **Walls and Regions** to view the segregation of regions and walls in the selected floor.
	Click the **Refresh** icon to refresh the floor plan details.
	Click the **+** or **-** icon to zoom in or zoom out of a floor plan. You can also scroll to increase or decrease the floor plan view. Additionally, click the box icon to view the floor plan in full screen mode.

Floorplans APIs

Aruba Central supports the following APIs for retrieving client location and floor plan information:

- **GET /visualrf_api/v1/building/{building_id}**—Retrieves information about specific building and its floors.
- **GET /visualrf_api/v1/floor/{floor_id}**—Retrieves details about a specific floor.
- **GET /visualrf_api/v1/floor/{floor_id}/image**—Retrieves background image from a specific floor plan.
- **GET /visualrf_api/v1/floor/{floor_id}/access_point_location**—Retrieves information about the location of the APs on a specific floor plan.
- **GET /visualrf_api/v1/access_point_location/{ap_id}**—Retrieves location details of a specific AP.
- **GET /visualrf_api/v1/client_location/{macaddr}**—Retrieves location details of a specific client.
- **GET /visualrf_api/v1/floor/{floor_id}/client_location**—Retrieves information about the location of clients on a specific floor.

For more information on APIs, see Aruba Central APIs and refer to API documentation at https://app1-apigw.central.arubanetworks.com/swagger/central.

Alerts & Events

The **Alerts & Events** pane displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management.

This section includes the following topics:

Alerts & Events Dashboard

The **Alerts and Events** dashboard displays a list of alerts and events generated for events pertaining to device provisioning, configuration, and user management. You can view the alerts and events in **List** view and **Summary** view. Configuration view is used to configure alerts and it is available only at the **Global** context. The components of the **List** view is different for **Alerts** and **Events** tab whereas the **Summary** view displays similar components.

This section includes the following topics:

Viewing Alerts in List view

You can view the details of the alerts and acknowledge alerts. Alerts are acknowledged automatically when the event count drops below the lowest severity threshold configured for the alert. Users with admin access can acknowledge alerts irrespective of the severity configuration. As manually acknowledging an alert does not reset the count data, the alert service continues to aggregate events. When the number of new events meets the configured threshold, an alert is triggered again.

To view the of list alerts and events and acknowledge alerts, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.
     c. A list of devices is displayed in the **List** view.
     d. Click a device listed under **Device Name**.

     The dashboard context for the device is displayed.

2. Under **Analyze**, click **Alerts & Events.**

   By default, the **Alerts & Events** page displays the alert and events in the **List** view.

   The **Alerts & Events** page offers a list view, summary view, and a configuration view.

Configuration view is only available at the **Global** context.

   By default, the **Alerts** tab is selected and the **Open Alerts** table is displayed. The table displays all the generated alerts. The **Alerts** bar categorizes the alerts as **Critical**, **Major**, **Minor**, and **Warning**.

The **Gateway Emergency Mode** and **VPN Peer Failover** alerts can be configured and enabled for all gateways. However, these alerts will not be generated for gateways on versions other than ArubaOS 8.0.x.

3. Optionally, click **Acknowledge All** to acknowledge all the alerts at once.

   Important Points:

   - Once an alert is acknowledged, the alert is moved to the **Acknowledged** tab.
   - All **Acknowledged Alerts** can be viewed when the **Show Acknowledged Alerts** button is ON.
   - If the user does not acknowledge an alert, the alert is suppressed for 5 minutes. The alert notification is then sent to the user every 5 minutes in case the issue still persists.
   - If the user acknowledges an alert, the alert is suppressed until the issue is resolved. After resolving the issue, if it re-occurs the alert is sent again.

4. Optionally, enable the **Show Acknowledged Alerts** button to display the list of acknowledged alerts.

Table 316: *Acknowledged Alerts Pane*

Data Pane Content	Description
Acknowledged On	Displays the timestamp of the acknowledged alert. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the alerts.
Acknowledged By	Displays the entry by whom the alert is acknowledged.
Occurred On	Displays the timestamp of the alert. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the alerts.
Elapsed Time	Displays the timestamp difference between when the alert actually occurred and, when the alert was acknowledged.
Category	Displays the category of the alert. Use the filter option to filter the alert by category.
Label	Displays the label name of the alert.
Site	Displays the site name of the alert.
Group	Displays the group name of the alert.

Data Pane Content	Description
Severity	Displays the severity level of the alert. The severity can be **Critical**, **Major**, **Minor**, or **Warning**.
Description	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

Advanced Alert Filtering

Aruba Central allows you to filter the alerts based on the alert categories. To filter alerts based on alert categories, complete the following steps:

1. In the **Alerts** page, click **Click here for advanced filtering** to filter the alerts based on alert categories.
2. Select the alert category and click **Filter**. You can select multiple categories from the advanced filtering option.
3. The **Open Alerts** table displays the list of alerts generated in each alert category. The filter summary bar displays the total number of alerts in the selected categories.
4. Optionally, to clear advanced filtering option, from the alerts summary bar, click **Clear All**. The advanced filtering gets cleared.

The following table describes the information displayed in each column of the **Alerts** table:

Table 317: *Alerts Pane*

Data Pane Content	Description
Occurred On	Displays the timestamp of the alert. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the alerts.
Category	Displays the category of the alert. Use the filter option to filter the alert by category.
Label	Displays the label name of the alert.
Site	Displays the site name of the alert.
Group	Displays the group name of the alert.
Severity	Displays the severity level of the alert. The severity can be **Critical**, **Major**, **Minor**, or **Warning**.
Description	Displays a description of the alert. Use the search option in filter bar to filter the alert based on description.

To customize the **Alerts & Events** table, click the ellipses  icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Viewing Events in List view

To view a summary of events, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
2. Under **Analyze**, click **Alerts & Events**.

   By default, the **Alerts & Events** page displays the alert and events in the **List** view.

   The **Alerts & Events** dashboard offers a list view, summary view, and a configuration view.

Configuration view is only available at the **Global** context.

3. In the **Alerts & Events** summary bar, click **Events**. By default, the **List** view is selected and a consolidated list of events is displayed in the events table.

Advanced Event Filtering

Aruba Central allows you to filter the events based on the event types. To filter events based on event types, complete the following steps:

1. In the **Events** page, click **Click here for advanced filtering** to filter the events based on event types.
2. Select the event type and click **Filter**. You can select multiple event types from the advanced filtering option.
3. The events table displays the list of events generated in each event type. The filter summary bar displays the total number of events in the selected category and the type(s) of events.
4. Optionally, to clear advanced filtering option, from the events summary bar, click **Clear All**. The advanced filtering gets cleared.

The following table describes the information displayed in each column of the **Events** table:

Table 318: *Events Pane*

Data Pane Content	Description
Occurred On	Displays the timestamp of the event. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the events.
Device Type	Displays the type of the device, Access Point, Gateway, Switch. Use the filter option to filter events by device types.
Device Hostname	Displays the host name of the device where the event is generated.

Data Pane Content	Description
Device MAC	Displays the MAC address of the device.
Client MAC	Displays the MAC address of the device to which the client is connected.
BSSID	Displays the BSSID of the device.
Event Type	Displays the type of the event.
Label	Displays the label name of the event.
Site	Displays the site name of the event.
Group	Displays the group name of the event.
Description	Displays the description of the event. Use the column filter to filter an event based on the description.

For events related to IAPs running ArubaOS version 8.5 or later, Aruba Central offers additional details regarding the selected event. Click the expand arrow in the events row for the IAP, to see the additional details.

If you have an IAP running ArubaOS version 8.7 or later, the expanded text box for an event displays more data compared to a similar event generated for an IAP running an earlier version of ArubaOS.

The additional details expansion box is not available for events related to gateways, switches, and IAPs running an ArubaOS version which is earlier than 8.5.

Figure 502 *Additional Details for an Event Related to an IAP Running ArubaOS Version 8.7*

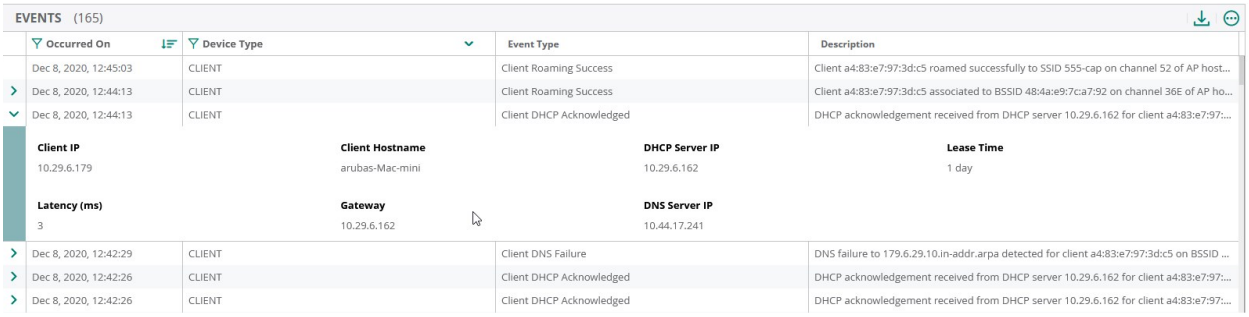
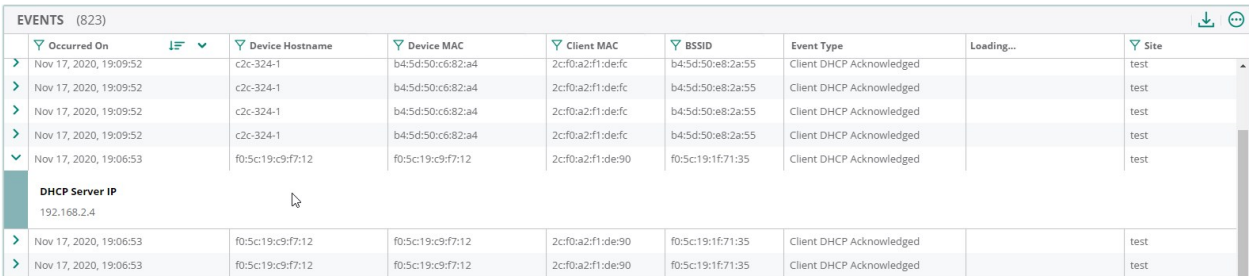


Figure 503 *Additional Details for an Event Related to an IAP Running ArubaOS Version 8.6*



To customize the **Alerts & Events** table, click the ellipses icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Aruba Central allows you to download the global list of events to your local browser. Click to download the events list in a CSV format.

Viewing Alerts & Events in Summary view

To view a summary of alerts and events, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

     The dashboard context for the device is displayed.
2. Under **Analyze**, click **Alerts & Events.**

   By default, the **Alerts & Events** page displays the alert and events in the **List** view.

   The **Alerts & Events** page offers a list view and summary view, and a configuration view.

NOTE

Configuration view is only available at the **Global** context.

3. To view the graphs displaying alerts and events, click the **Summary** icon. By default, **ALL** tab is selected. Select each tab **Access Points**, **Switches**, or **Gateways** to view the graphs pertaining to each device type.

NOTE

The **Alerts & Events** graphs are displayed for the time range selected. Select the time range from the Time Range Filter ( ) to filter alerts and events.

The graphs in the **Summary** view displays the alerts and events in the following categories:

- **Alerts By Type**—Displays the alert categories under which the maximum alerts are generated. Hover your mouse over the bar graphs to see the total count of alerts generated under each category.
- **Alerts By Severity**—Displays the alert severity categorized under **Critical**, **Major**, **Minor**, and **Warning**. Hover your mouse to see the total count of alerts generated under each severity level.
- **Events By Type**—Displays the event categories under which the maximum events are generated. Hover your mouse over the bar graphs to see the total count of events generated under each category.

Configuring Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. To configure alerts, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

2. Under **Analyze**, click **Alerts & Events**.

   The **Alerts & Events** page is displayed in the **List** view.

3. In the **Alerts & Events** page, click the **Config** icon.

   The **Alert Severities & Notifications** is displayed.

4. Use the tabs to navigate between the alert categories. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile and do the following:

   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:
      - Virtual Controller Disconnected
      - Rogue AP Detected
      - New User Account Added
      - Switch Detected
      - Switch Disconnected

For a few alerts, you can configure threshold value for one or more alert severities. Enter a value in the **exceeds** text box to set a threshold value for the alerts. The alert is triggered when one of the threshold values exceed the duration.

   b. **Duration**—Enter the duration in minutes.

   c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:
      - **Group**—Select a group to limit the alert to a specific group.
      - **Label**—Select a label to limit the alert to a specific label.
      - **Device**—Select a device to limit the alert to a specific device.
      - **Site**—Select a site to limit the alert to a specific site.

   d. **Other Filter Options**—(Optional) In addition to the device filter options few alerts also has further filtering options in order to restrict the alert scope by setting one or more of the following parameters:
      - **SSID**—For few **Connectivity** alerts, you can select a SSID to limit the alert to a specific SSID.
      - **Interface**—For few switch port alerts, you can mention an interface value to limit the alert criteria to a specific port.
      - **Band**—For few **Access Point** alerts, you can select the band, 2.4 GHz or 5 GHz to limit the alert to a specific band.
      - **Subnet**— For few gateway alerts, you can limit the alert for a specific DHCP pool identified by its subnet.
      - **Provider Tag**—For few gateway alerts, you can limit the alert to a particular uplink identified by its link tag (Provider Tag).

   e. **Notification Options**
      - **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma. The **Default Recipient** check box is selected by default. If you want to disable specific email addresses from the default list to avoid sending alert notification, click the number displayed in parenthesis and click ✕ against each email address. To add or delete default recipient, see Adding Default Recipients. Uncheck the **Default Recipient** check box in order to disable alert notifications to all the default email addresses.

NOTE

The number displayed in the parenthesis denotes the total number of email addresses that have been already configured as default recipients to receive notifications when an alert is generated.

- **Streaming**—Select the **Streaming** check box to receive the streaming notifications when an alert is generated.
- **Webhook**—Select the Webhook check box and select the webhook as required. You can also Create Webhook for alert notification. For more information, see Webhooks.

f. Click **Save**.

g. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the page.

NOTE

You can use the **Search box**, to search for alerts using keywords.

Aruba Central allows you to configure the following alerts:

- User Alerts
- Access Point Alerts
- Switch Alerts
- Gateway Alerts
- Connectivity Alerts
- Audit Alerts
- Site Alerts

User Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see Configuring Alerts.

Following are the user management alerts that you can configure:

- **New User Account Added**—Generates an alert when a new user account is added. This alert is enabled by default and the alert severity is **Major**.
- **User Account Deleted**—Generates an alert when a user account is deleted.
- **User Account Edited**—Generates an alert when a user account is edited.

Switch Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see Configuring Alerts.

Following are the switch alerts that you can configure:

- **New Switch Connected**—Generates an alert when a new switch is connected.
- **Switch Disconnected**—Generates an alert when a switch is disconnected. This alert is enabled by default and the alert severity is **Major**. In the **Duration** field, enter the duration during which the condition persists. The alert must be generated if the condition persists even after this duration. The default value is 10 minutes.
- **Switch Mismatch Config**—Generates an alert when there is a mismatch in switch configuration.

- **Switch Hardware Failure**—Generates an alert when the switch hardware fails. The following are the typical hardware failures for Aruba and MAS switches:

  Aruba switches

  - Fan failure
  - Power supply failure
  - Redundant power supply failure
  - High temperature
  - Management module failures—Management module failed self-test or lost communication with management module
  - Slot failure—Lost communications detected, slot self-test failure or unsupported module, or chassis hot swap failure
  - Fabric power failure
  - Internal power supply: Fan failure
  - Internal power supply failure
  - Internal power supply main PoE power failure
  - Internal power supply: Main inlet exceeds/within total fault count
  - Bad driver—Too many undersized/giant packets
  - Bad transceiver—Excessive jabbering
  - Bad cable—Excessive CRC/alignment errors
  - Too long cable—Excessive late collisions
  - Over bandwidth—High collision or drop rate
  - Broadcast storm—Excessive broadcasts
  - Duplex mismatch HDx—Duplex mismatch. Reconfigure to Full Duplex
  - Duplex mismatch FDx—Duplex mismatch. Reconfigure port to Auto
  - Link flap—Rapid detection of link faults and recoveries

  MAS switches

  - Fan failure
  - High temperature
- **Switch NAE Status**—Generates an alert when the **NAE Status** for the AOS-CX switches exceed the **Normal** value, based on the severity configured. This alert is disabled by default and the alert severity is **Major**. If you want to generate alerts for the **NAE Status** of value **Disabled**, then set the alert severity to **Warning**.
- **Switch CPU Utilization**—Generates an alert when the switch CPU utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Switch Memory Utilization**—Generates an alert when the switch memory utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Switch Port Tx Rate**—In the **Transform Function** drop-down, select either **absolute** or **percentage**. Select **absolute** to generate an alert if the data transmission rate of the port (in terms of Mbps) exceeds the threshold value. Select **percentage** to generate an alert if the data transmission rate of the port (in terms of utilization as a percentage of total bandwidth available) exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.

- **Switch Port Rx Rate**—In the **Transform Function** drop-down, select either **absolute** or **percentage**. Select **absolute** to generate an alert if the data reception rate of the port (in terms of Mbps) exceeds the threshold value. Select **percentage** to generate an alert if the data reception rate of the port (in terms of utilization as a percentage of total bandwidth available) exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Input Errors**—Generates an alert when the percentage of input errors on the port exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Output Errors**—Generates an alert when the percentage of output errors on the port exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule (s) for this alert.
- **Switch Port Duplex Mode**—Generates an alert when the port is operating in half-duplex mode. In the **Interface** field, enter the interface name.
- **Switch PoE Utilization**—Generates an alert when the PoE utilization for a port exceeds the critical and major threshold value. This alert is enabled by default and the alert severity is **Critical**. You can add additional rule(s) for this alert.
- **Switch STP Root Change**—Generates an alert when there is a change in the Spanning Tree Protocol (STP) root. This alert is enabled by default and the alert severity is **Major**.
- **Stack Member Added/Removed**—Generates an alert when a stack member is added or removed. This alert is enabled by default and the alert severity is **Major**.
- **Switch Stack Commander Change**—Generates an alert when there is a change in Stack commander. This alert is enabled by default and the alert severity is **Major**.
- **Switch Uplink Port Usage**—Generates an alert when the total uplink port usage of a switch at a site exceeds the configured value in gigabytes (GB) within a specified duration. The severity for this alert is **Warning**. In the **exceeds** field, enter the uplink port usage value in GB. In the **Duration** field, enter the duration after which the alert occurs. The alert must be generated if the condition persists even after this duration.

Gateway Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts.

Following are the SD-WAN and Gateway appliance-related alerts that you can configure:

- **SLA DPS Compliance Violations**—Generates an alert when the WAN policy does not meet the compliance criteria.
- **New Gateway Connected**—Generates an alert when a new Branch Gateway is connected.
- **Gateway Disconnected**—Generates an alert when a Branch Gateway is disconnected. When a gateway disconnects because of license expiry, the alert description shows 'Reason: Device unlicensed'.
- **Gateway CPU Utilization**—Generates an alert when the Branch Gateway CPU utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Gateway Memory Utilization**—Generates an alert when the Branch Gateway memory utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **OSPF Session Error**—Generates an alert when an OSPF session fails.
- **BGP Session Error**—Generates an alert when a BGP session fails.
- **Gateway Base License Capacity Limit Exceeded**—Generates an alert when a Gateway with Foundation-Base Capacity subscription exceed the client capacity threshold.
- **Routing Table Limit**—Generates an alert when the routing table size exceeds the 90% of the capacity. This alert is auto-acknowledged when the Routing table size goes below 85% of the capacity.

- **BGP Neighbor Route Limit**—Generates an alert when the number of routes received from a BGP neighbor exceeds the configured limit. This alert is auto-acknowledged when the number of routes from the BGP neighbor goes below the configured limit.
- **Overlay Route Orchestrator Connection**—Generates an alert when the control connection between the Branch Gateway and the Overlay Route Orchestration (ORO) is down. This alert is auto-acknowledged when the control connection is re-established.
- **Gateway Cellular Data Usage**—Generates an alert when the cellular data usage exceeds the threshold value. You must set the **Data Usage alert limit** and **Billing start date** in the **Uplink** configuration page for this alert to generate.

  Note: This alert configuration is only applicable for 9004-LTE gateways that have an integrated LTE modem.
- **WAN Health-Check Failure**—Generates an alert when WAN health check fails.
- **WAN VPN-Peer Unreachable**—Generates an alert when the WAN VPN peer is unreachable.
- **WAN Uplink Status Change**—Generates an alert when the WAN uplink status changes.
- **WAN Uplink Autonegotiation State Change**—Generates an alert when the WAN uplink automatic negotiation status changes.
- **WAN Uplink Input Errors**—Generates an alert when the percentage of WAN uplink input errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink Output Errors**—Generates an alert when the percentage WAN uplink output errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule (s) for this alert.
- **WAN Uplink PHY Errors**—Generates an alert when the percentage WAN uplink PHY errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **DHCP Pool Consumption Alert**—Generates an alert when the percentage DHCP pool consumption exceeds the threshold value. In the **Subnet** field, enter the subnet address to filter the alert based on subnet.
- **IPSec Establishment Failure**—Generates an alert when the IPsec tunnel fails to establish.
- **IPSec SA Down**—Generates an alert when the IPsec SA is down.
- **All IPSec SAs Down**—Generates an alert when all the IPsec SAs are down.
- **CFG-SET Advertisement Failure**—Generates an alert when the CFG-SET advertisement fails.
- **Uplink Flapping**—Generates an alert when the uplink state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Tunnel Flapping**—Generates an alert when the tunnel state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Uplink Speed Flapping**—Generates an alert when the uplink speed changes. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **EST Enrollment Failure**—Generates an alert when the Virtual Gateway fails to enroll with the EST server.
- **VGW VM Down**—Generates an alert when an Aruba Virtual Gateway deployed as a Virtual Machine is down.
- **Gateway Firmware Upgrade Failed**—Generates an alert when there is a firmware upgrade failure.
- **Gateway IDS/IPS Engine Error State**—Generates an alert when the Gateway's IDS/IPS Engine state is either crashed or stopped. A severity of **Critical** indicates that the engine has crashed and **Major** indicates that the engine has stopped.

- **Gateway IDS IPS Engine CPU Utilization**—Generates an alert when the CPU utilization by IDS/IPS engine exceeds the threshold value and duration. You can add additional rule(s) for this alert.
- **Gateway IDS IPS Engine Memory Utilization**—Generates an alert when the memory utilization exceeds the threshold value and duration. You can add additional rule(s) for this alert.
- **Gateway IDS IPS Engine Packer Dropped Detected**—Generates an alert every time when the number of packets dropped exceeds the configured threshold value.
- **Gateway Threat Count**— Generates an alert when the number of threats exceeds the configured limit (Range - 50 to 500 threats) in the given duration. The gateway threat counts are aggregated at the device level.
- **Gateway Threat Count Per Signature**— Generates an alert when the number of threats associated with a specific signature exceeds the configured limit in the given duration. These alerts are aggregated for all the gateways at the customer level.

Currently, Aruba IDPS is supported only on 9004, 9012, and 9004-LTE Branch Gateways that have Security license entitled to them.
Alerts that fall under WAN/ Tunnels/ DPS/ Routing/ Firewall are not applicable to Aruba Unified Network Architecture deployments.

You can configure the following alerts for gateways running ArubaOS 8.0.x:

- **Gateway Emergency Mode**—Generates an alert when a gateway enters the emergency mode, where all the uplinks are down and the backup uplink is activated.
- **VPN Peer Failover**—Generates an alert when all the tunnels from the gateway to the primary VPN controller go down including via backup uplink and establishes a tunnel with the secondary VPN controller.

You can configure and enable these alerts for gateways running other ArubaOS versions also. However, these alerts will not be generated for gateways on versions other than ArubaOS 8.0.x.

Access Point Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see Configuring Alerts.

Following are the Instant access point (AP) alerts that you can configure:

- **New Virtual Controller Detected**—Generates an alert when a new virtual controller is detected.
- **Virtual Controller Disconnected**—Generates an alert when a virtual controller is disconnected. This alert is enabled by default and the alert severity is automatically set to **Major**. To customize the alert trigger, enter a duration in minutes, in the **Duration** field. By default, the trigger to generate the alert is set to 10 minutes.
- **New AP Detected**—Generates an alert when a new IAP is detected.
- **AP Disconnected**—Generates an alert when an IAP is disconnected. This alert is enabled by default and the alert severity is automatically set to **Major**. To customize the alert trigger, enter a duration in minutes, in the **Duration** field. By default, the trigger to generate the alert is set to 15 minutes.
- **Rogue AP Detected**—Generates an alert when a rogue IAP is detected. This alert is enabled by default and the alert severity is **Major**.

- **Infrastructure Attack Detected**—Generates an alert when an infrastructure attack is detected.
- **Client Attack Detected**—Generates an alert when a client attack is detected.
- **Uplink Changed**—Generates an alert when an uplink has changed.
- **Modem Unplugged**—Generates an alert when the modem is unplugged.
- **Modem Plugged**—Generates an alert when the modem is plugged.
- **AP CPU Utilization**—Generates an alert when the IAP CPU utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **AP Memory Utilization**—Generates an alert when the IAP memory utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Insufficient Power Supplied**—Generates an alert when the IAP is supplied with lesser power than the required power.
- **Radio Channel Utilization**—Generates an alert when the IAP radio channel utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **Radio Noise Floor**—Generates an alert when the Noise Floor (dBm) exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **Connected Clients per VC**—Generates an alert when the number of connected clients to the VC exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Connected Clients per IAP**— Generates an alert when the number of connected clients to the IAP exceeds the threshold value. You can enter the threshold value after which the alerts must be generated. The recommended value is 15 minutes and above. You can add additional rule(s) for this alert.
- **Radio Frames Retry Percent**—Generates an alert when the IAP radio frames retry percent exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **AP Tunnel Down**—Generates an alert when a single L3 tunnel configured on the AP goes down.
- **All AP Tunnels Down**—Generates an alert when all the L3 tunnels configured on the AP go down.
- **IAP Firmware Upgrade Failed**—Generates an alert when there is any IAP upgrade failure such as, no firmware image is available or there is no response from the device.
- **Radio Non Wifi Utilization**—Generates an alert when the IAP radio non-Wi-Fi utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.

Connectivity Alerts

Aruba Central allows network administrators and users with admin permissions to configure alerts. For more information, see Configuring Alerts.

Following are the connectivity alerts that you can configure:

- **DNS Delay Detected**—Generates an alert when clients experience significant delays in response from the DNS server. Set the severity values to generate an alert if the percentage of delay from the DNS server exceeds the threshold value. The **Duration** field displays the duration after which the alert is

generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

- **DNS Failure Detected**—Generates an alert when wireless APs experience a high number of connection failures with the DNS server. Set the severity values to generate an alert if the DNS failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DHCP Delay Detected**—Generates an alert when there is excessive DHCP delay from client to AP in the network. Set the severity values to generate an alert if the percentage of the DHCP delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DHCP Failure Detected**—Generates an alert when there is high number of DHCP failure observed from client to AP in the network. Set the severity values to generate an alert if the DHCP failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Authentication Delay Detected**—Generates an alert when there is excessive delay in the client authentication process with the AP in the network. Authentication failures include the following:
  - Wi-Fi security key-exchange failures
  - 802.1x authentication failures
  - MAC authentication failures
  - Captive failures

  Set the severity values to generate an alert if the percentage of the authentication delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Authentication Failure Detected**—Generates an alert when there are high number of client authentication failures in the network. Authentication failures include the following:
  - Wi-Fi security key-exchange failures
  - 802.1x authentication failures
  - MAC authentication failures
  - Captive failures

  Set the severity values to generate an alert if the authentication failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Association Delay Detected**—Generates an alert when client association delay is detected in the network. Set the severity values to generate an alert if the percentage of the association delay exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Association Failure Detected**—Generates an alert when client association failure is detected in the network. Set the severity values to generate an alert if the association failure percentage exceeds the threshold value. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

Audit Alerts

Aruba Central allows administrators to enable alerts for configuration changes at group level. The **Config Change Detected** alert is under **Audit** tab. Configuration change alerts are intended for administrators handling large distributed network. For more information on how to configure alerts, see Configuring Alerts. Audit alerts are triggered under the following scenarios:

- Create New Template
- Update Existing Template
- Variable Upload
  - Device Level: Sends an alert with additional parameters such as serial number and MAC address of the device
  - Group Level: Sends an alert with respective group name
  - Configuration restore
- Configuration change at Device Level
- Configuration change at Group Level

The alert content includes the following information:

- Group Name
- Device Type
- User ID
- Config Change
- Device Serial number and MAC Address

The following table describes the behavior of the alert and alert content depending on the user action:

Table 319: *Config Alert Behavior*

User Action	Group Name	Device Type	User ID	Config Change	Device Serial/ MAC
Created a template	Template group name	IAP/ Switch. Gateway	User ID	No Content	NO
Updated existing template	Template group name	IAP/ Switch/ Gateway	User ID	Changed content is displayed	NO
Uploaded variable at device level	Group name to which the device belongs	IAP/ Switch/ Gateway	User ID	No Content	YES
Uploaded variable at group level	Template group name	IAP/ Switch/ Gateway	User ID	No Content	NO
Made configuration at the device level	Group name to which the device belongs	IAP/ Switch/ Gateway	User ID	Changed content is displayed	YES
Made configuration change at the group level	UI group name	IAP/ Switch/ Gateway	User ID	Changed content is displayed	NO

Site Alerts

Aruba Central allows you to configure and enable this alert for aggregated device disconnections. For more information on how to configure alerts, see Configuring Alerts.

The **Aggregated Device Disconnections** alert is under **Site** tab. It is intended to reduce the number of alerts that are generated for customers that prefer to have a single notification or a handful of notifications for mass outages where several devices may go down simultaneously in a given site.

For example, if site alerts are configured with **Severity** as Major, **Duration** being 10 minutes, and **Site** as site1, a single alert saying "Aggregated Device Disconnects" is raised on the user interface for every set of device belonging to "site1" that goes down within 10 minutes of the first DOWN event limited to 100 devices per alert. Any device that is not a part of "site1" is treated as not being aggregated.

The alert content includes the following information for each device:

- Hostname
- Device Serial Number
- MAC Address
- IP Address

Unlike other alerts types, site alerts will not be auto closed.

Adding Default Recipients

To set default recipients for alert notification, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
   The **Alerts & Events** page is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
   The **Alert Severities & Notifications** is displayed.
4. In the **Alert Severities & Notifications** page, click **Default Recipients**.
   The **Default Recipients** dialog box is displayed.
5. Click the **+** icon to add the email address that you want add as a default recipient to receive notifications when an alert is generated.
   You can add multiple email addresses as required.
6. Click **Save**.

- You can also delete the existing email addresses that is already added as default recipients.
- When you configure email addresses in the site dashboard, it overrides the email addresses configured in the global dashboard.

Suppressing Alert Notifications in the Site Dashboard

Suppressing alerts for a particular site prevents all devices in the site from generating alert notifications. You can suppress alert notifications only in the site dashboard.

To suppress alerts in the site dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
   The **Alerts & Events** page is displayed in the **List** view.

3. Click the **Config** icon.
   The **Alert Notifications** page is displayed.
4. Enable the **Suppress Alerts** toggle button.
   The **Suppress Alerts** dialog box is displayed for confirmation.
5. Click **Suppress Alerts**.
6. Click **Save**.

Configuring Site-specific Email Notifications

Aruba Central enables you to configure site-specific email addresses for notifying alerts. When alerts are generated for a specific site, the email notification is automatically sent to the email addresses configured for that site. The email addresses configured in the site dashboard overrides the email addresses configured in the global dashboard. For more information on configuring alerts in the global dashboard, see Configuring Alerts.

To add an email address in the site dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
   The Alerts & Events page is displayed in the **List** view.
3. Click the **Config** icon.
   The Alert Notifications page is displayed.
4. In the **Email Configuration Override** window, click **+** to add an email address.
5. In the text-box, enter a valid email address.
6. Click **Save**.

- You can add up to a maximum of 10 email addresses for alert notifications in the site dashboard.
- When you configure email addresses in the site dashboard, it overrides the email addresses configured in the global dashboard.

Deleting an Email Address in the Site Dashboard

To delete an email address in the site dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
   The Alerts & Events page is displayed in the **List** view.
3. Click the **Config** icon.
   The Alert Notifications page is displayed.
4. In the **Email Configuration Override** window, click the delete icon beside the email address, that you want to delete.
5. Click **Save**.

Viewing Enabled Alerts

To view alerts that you have enabled, complete the following procedure:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Alerts & Events**.
   The **Alerts & Events** page is displayed in the **List** view.
3. In the **Alerts & Events** page, click the **Config** icon.
   The **Alert Severities & Notifications** is displayed.
4. In the **Alert Severities & Notifications** page, click **Enabled**.
   Use the tabs to navigate between the alert categories. The alerts enabled for each category are displayed in the respective tabs.

Supported AP Events

Aruba Central provides an **Events** dashboard for viewing the events triggered from access points (APs), clients, switches, and gateways.

The following table lists the AP events that are supported in Aruba Central:

Table 320: *AP Events*

Event	Description
AP IP Conflict	IP Conflict detected for IP [*Device IP*] to MAC [*Device MAC*].
AP Upgrade Failure	Upgrade failure.
AP Insufficient Power Supply	Received low POE power.
AP Modem Plugged	Modem plugged.
AP Modem Unplugged	Modem unplugged.
AP User Reboot	User reboot triggered.
AP Tri-Radio Enabled	Access point is online with tri-radio mode enabled.
AP Tri-Radio Disabled	Access point is online with tri-radio mode disabled.
AP Thermal Shutdown Event	Thermal management enabled.
AP Thermal Shutdown Recovery Event	Thermal management disabled.
Radio Radar Detected	802.11 Radar detected on channel [*Channel*].
Radio Radar Cleared	802.11 Radar cleared on channel [*Channel*].
Radio Tx Hang	802.11 Radio Tx hanged on channel [*Channel*].
Radio Tx Clear	802.11 Radio Tx cleared on channel [*Channel*].
Radio 40MHz Intolerance	40MHz Intolerance observed on channel [*Channel*].

Event	Description
Radio Cancel 40MHz Intolerance	40MHz Intolerance cleared on channel [*Channel*].
Radio 40MHz Align	40MHz aligned on channel [*Channel*].
Radio ARM Interference	ARM Interference detected on channel [*Channel*].
Radio ARM Invalid Channel	ARM invalid channel [*Channel*].
Radio ARM Error Threshold Exceeded	Radio errors threshold exceeded on channel [*Channel*].
Radio ARM Noise Threshold Exceeded	Radio noise threshold exceeded.
Radio ARM Empty Channel	ARM empty channel.
Radio ARM Rogue Containment Triggered	Rogue containment triggered.
Radio ARM Decreased Power	Radio output power decreased to *[EIRP]* dBm.
Radio ARM Increased Power	Radio output power increased to *[EIRP]* dBm.
Radio RADAR Turn Off Radio	Radar detected radio up.
Radio ARM Turn On Radio	Radar detected radio down.
Radio ARM Channel Quality Threshold Exceeded	Radio channel quality threshold exceeded
Radio ARM Dynamic BW	Channel width set to channel [*Channel*].
Radio ARM Interference CCA	Channel width set to channel [*Channel*].
Radio Freeze	Radio stopped service.
Radio Un-Freeze	Radio resumed service.
Mesh Link Up	Mesh link established to Portal [*Portal Device MAC*].
Mesh Link Down	Mesh link to Portal [*Portal Device MAC*] is down.
VPN IPSec Tunnel Up	VPN IPSec Tunnel to Gateway peer [*Peer Device Hostname*] ([*Peer Device IP*]) is up.
VPN IPSec Tunnel Down	VPN IPSec Tunnel to Gateway peer [*Peer Device Hostname*] ([*Peer Device IP*]) is down.
VPN GRE Tunnel Up	VPN L3 GRE Tunnel to Gateway peer [*Peer Device Hostname*] ([*Peer Device IP*]) is up.
VPN GRE Tunnel Down	VPN L3 GRE Tunnel to Gateway peer [*Peer Device Hostname*] ([*Peer Device IP*]) is down.
WLAN SSID Scheduled Active	SSID [*SSID*] scheduled activation.
WLAN SSID Scheduled De-active	SSID [*SSID*] scheduled deactivation.

Supported Client Events

Aruba Central provides an **Events** dashboard for viewing the events triggered from access points (APs), clients, switches, and gateways.

The following table lists the client events that are supported in Aruba Central:

Table 321: *Client Events*

Event	Description
Client 802.11 Association Reject	802.11 Association rejected for client [*Client MAC*] to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client 802.11 Disassociation to Client	802.11 Disassociation sent to client [*Client MAC*] from BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client 802.11 Disassociation from Client	802.11 Disassociation received from client [*Client MAC*] associated to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client 802.11 Authentication Failure	802.11 Authentication failed for client [*Client MAC*] on BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client 802.11 De-authentication to Client	De-authentication sent to client [*Client MAC*] from BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client 802.11 De-authentication from Client	De-authentication sent from client [*Client MAC*] associated to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Roaming Success	Client [*Client MAC*] associated to BSSID [*From BSSID (roamed from)*] on channel [*From Channel (roamed from)*] of AP hostname [*From Device Hostname (roamed from)*] roamed successfully to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client MAC Authentication Reject	MAC Authentication failed for client [*Client MAC*] to Radius Server [*Radius Server IP*] through BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client 802.1x Radius Reject	802.1x Radius Reject received for client [*Client MAC*] on BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client 802.1x Radius Timeout	802.1x Radius Timeout occurred for client [*Client MAC*] on BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Captive Portal Authentication Failure	Captive Portal failure occurred for client [*Client MAC*] associated to BSSID [*BSSID*] of AP hostname [*Device Hostname*].
Client EAP Failure	EAP failure occurred for client [*Client MAC*] associated to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].

Event	Description
Client EAP Timeout from Client	EAP response from client [*Client MAC*] associated to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*] timed out.
Client VoIP Call Start	VoIP call initiated from station [*Source Client Name*] ([*Source Client IP*]) to station [*Destination Client Name*] ([*Destination Client IP*]) on AP hostname [*Device Hostname*].
Client VoIP Call Stop	VoIP call terminated from station [*Source Client Name*] ([*Source Client IP*]) to station [*Destination Client Name*] ([*Destination Client IP*]) on AP hostname [*Device Hostname*].
Client DHCP Acknowledged	DHCP acknowledgment received from DHCP server [*DHCP Server IP*] for client [*Client MAC*] ([*Client IP*]) associated to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client DHCP Not Acknowledged	DHCP NACK to DHCP server [*DHCP Server IP*] from client [*Client MAC*] ([*Client IP*]) associated to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client DHCP Declined	DHCP declined from DHCP server [*DHCP Server IP*] for client [*Client MAC*] ([*Client IP*]) associated to BSSID [*BSSID*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client DNS Failure	DNS failure to [*Domain Name*] detected for client [*BSSID*] on BSSID [*BSSID*] of AP hostname [*Device Hostname*].
Client DHCP Timeout	DHCP request to DHCP server [*DHCP Server IP*] from client [*Client MAC*] timed out.
Client Blacklisted	Blacklisted client [*Client MAC*] on AP hostname [*Device Hostname*] for SSID [*SSID name*].
Client Fast Roaming Failure	Fast Roaming failed for client [*Client MAC*] with roaming type [*Roaming Type*] on AP hostname [*Device Hostname*].
Client Roaming Success	Client [*Client MAC*] roamed successfully to SSID [*SSID name*] on channel [*Channel*] of AP hostname [*Device Hostname*].
Client Match Steer Attempt	Client match attempted a [*Steer Type*] using [*Steer Mode*] for client [*Client MAC*] from radio BSSID [*From BSSID*] to radio BSSID [*To BSSID*] with result: [*Steer Result*].
Client Match Steer Reject	Client match attempted a [*Steer Type*] using [*Steer Mode*] for client [*Client MAC*] from radio BSSID [*From BSSID*] to radio BSSID [*To BSSID*] which was rejected by the client with reason code [*802.11v Move Result*].
Client Match Steer Wrong Destination	Client match attempted a [*Steer Type*] using [*Steer Mode*] for client [*Client MAC*] from radio BSSID [*From BSSID*] to radio BSSID [*To BSSID*] which resulted in the client moving to a different radio BSSID [*Destination Radio BSSID*].

Reports

The Aruba Central dashboard enables you to create various types of reports. To create a report, you must have Read/Write or Admin access for Aruba Central.

The Reports feature is available for Foundation license of APs, switches, and gateways.

Viewing the Reports Page

To view the **Reports** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.

The **Reports** page has the following sections:

- **Browse**—Allows you to browse through the generated reports.
- **Manage**—Allows you to manage the scheduled reports.
- **Create**—Allows you to create and schedule a report.

This section includes the following topics:

Report Categories

The following list provides information about the types of report under each category of the report. For information about how to configure the Context, Transport Type, Report Order, Top N Count, Classify On, Report Subtype, Report Period, Recurrence, and Report Information for a report, see Report Configuration Options

- **Clients**
  - **Client Inventory**—The Client Inventory report provides information about the total number of clients and the type of connected networks that assists the administrators in planning for scalability and to evaluate the deviations from the baseline. You can select the context of the report from the available options:
    - **Groups**
    - **Labels**
    - **Sites**
  - **Client Session**—The Client Session report monitors the sessions of all the users in the network and provides insights related to usage analysis and connectivity patterns. In the Central 2.5.3 release, the report also projects the WLAN user experience to assist the user in measuring the efficiency of the deployed networks. You can select the context of the report from the available options:

- **Groups**
- **Labels**
- **Sites**

- **Client Usage**—The Client Usage report displays the client usage and client connectivity details to assist the administrator in planning the expansion of the network and the application requirements. You can select the context of the report from the available options:
  - **Groups**
  - **Labels**
  - **Sites**
- **Guest**—Displays the guests and guest session details for all the SSIDs for a specific time period. The Guest report provides visibility for all the users associated to the cloud guest network that assists the user in conducting campaigns and also provides analytics of the guest users in the network.

Guest report does not support location based filtering for any selected device group, site, or label to ensure end user privacy protection.

- **Summary**—Displays the details about the wireless and wired clients, and the usage details of the wireless and wired clients over a time period of the last one year (except the current date). The Summary report assists the user in measuring the Key Performance Indicator (KPI) trends for the last one year that aids the user in planning for scalability.
  In the **Summary** report, you can choose to generate a report from **Trends** such as **Unique clients per day**, **Clients per SSID**, **Unique client sessions per day**, **Average client sessions per day**, **Average clients per day**, and **Usage over time**. The **Average clients per day** is the number of concurrent users at a given time (updated every five minutes). **Unique clients per day** is the total number of clients that were seen for that day. For example, consider a scenario where four clients were connected in a day, and after every hour, one client disconnected and another was connected. Then, the count for **Average clients per day** was four and **Unique clients per day** was 27 (3+24 =27).
  You can further chose to generate a report form **Top N Widgets** such as **Top clients by usage**, **Top OS by usage**, **Top APs by usage**, **Bottom APs by usage**, **Top sites by WLAN usage**, and **Bottom sites by WLAN usage**. The **Top sites by WLAN usage** and **Bottom sites by WLAN usage** options are only available under **Top N widgets** section, when you select **All** in the **Groups** context level. You can choose **Top 5**, **Top 10**, **Top 25**, or **Top 50** from the **Show Results** drop-down list to view the data for top 5, top 10, top 25, or top 50 widgets. You can select the context of the report from the available options:
  - **Groups**
  - **Label**
  - **Site**

The **Summary** report is supported from Aruba Central 2.5.2 onwards and the data is available only after an upgrade to version 2.5.2 or later. Data prior to the 2.5.2 upgrade is not available in the report.

- **Infrastructure**
  - **Capacity Planning**—The Capacity Planning report provides information about the subscription utilization and most used devices in the network that assists the administrator to add more devices in a specific location to enhance the scalability and to increase the uplink capacity of the switching infrastructure. You can select the context of the report from the available options:

    - **Groups**
    - **Label**
    - **Site**
- **Configuration & Audit**—Displays the configuration and audit logs for all the device management, configurations, and user management events triggered in Aruba Central. The Configuration & Audit report aids the user in tracking the configuration changes in the network that assists in tracking the deviations from the IT polices. The context available for this report is only **Groups**.
- **Infra Inventory**—Displays the inventory and subscription information for the devices that are online or offline during a specific time period. The Infra Inventory report aids the user in maintaining a record of the infrastructure devices and validate the firmware versions compliance. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
- **Network**—Displays the summary details of the network that aids the user in measuring the availability of every device in the network and projects compliance to the defined Network SLAs. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
- **New Infra Inventory**— The New Infra Inventory report provides detail of the infrastructure devices added in a time period that assists the administrator in validating the network deployment progress against the deployment schedule. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
- **Resource Utilization**—Displays the details of the infrastructure devices that exceeded the configured thresholds on a daily, weekly, and monthly basis in the report. The Resource Utilization report provides information about the devices with high CPU and memory utilization that assists the administrator in evaluating the deviations against the device utilization baselines. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
- **RF Health**—The RF Health report provides detail of the radios of an access point with poor health indicators and assists the administrator in evaluating the deviation from the network baselines. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
- **Switch Capacity Planning**—The Switch Capacity Panning report provides an user with insights on the used and unused ports usage along with power consumed by clients that helps the user plan for scalability. You can select the context of the report from the available options:

- **Groups**
- **Label**
- **Site**

The data for this report is generated only after you upgrade to Aruba Central version 2.5.2. You can view or generate the report for 1, 7, 30, and 90 days after upgrading to Aruba Central version 2.5.2.

- **WAN Availability**—The report displays the WAN overlay and underlay availability information. You can select the transport type for the report from the available options:
  - **Overlay**
  - **Underlay**
- **WAN Inventory**—Displays a list of Branch Gateways onboarded. The report is segregated by ArubaOS software version.
- **WAN Compliance**—Displays the worst performing or best performing links according to the SLA compliance violations.
- **WAN Transport Health**—Displays the top N links with probed values. You can select the transport type for the report from the available options:
  - **Overlay**
  - **Underlay**
- **WAN Utilization**—Displays WAN bandwidth utilization information for Underlay, Overlay, and overall network. You can select the transport type for the report from the available options:
  - **Overlay**
  - **Underlay**
- **WAN Web Content Classification**—The WAN Web Content Classification report provides information regarding the URLs, IP reputations, and geo-locations that aids an user in implementing policy enforcements. You can select the transport type for the report from the available options:
  - **Internet**
  - **VPN**

- **Security Compliance**
  - **PCI Compliance**—Displays the PCI Compliance result with the number of violations and the PCI DSSv3.2 for an Instant AP. The PCI compliance report automatically executes some of the test cases of the PCI DSS test requirements and projects compliance results that reduces the manual efforts in validating the test cases. The context available for this report is only **Groups**.
  - **RAPIDS**—Displays the details of all the rogue devices in the network that assists the administrator about the possible threat and provides essential information needed to locate and manage the threat. You can select the context of the report from the available options:
    - **Groups**
    - **Label**
    - **Site**
  - **Security Compliance**—Displays the details of the rogue APs and wireless intrusions detected in the network that assists the administrator in validating the compliance to the security guidelines. You can select the context of the report from the available options:

    - **Groups**
    - **Label**
    - **Site**
- **Applications**
    - **AppRF**—Displays the application usage report for a specific device group in the network. The AppRF report provides information about the application usage patterns and the web usage patterns in the network that assists the administrators in evaluating the deviations from the data usage patterns. The context available for this report is only **Groups**.

Important Points to Note

- When you select **Custom range** under **Report Period**, the **Every day**, **Every week**, and **Every month** options are not available under **Recurrence**.
- For the **Client Session** report, the **Show Detailed Report** option is available only for a selected site. Selecting this option restricts the **Report Period** to **Last Day** and **Custom Range** only. Selecting custom range enables you to select a one day time range from the particular day till the last seven days only.
- In the **Infra Inventory** report, select the **Offline** option in the **Device Inventory** section to generate the report with details of the devices that are offline. The PDF displays the distribution of inactive devices by the device type and CSV displays the list with additional information.
- In the **Configuration and Audit** report with local overrides details, the count for device override is available only for the **Groups** context. To include local overrides column in the **Configuration and Audit** report, select the **Show Override** option in the **Audit Report** section.
- When a new switch connects to Aruba Central, the **Last Used at** and **Unused Since (Days)** columns value is displayed as **NA** for all the ports that are down in the .csv file, that is created for the Switch Ports in the **Switch Capacity Planning** report. When a port continues to be in a down state, the **Last Used at** and **Unused Since (Days)** columns value will be displayed as **NA** for the time period of the generated report.

Report Configuration Options

Aruba Central allows you to create various types of reports based on your network requirements. For information about each type of report, see Report Categories.

The types of report categories supported by Aruba Central are:

- **Clients**
- **Infrastructure**
- **Security Compliance**
- **Applications**

Sections in Reports

Context

Allows you to select the context for which you want to create the report. Select one of the available options from the following:

- **Groups**—Allows you to generate the report for the devices attached to a group.
    - **Filter By**—Select either **Roles** or **SSIDs** to filter the devices within the selected group(s) based on their roles or SSIDs.

- **Roles**—Select a device from the list of roles for which you want to generate the report.
- **SSIDs**—Select a device from the list of SSIDs for which you want to generate the report.
- **Trends**—Select a trend or multiple trends from the list for which you want to generate the report. Select **All** to generate the report for all the available trends in the list. Allows you to generate the report to view the data for one year for trends such as **Unique clients per day**, **Clients per SSID**, **Unique client sessions per day**, **Average client sessions per day**, **Average clients per day**, and **Usage over time**.
- **Top N Widgets**—Select a widget or multiple widgets from the list for which you want to generate the report. Select **All** to generate the report for all the available widgets in the list. Allows you to generate the report to view the data for one year for widgets such as **Top clients by usage**, **Top OS by usage**, **Top APs by usage**, **Bottom APs by usage**, **Top sites by WLAN usage**, and **Bottom sites by WLAN usage**.
- **Audit Report**—Select **Show Overrides** to include the override data of the devices within the group in the **Configuration & Audit** report.
- **Device Inventory**—Select **Offline** to include the details of the offline devices within the group in the **Infra Inventory** report.
- **Threshold**—Select the **Same as AP threshold** check-box to set the same threshold as the AP. Allows you to set the percentage of the CPU and the memory thresholds for APs, switches, and gateways within the group.
- **Criteria**—Select **Used/Unused Ports** and/or **PoE** to include the data regarding the used ports, unused ports, and/or PoE usage in the **Switch Capacity Planning** report. When you select **Used/Unused Ports**, the **Switch Port Summary** report is generated. When you select **PoE**, the **Switch PoE Usage Summary** report is generated. The individual port details are available only in the .csv export of the **Switch Port Summary** report.
- **Subnet/SSID List**—Select **Subnet/SSID List** to generate the report based on the CDE SSIDs or CDE subnets.
- **CDE SSIDs**—Select an SSID from the list for which you want to generate the report.
- **CDE Subnets**—Select a subnet from the list for which you want to generate the report.

- **Label**—Allows you to generate the report for the devices attached to a label.
  - **Label**—Select a label or multiple labels from the list for which you want to generate the report. Select **All** to generate the report for all the available labels in the list. The search bar allows you to filter a label from the list.
- **Site**—Allows you to generate the report for the devices attached to a site.
  - **Site**—Select a site or multiple sites from the list for which you want to generate the report. Select **All** to generate the report for all the available sites in the list. The search bar allows you to filter a site from the list.
  - **Detailed Report**—Select **Show Detailed Report** to include the client session details for each client within the site in the **Client Session** report.

Transport Type

Select one of the available options from the following:

- **Overlay**—Select **Overlay** you to include the WAN overlay availability information in the report.
- **Underlay**—Select **Underlay** to include the WAN underlay availability information in the report.
- **Internet**—Select **Internet** to include details of WebCC over the internet in the report.
- **VPN**—Select **VPN** to include details of WebCC over the VPN tunnel in the report.

Report Order

Select either **Best Performing** or **Worst Performing** to include the details of the best or worst performing WAN interfaces in the report.

Top N Count

Enter the range in the **Top N** for the number of results you want the include in the report. The Top N range should be between 1 to 250.

Classify On

Select either **web category** or **web reputation** to include data about the total usage of each device based on the web reputation or web category in the report.

Report Subtype

Select either **summary report** or **blocked urls report** to include the summary or blocked urls details in the report. A blocked URLs report will contain blocked URL Information along with the number of attempted session count.

Report Period

Specify the time period for which you want to create the report. Select one of the available options from the following:

- **Last day**—Select **Last day** to generate the report for the last day.
- **Last 7 days**—Select **Last 7 days** to generate the report for the last 7 days.
- **Last 30 days**—Select **Last 30 days** to generate the report for the last 30 days.
- **Last year**—Select **Last year** to generate the Summary report for the last year.
- **Custom range**—Select **Custom range** to generate the report for a time period within the last 90 days. When you select **Custom range**, the **Date Range** option is displayed. In the **Date Range** window, select a time period within the last 90 days for which you want to create the report.

The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

Recurrence

Select **Recurrence** to schedule the report. Select one of the available options from the following:

- **One time (Now)**—Select **One time (Now)** to schedule the report generation once for the current time.
- **One time (Later)**—Select **One time (Later)** to schedule the report generation once for a later time. When you select **One time (Later)**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the date for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every day**—Select **Every day** to schedule the report generation for every day. When you select **Every day**, the **Run Time** option is displayed. In the **Run Time** window, select the time for which you want to schedule the report.
- **Every week**—Select **Every week** to schedule the report generation for every week. When you select **Every week**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the day for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.

- **Every month**—Select **Every month** to schedule the report generation for every month. When you select **Every week**, the **Run Day** and **Run Time** options are displayed. In the **Run Day** window, select the date from the **Day** drop-down list for which you want to schedule the report. In the **Run Time** window, select the time for which you want to schedule the report.

Report Information

Allows you to add a title, an email address, and specify the format of report to receive the email. Enter the following information:

- **Report title**—Enter the title of the report.
- **Email to**—Enter an email address to receive the report over an email.
- **Email Format**—Select **PDF** and/or **CSV** to specify the format of the report to receive the email.

Previewing a Report

Aruba Central allows you to preview a type of report prior to generating the report. The preview of the report displays dummy values.

To preview the report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The Reports page is displayed in the **Summary** view.
3. Click **Create**.

   The **Reports** page is displayed in the **List** view.
4. Hover over a report and then click **Preview** to preview the report.

The report preview provides the following details:

- **Report Name**—Name of the report.
- **Report Type**—Type of the report.
- **Date Run**—Time when the report was last run.
  - **Group/Device**—The group or device for which the report was run.

In the preview of the report, the **PDF**, **CSV**, and **Email to** icons are dummy icons.

For more information about the reports under each category, see Report Categories.

Creating a Report

Aruba Central allows you to generate a report for devices associated with a group, multi-group, label, or a site.

Although your page view is set to a specific group, site, or label, you can create reports for a different group, site, or a label. However, if your page view is set to an Instant Access Point (IAP) cluster or switch, you can schedule a report only for that IAP cluster or switch.

To create a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Create**.

   The **Reports** page is displayed.
4. Select the type of report you want to create and then click **Next**.
5. Based on the type of report you select, a few options are displayed. Select one of the available options to set the context of the report. For example, for the **Client Inventory** report, select one of the available options under **Context**, which is either **Groups**, **Labels**, or **Sites**.
   - **Groups**—Select **Groups** to generate reports for the devices attached to a group.
   - **Labels**—Select **Labels** to generate reports for the devices attached to a label.
   - **Sites**—Select **Sites** to generate reports for the devices attached to a site.

   Based on the selected context, further options are displayed to create a report with more details. For more information, see Report Configuration Options.
6. Click **Next**.

   The **Report Period** option is displayed.
7. Under **Report Period**, select one of the available options to create a report for the last day, last 7 days, last 30 days, last year, or for a custom range.

The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

8. Click **Next**.

   The **Recurrence** option is displayed.
9. Under **Recurrence**, select one of the available options to schedule a report for the current time, later time, every day, every week, or every month.
10. Under **Report Information**, enter the title of the report and an email address.
11. Select **PDF** and/or **CSV** to specify the format of the report to receive the email.
12. Click **Generate**.

    The report gets generated and is displayed under the **Scheduled Reports** table. The report gets emailed as an attachment to the email address provided.

Editing a Report

Aruba Central allows you to edit a report for devices associated with a group, multi-group, label, or a site.

To edit a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The Reports page is displayed in the **Summary** view.

3. Click **Manage**.

   The **Scheduled Reports** table is displayed in the **Config** view.
4. In the **Scheduled Reports** table, select a report and then click the edit icon.

   The report that you want to edit is auto-selected in the **Reports** page.
5. Click **Next**.
6. Based on the type of report you select, a few options are displayed. Select one of the available options to set the context of the report. For example, for the **Client Inventory** report, select one of the available options under **Context**, which is either **Groups**, **Labels**, or **Sites**.
   - **Groups**—Select **Groups** to generate reports for the devices attached to a group.
   - **Labels**—Select **Labels** to generate reports for the devices attached to a label.
   - **Sites**—Select **Sites** to generate reports for the devices attached to a site.

   Based on the selected context, further options are displayed to create a report with more details. For more information, see Report Configuration Options.
7. Click **Next**.

   The **Report Period** option is displayed.
8. Under **Report Period**, select one of the available options to create a report for the last day, last 7 days, last 30 days, last year, or for a custom range.

The **Custom range** for the Summary report is available for the last one year, except the current date (today). All other reports are available for 90 days.

9. Click **Next**.

   The **Recurrence** option is displayed.
10. Under **Recurrence**, select one of the available options to re-schedule a report for the current time, for a later time, every day, every week, or every month.
11. Under **Report Information**, edit the title of the report and an email address.
12. Select **PDF** and/or **CSV** to specify the format of the report to receive the email.
13. Click **Generate**.

    The report gets generated and is displayed under the **Scheduled Reports** table. The report gets emailed as an attachment to the email address provided.

Viewing the Generated Report

To view a generated report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The Reports page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.
4. In the **Generated Reports** table, click a report name listed under **Title**.

   The report details are displayed.

The **Generated Reports** table provides the following information:

- **Title**—Name of the report. Click to filter the report based on the name of the report.
- **Date Run**—Time when the report was last run.
- **Group/Device**—The group or device for which the report was run.
- **Label/Site**—The label or site for which the report was run.
- **Type**—Type of report. Click to filter the report based on the type of the report. Click to select a type of report from the drop-down list.
- **Created By**—Email address of the user who created the report.

Viewing the Scheduled Report

To view a scheduled report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Manage**.

   The **Scheduled Reports** table is displayed in the **Config** view.
4. In the **Scheduled Reports** table, click a report name listed under **Title**.

   The report details are displayed.

The **Scheduled Reports** table provides the following information:

- **Title**—Name of the report. Click to filter the report based on the name of the report.
- **Next Run**—Time when the report will run in the future.
- **Group/Device**—The group or device for which the report was run.
- **Label/Site**—The label or site for which the report was run.
- **Recurrence**—Time period of the scheduled report.
- **Type**—Type of report. Click to filter the report based on the type of the report. Click to select a type of report from the drop-down list.
- **Created By**—Email address of the user who created the report.
- **Status**—Status of the report. Click to filter the report based on the status of the report. Click to select a status of report from the drop-down list.

Downloading a Report

To download a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.

4. In the **Generated Reports** table, hover over the report you want to download.
5. Click the **PDF** or the **CSV** icon to download the report to the local system.
6. Optionally, click the **Email to** icon to generate an email attachment of the report.

Deleting a Report

To delete a report, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.
4. In the **Generated Reports** table, hover over the report that you want to delete.
5. Click the **Delete** icon.

   The **Delete Report** pop-up window is displayed.
6. Click **Yes** to delete the report.

   The selected report is deleted.

Deleting Multiple Reports

To bulk delete multiple reports, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Analyze**, click **Reports**.

   The **Reports** Reports page is displayed in the **Summary** view.
3. Click **Browse**.

   The **Generated Reports** table is displayed in the **List** view.
4. To bulk delete, select multiple reports by clicking the rows. Alternatively, press and hold the **Ctrl** key and select the reports.

   The number of selected reports is displayed in a pop-up window.
5. In the pop-up window, click the icon.

   The **Delete Report** pop-up window is displayed.
6. Click **Yes** to bulk delete the selected reports.

   The selected reports are deleted.

Viewing Audit Trail

The **Audit Trail** page shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. Additionally, the audit trail logs also shows monitoring and troubleshooting information that can be used to diagnose any Switch related issues in the network.

To view the **Audit Trail** logs perform the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group or all devices in the filter, set the filter to **Group**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
2. Under **Analyze**, click **Audit Trail**.

   The Audit Trail table is displayed with the following details:
   - **Occurred On**— Timestamp of the audit log. Use the sort option to sort the audit logs by date and time. Use the filter option to select a specific time range to display the audit logs.
   - **IP Address**—IP address of the client device.
   - **Username**—Username of the admin user who applied the changes.
   - **Target**—The group or device to which the changes were applied.
   - **Category**—Type of modification and the affected device management category.
   - **Description**—A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click to view the complete details of the event. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.

To customize the **Audit Trail** table, click the eclipses  icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Chapter 35
All Clients

The **Clients** page provides a list view of all the access point (AP), switch, or gateway clients connected to the network. You can filter clients based on the network the clients are connected to. The page displays key client information and also allows you to view a specific client detail page.

The client monitoring features in the **List** and **Summary** pages run on the Foundation license that is auto-assigned for the AP, switch, and gateway. For more information, see Aruba Central Licenses Feature Details.

For monitoring clients connected to an Aruba Switch, the client entry is displayed in the **All Clients** page only if the client is connected to one of the following supported Aruba Switches:

- Aruba 2530 Switch Series (applies to wired authenticated clients only)
- Aruba 2540 Switch Series
- Aruba 2920 Switch Series
- Aruba 2930F Switch Series
- Aruba 2930M Switch Series
- Aruba 3810 Switch Series
- Aruba 5400R Switch Series
- Aruba CX Switch Series

The clients dashboard is displayed when the filter is set to **Groups**, **Labels**, **Sites**, or **Global**. For information about all the available menu items, see The Client Dashboard.

Clients

To view the list of clients connected:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients. The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.
4. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the AP.
   - **Switch**—Displays a list of clients connected to the switch.
   - **Gateway**—Displays a list of clients connected to the gateway.
5. To filter clients based on the network to which the clients are connected, click the network type from the **Client Summary** bar:

- **All**—Displays a list of all the clients connected to the network.
- **Wireless**—Displays a list of clients connected to the wireless network. The wireless clients are denoted by the icon.
- **Wired**—Displays a list of clients connected to the wired network. The wired clients are denoted by the icon.
- **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the icon.

6. To filter the clients based on the state of connectivity, click the connectivity type from the **Client Summary** bar:
   - **Connecting**—Displays a list of client connections that are in progress.
   - **Connected**—Displays a list of clients that are successfully connected to the network.
   - **Failed**—Displays a list of all failed client connections.
   - **Offline**—Displays a list of all offline clients.
   - **Blocked** —Displays a list of all blocked clients.

The **Clients** table lists the details of each client. By default, **All** clients is selected and the table displays the following columns: **Client Name**, **Status**, **IP Address**, **VLAN**, **Connected To**, **SSID/Port**, **AP Role**, **Gateway Role**, and **Health**. The default columns displayed is different and contextual based on AP, switch, and gateway.

Click the ellipsis icon to perform additional operations:

- **Download CSV**—Downloads the client details in the .csv file format.
- **Select All**—Selects all columns.
- **Reset Columns**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click and enter the filter criteria or select a filter criteria. For example, to search a client, click the predefined filter criteria: **Connecting Connected**, **Offline**, **Failed**, or **Blocked** from the **Client Summary** bar and in the **Client Name** column enter the name of the client. Aruba Central provides a near-instant refresh of the client status if the client is connecting or connected to an access point. For more information, see Client Status Changes.

Figure 504 *Clients—List View*

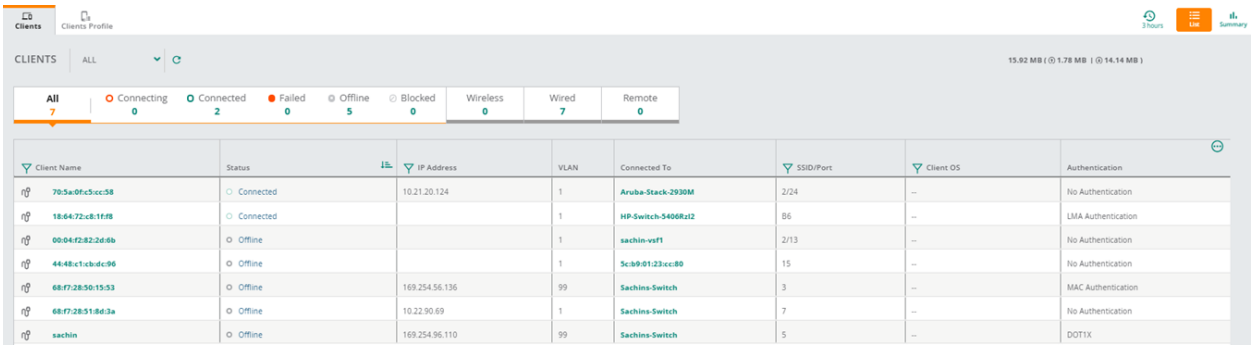


Table 322: *All Client Details*

Column Names	Applicability	Description
Client Name	■ All ■ AP ■ Switch ■ Gateway	Username, hostname, or MAC address of the client. Click the client name to view the **Summary** page.
Status	■ All ■ AP ■ Switch ■ Gateway	Client connection status. Use the filter option to view the following: ■ Connecting—Applicable only for wireless clients. ■ Connected—Applicable for all client types. ■ Offline—Applicable for all client types. ■ Failed—Applicable only for wireless clients. ■ Blocked—Applicable only for wireless clients. Hover the cursor over the status column to view a pop-up summary based on the connection status. The status summary is populated based on the status type. Each status type and the summary is described below: ■ **Connecting**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the client was last connected. ■ **Connected**: ◦ **Client name**—Name of the client. ◦ **Authentication**—Type of authentication. Displays the authentication label only for authenticated clients. ◦ **IP address**—Client IP address. ◦ **Connected Since**—Date and time at which the client was connected. ◦ **Failure Stage**—Stage of the connection where the client failed to connect. It is not applicable for the wired clients, so displayed as NA. ◦ **Health Score**—Device health. ◦ **Connected Device Port**—The device port that the wired client is connected to. ■ **Failed**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the client was last connected. ◦ **Failure Stage**—Stage of the connection where the client failed to connect. ◦ **Failure Reason**—Reason for the connection failure. ■ **Offline**: ◦ **Client name**—Name of the client. ◦ **Authentication**—Type of authentication. Displays the authentication label only for authenticated clients.

Table 322: *All Client Details*

Column Names	Applicability	Description
		◦ **IP address**—Client IP address ◦ **Connected Since**—Date and time at which the client was connected. ◦ **Last Seen Time**—Date and time the client was last connected. ◦ **Failure Stage**—Stage of the connection where the client failed to connect. ◦ **Connected Device Port**—The device port that the wired client is connected to. ■ **Blocked**: ◦ The values available for clients that are blocked when in failed status, offline status, dynamically blocked, or if a new client is blocked is as follows: • **Client name**—Name of the client. • **Last Seen Time**—Date and time the client was last connected. ◦ The values available for clients that are blocked when in connected status is as follows: • **Client name**—Name of the client. • **Authentication**—Type of authentication. Displays the authentication label only for authenticated clients. • **IP address**—Client IP address • **Connected Since**—Date and time at which the client was connected. • **Last Seen Time**—Date and time the client was last connected.
IP Address	■ All ■ AP ■ Switch ■ Gateway	IP address of the client.
VLAN	■ All ■ AP ■ Switch ■ Gateway	VLAN of the device to which the client is connected.
Connected To	All	AP name, Switch name, or Gateway name. This is the first layer 2 hop for the client. If the device does not have a name, the MAC address is displayed.
AP Role	■ All ■ AP	Role assigned by the AP.
Gateway Role	■ All ■ Gateway	Role assigned by the Aruba Gateway.

Table 322: *All Client Details*

Column Names	Applicability	Description
Health	■ All ■ AP	Client health. The value can be one of the following: ■ **Poor**—0-30 ■ **Fair**—31-70 ■ **Good**—71-100
SSID/Port	■ All ■ AP ■ Switch ■ Gateway	Displays the SSID for wireless clients and the port number for wired clients. The column title displays **SSID** and **Port** interchangeably based on the device filters. For APs, the column title displays **SSID**. For switch and gateway, the column title displays **Port**.
Insights	■ All ■ AP	The total number of AI insights generated for the client.
Switch Role	■ All ■ Switch	Role assigned by the Aruba switch.
Failure Stage	■ All ■ AP	Failure status of the client that failed to connect. The failure reasons could be: ■ Association failure ■ MAC authentication failure ■ 802.1X authentication failure ■ Key exchange failure ■ DHCP failure ■ Captive Portal failure
Group Name	■ All ■ AP ■ Switch ■ Gateway	Displays the name of the group that the device is connected to. The **Connected To** column displays the device name that the client is connected to.
Site Name	■ All ■ AP ■ Switch ■ Gateway	Displays the name of the site that the device is connected to. The **Connected To** column displays the device name that the client is connected to.
MAC Address	■ All ■ AP ■ Switch ■ Gateway	MAC address of the client.
Hostname	■ All ■ AP ■ Gateway	Host name of the client.
User Name	■ All ■ AP ■ Switch	Username of the client.

Table 322: *All Client Details*

Column Names	Applicability	Description
	■ Gateway	
Key Management	■ All ■ AP	Security mode used by the client.
Authentication	■ All ■ AP ■ Switch ■ Gateway	Authentication type used by the client to connect with the device.
Global Unicast IPv6 Address	■ All ■ AP ■ Gateway	When the IPv6 address is present for a client, you can view its Global Unicast IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Link Local IPv6 Address	■ All ■ AP ■ Gateway	When the IPv6 address is present for a client, you can view its Link Local IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Capabilities	■ All ■ AP	Client 802.11 capabilities.
Usage	■ All ■ AP ■ Switch ■ Gateway	Total data usage for the selected time period.
Last Seen Time	■ All ■ AP ■ Switch ■ Gateway	Date and time when the client was last seen.
Connected Since	■ All ■ AP ■ Switch ■ Gateway	Date and time since when the client was connected.
AP Name	■ All ■ AP	Name of the AP.
AP Mac Address	■ All ■ AP	MAC address of the AP.
Channel/Band	■ All ■ AP	Last connected channel and band.
Switch Name	■ All	Name of the switch.

Table 322: *All Client Details*

Column Names	Applicability	Description
	▪ Switch	
Port	▪ All ▪ Switch ▪ Gateway	Port number of the switch.
Gateway Name	▪ All ▪ Gateway	Name of the Aruba Gateway.
Tunneled	▪ All ▪ AP ▪ Switch ▪ Gateway	Tunnel mode applicable for the Aruba Gateway managed WLAN, UBT, or PBT client.
Segmentation	▪ All ▪ AP ▪ Switch ▪ Gateway	Type of segmentation. The type of segmentation can be: ▪ None ▪ UBT ▪ PBT ▪ Underlay ▪ Overlay **NOTE:** To view the details about dynamic segmentation, a gateway must be licensed in Aruba Central and connected to the switch.
Client OS	▪ All ▪ AP ▪ Gateway	Displays the operating system that the device runs on. For example, if the client category is Computer and the client family is Windows, the client OS can be Windows or Windows 8/10. For more information, see Classifying Clients.

Client Overview

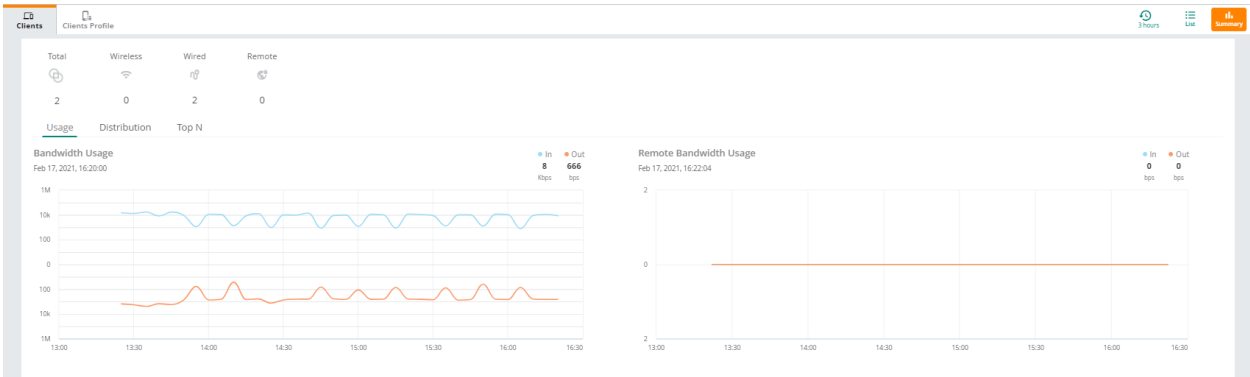
The **Clients** page displays the details of clients connected to the devices in Aruba Central and their connectivity status.

To view the clients overview page, perform the following steps:

1. In the **Network Operations** app, use the filter bar to select a group, label, site, or a device.
2. Under **Manage**, click **Clients**. The All Clients overview page is displayed.
3. Click the Summary icon to view the client overview page.

The overview page displays the total number of clients, usage, and the application usage by the clients connected to the wired, wireless, and remote networks.

Figure 505 *Clients—Summary Page*



The following table describes the information displayed in each section.

Table 323: *Client Overview Page*

Data Pane Content	Description
Time Range Filter	By default, the graphs on the **Clients** page are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months. However, the Distribution data (Client OS) under the **Distribution** tab does not honor the time range you selected in the time range filter.
Total	Displays the total number of clients.
Wireless	Displays the total number of clients connected to wireless network.
Wired	Displays the total number of clients connected to the wired network.
Remote	Displays the total number of remote clients connected through VPN.
Usage	Displays the **Bandwidth Usage** and **Remote Bandwidth Usage** of the incoming and outgoing throughput traffic for all the clients and remote clients during a specific time range in kilobits per second (Kbps). The graph will not show any data for the clients that are connected to the network for less than two hours.
Distribution	Displays the type of client device connected to the wireless network.
Top N	Displays a list of clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. The **Top Clients by Usage** table displays data only for the clients that are connected to the network for a total duration of two or more hours.

Client Status Changes

The **Clients** page provides a list view of all the clients connected to the network. You can filter clients based on the network the clients are connected to. The page displays key client information and also allows you to navigate to a specific client detail page. For more information about clients, see All Clients.

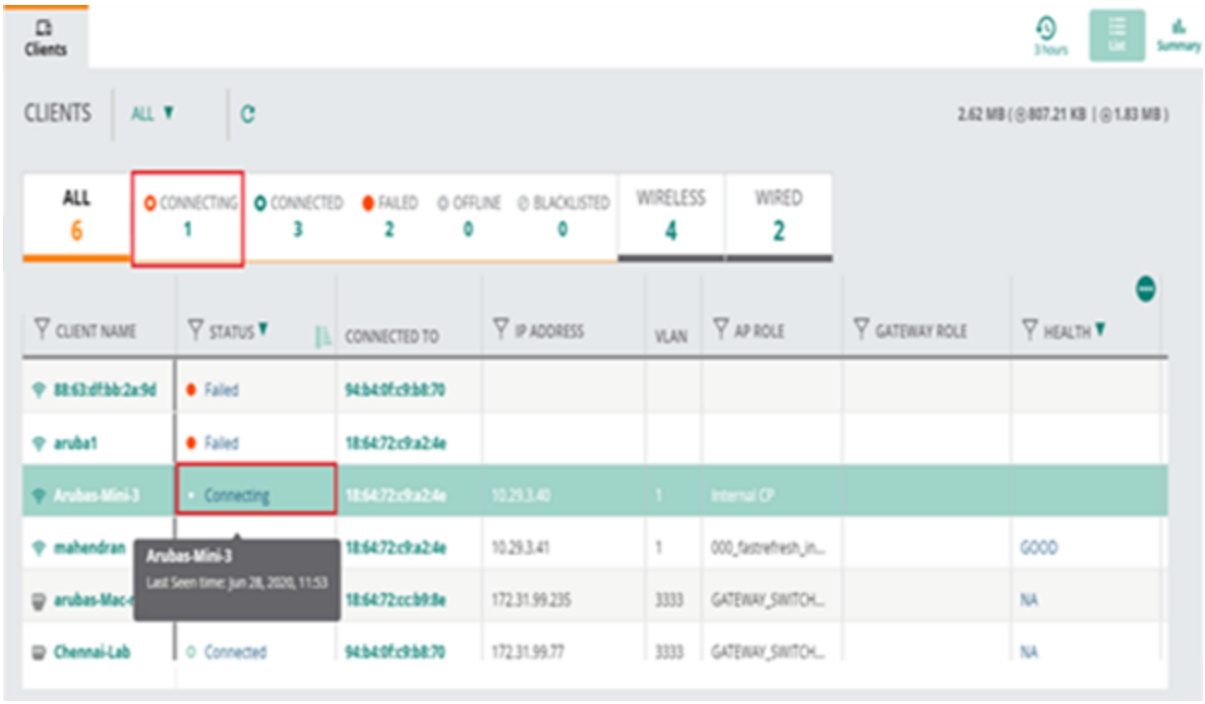
Aruba Central provides a near-instant refresh of the client status if the client is connecting or connected to an access point. The access point must be running 8.6.0.5 or a later version and 10.1.0.0 or a later version.

If the client connection is in progress, the status changes to **Connecting** and the client appears in Aruba Central within 35 seconds after it is connected. If the client goes offline, the status is updated to **Offline** in the **Clients** page within 50 seconds.

Hover the cursor over **Connecting** in the **Status** column to view the following details:

- Name of the client
- Date and time the client was last seen

Figure 506 *Connecting Clients*



To view the clients page, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The clients page is displayed in **List** view. By default, the **Clients** table displays all clients and the list of clients is populated for a time range of 3 hours.
3. To filter the clients based on connectivity status, click the connectivity type from the **Client Summary** bar:
   - **Connecting**—Displays a list of client connections that are in progress.
   - **Connected**—Displays a list of clients that are successfully connected to the network.
   - **Failed**—Displays a list of all failed client connections.
   - **Offline**—Displays a list of all offline clients.
   - **Blocked**—Displays a list of all blocked clients.

Clients > Wireless Client > Overview

The **Clients** page displays the number of clients connected to the wireless and wired networks. By default, the **Clients** page displays a unified list of clients for the selected group, label, site or device. The wireless

client overview page displays the client summary details, AI Insights, Location, and client sessions details for the selected client.

The wired client shows up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

The section includes the following topics:

- Viewing Clients Connected to Wireless Networks
- Overview
- Applications
- Live Events
- Events
- Tools

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
5. Enter the client name in the **Client Name** column and then click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details.

For a visual representation of the procedure, click here.

Overview

The wireless client overview tab displays the wireless client summary, AI insights, location, sessions, and profile details for each client.

Wireless Client Health Bar

The client heath bar displays the client connection, device health, and transmission rate along with name of the device the client is connected to. For more information, see The Health Bar.

The **Health** bar displays the following information:

Table 324: *Wireless Client Health Bar*

Field	Description
Connection status icon	Displays the icons with the connection status of the client. Connection status is updated immediately on state change. The available statuses are: ■ **Connecting**—Displays a list of client connections that are in progress. ■ **Connected**—Displays a list of clients that are successfully connected to the network. ■ **Failed**—Displays a list of all failed client connections. ■ **Offline**—Displays a list of all offline clients. ■ **Blocked**—Displays a list of all blocked clients.
Device Health	Signal strength of the client device. The signal strength value is displayed in percentage: ■ 0-30—Poor ■ 31-70—Fair ■ >71—Good
Signal Quality	SNR for the client as measured by the AP. The SNR value is displayed in decibels: ■ 0-20—Poor ■ 21-35—Fair ■ >35—Good
Tx | Rx Rate	Data transmission and reception rate.
Connected To	Name of the AP that broadcasts the SSID to which the client is connected. Click the name of the AP to view the device details page.
Refresh icon	Restarts the **Live Health Bar** session. This icon appears only after 15 minutes of pinning the **Health Bar** to the **Client Details** page and it is called as the **Live Health Bar** because the data is updated every 5 seconds. For more information, see Client Live Monitoring.

Summary

The wireless **Client Details** page displays the information about the type of data path that the client uses, the network and connectivity, and basic client details such as IP address of the client, type of encryption, and so on. The client details page refreshes automatically to display real time data and graphs. To refresh the page manually, click the refresh icon.

The following table describes the information displayed in the sections:

Table 325: *Wireless Client Details*

Section	Description
Data Path	Displays the data path of the client in the network. Click the AP icon to view the AP details page. The data path can be one of the following: ■ **Client** > **SSID** > **AP** ■ **Client** > **SSID** > **AP** > **Switch** ■ **Client** > **SSID** > **AP** > **Switch** > **Gateway** ■ **Client** > **SSID** > **AP** > **Gateway**
Client	Displays the following information: ■ **Username**—User name of the client. ■ **Hostname**—Hostname of the client.

Table 325: *Wireless Client Details*

Section	Description
	■ **Client Type**—Type of the client, wireless or wired. ■ **IP Address**—IP address of the client. ■ **MAC Address**—MAC address of the client. ■ **Global Unicast IPv6 Address**—Global unicast IPv6 address of the client. ■ **Link Local IPv6 Address**—Link local IPv6 address of the client. ■ **Client Category**—Category of the profiled device. For example, Access Points, Computer, Smart Device, VoIP phone, and so on. For details, see Classifying Clients. ■ **Client Family**—Displays the type of operating system or vendor. For example, if the client category is Computer, the client family can be Windows, Linux, or Apple Mac. For details, see Classifying Clients. ■ **Client OS**—Displays the operating system that the device runs on. For example, if the client category is Computer and the client family is Windows, the client OS can be Windows or Windows 8/10. For details, see Classifying Clients. ■ **Connected Since**—Date and time since when the client is connected. ■ **Manufacturer**—Manufacturer of the client device. ■ **Encryption**—Type of client encryption. ■ **AI Insights**—The total number of AI insights seen on the client device.
Network	Displays the following information: ■ **VLAN**—Displays the VLAN ID on which the client is connected to the AP. ■ **VLAN Derivation**—Displays the VLAN derivation method used for assigning an IP address to the client. Aruba devices can assign a static or dynamically derived IP address from a DHCP pool to the clients. ■ **AP Role**—Displays the role assigned to the client by the AP. ■ **AP Derivation**—Displays the role derivation method used for assigning a role to a client. For example, clients that authenticate successfully can be assigned a default role as per the AAA profile. ■ **Gateway Role**—Displays the role assigned to the client by the Gateway. ■ **Switch Role**—Displays the role assigned to the client by the Switch. ■ **Segmentation**—Displays the type of dynamic segmentation configured for the client. Supported values are UBT, PBT, Underlay, or Overlay. ■ **Auth Server**—Server that last authenticated the client device. The field displays the IP address of the server that performed either 802.1X or MAC authentication for the client device. If the client connects to the network through 802.1X and MAC authentication, Aruba Central displays only the IP address of the server that performed 802.1X authentication. ■ **DHCP Server**—DHCP server that last assigned IP address to the client. ■ **Tunneled**—Displays whether the client is tunneled or not. ■ **Tunnel ID**—Displays the tunnel ID the client is connected to.
Connection	Displays the following information: ■ **Channel**—Radio channel assigned to the client. ■ **Band**—Radio band on which the client is connected. ■ **Client Capabilities**—Capabilities of the client device. ■ **Client Max Speed**—Wireless link data transfer speed. ■ **LEDs on Access Point**—Enables the blinking of LEDs on the AP to identify the location. Click **Blink LED** to enable the blinking of LEDs on the AP. The default blinking time is set to 5 minutes and it stops automatically after 5 minutes. To stop the blinking, click **Stop Blinking**.

Table 325: *Wireless Client Details*

Section	Description
Throughput	Displays the incoming and outgoing throughput traffic for the client during a specific time range. By default, the graph on the **Throughput** pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the **Time Range Filter** link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months.
Health	Displays the health score and status of a wireless client. By default, the graph on the **Health** pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the **Time Range Filter** link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months. The graph is plotted against the client health and client score, where the client health is measured as **Poor**, **Fair**, or **Good** and the health score ranges between 0 to 100. The value is displayed in percentage: ■ 0-30—Poor ■ 31-70—Fair ■ >71—Good
Signal Quality	Displays the signal quality and the SNR for the wireless client as measured by the AP. The SNR value is displayed in decibels: ■ 0-20—Poor ■ 21-35—Fair ■ >35—Good
Retry Frames	Displays the percentage of Tx and Rx retries by a wireless client.
Tx/Rx Rate	Displays the data transmission and reception rate for the wireless client .
Roaming Experience	Displays the details of a roaming event and the latency of the client. When a wireless client roams between two APs, the destination AP creates an event. By default, the **Roaming Events & Latency** table displays data for the last 3 hours. To view the table for a different time range, click the **Time Range Filter** link. You can choose to view the data for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months. The **Roaming Events & Latency** displays two views, grid view and trend view. The grid view displays the following information: ■ **Date/Time**—Displays the time of occurrence of the client roaming/ association events. ■ **SSID**—The SSID to which the client is connected. ■ **Latency(ms)**—Roaming Latency in milliseconds between source and destination AP. ■ **To BSSID**—The BSSID of the destination AP. ■ **Source AP**—AP to which the client was connected. ■ **Destination AP**—AP to which the client is connected. ■ **Roaming Type**—The type of roam. ■ **Band**—Radio band on which the client is connected. ■ **RSSI(dBm)**—Received Signal Strength Indicator (RSSI) on the client, estimated measure of power level that the client is receiving from the AP. The trend view displays a chart that shows the percentage of high latency roaming events, total roaming events, and the number of high latency roaming events at a particular instance based on the value selected in the **Time Range Filter**. Clicking the chart icon brings you back to the grid view.

AI Insights

The **AI Insight** tab displays information about client performance and connectivity issues such as, excessive 2.4 GHz dwell and low SNR links. AI Insights are displayed for a selected time period based on the time selected in **Time Range Filter**. The user can select 3 hours, 1 week, 1 day, or 1 month to view the insight

data. AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

- Red—High priority
- Orange—Medium priority
- Yellow—Low priority

Each insight report provides specific details on the occurrences of these events for ease in debugging. For more information, see The AI Insights Dashboard.

The clients **AI Insights** page displays the following insights:

- Clients who Roamed Excessively
- Clients with High Roaming Latency
- Clients with Low SNR Minutes
- Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz
- Clients with DHCP Server Connection Problems
- Delayed DNS Request or Response
- DNS Servers Rejected High Number of Queries
- Clients with High MAC Authentication Failures
- Clients with High Wi-Fi Security Key-Exchange Failures
- Clients with High 802.1X Authentication Failures

Location

The **Location** tab displays the current physical location of the client device on the floor map.

Sessions

The client sessions page consists of the firewall session details for the client connected to an AP or a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. The **Sessions Summary** pane displays the device the client is connected to, total number of sessions, and the time stamp of when the page was last refreshed.

The **Sessions** table lists the details of each session. By default, the table displays the following columns: **Application**, **Source IP**, **Destination IP**, **Source Port**, **Destination Port**, **Action**, **Flags**, **Packets**, and **State**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each session:

Table 326: *Sessions Tab*

Section	Description
Application	Displays the list of applications.
Source IP	Displays the source IP address.
Destination IP	Displays the destination IP address.

Table 326: *Sessions Tab*

Section	Description
Protocol	Displays the communication protocol used.
Source Port	Displays the source port number.
Dest Port	Displays the destination port number.
Action	Displays the application specific action.
Flags	Displays the active flags
Packets	Displays the number of packets.
State	Displays the connection state of the application. The state can either be Denied, Active, or Inactive.
Start Time	Displays the start time.
Receive Time	Displays the receive time.
WebCC Category	Displays the WebCC category.
WebCC Reputation	Displays the WebCC reputation.
WebCC Score	Displays the WebCC score.
Application Category	Displays the application category.

Client **Sessions** is supported only if the Instant AP is running ArubaInstant 8.6.0.0 firmware version or later versions.

For details on the AP client sessions refer, Access Point > Clients > Clients. For details on the Branch Gateway client sessions refer, Gateway > Overview > Sessions.

Wireless Client > Applications

The **Applications** page provides you the client details for passive monitoring of the client connected to a wireless network.

The section includes the following topics:

- Viewing Clients Connected to Wireless Networks
- Applications
  - Visibility

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
5. Enter the client name in the **Client Name** column and then click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details.

Applications

The **Application** page displays the **Visibility** tab.

Visibility

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see Application Visibility.

Wireless Client > Live Events

The **Live Events** page consists of information to aid in troubleshooting.

The section includes the following topics:

- Viewing Clients Connected to Wireless Networks
- Live Events

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
5. Enter the client name in the **Client Name** column and then click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details.

Live Events

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. You can live troubleshoot clients connected to a wireless network. For more information on live troubleshooting a client, see Client Live Troubleshooting.

Wireless Client > Events

The **Events** page displays the details of events generated by the AP and client association.

The section includes the following topics:

- Viewing Clients Connected to Wireless Networks
- Events

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
5. Enter the client name in the **Client Name** column and then click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details.

Events

In the **Events** page, the table displays the following columns by default: **Occurred On**, **Event Type**, and **Description**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each event:

Table 327: *Events Tab*

Section	Description
Occurred On	Displays the time at which the event occurred.
Event Type	Displays the type of the event.
Description	Displays the detailed description of the event.
Device MAC	Displays the MAC address of the device.
BSSID	Displays the BSSID.

To download events into a CSV format, click the download button. Aruba Central generates the CSV report of all the events for the selected client.

You can also filter the events based on the type of events, click the **Click here for Advance Filtering**. Select the type of events from the list and click **Filter**. The events under the selected categories get listed in the **Events** table. For more information on Events, see Alerts & Events

Wireless Client > Tools

The **Tools** page aids the administrator users to monitor connections.

The section includes the following topics:

- Viewing Clients Connected to Wireless Networks
- Tools

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
5. Enter the client name in the **Client Name** column and then click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details.

Tools

The **Tools** page is automatically filtered based on the client you select. This enables network administrators to perform checks on the client and debug client connectivity issues. For more information on Tools, see Using Troubleshooting Tools.

Disconnecting a Wireless Client from an AP

To disconnect a wireless client from an online AP, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless client to open the corresponding **Client Details** page.

   If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network, enter the client name in the **Client Name** column, and click the client name.

5. From the **Actions** drop-down list, click **Disconnect from AP**.
   The client is disconnected from the AP.

The **Actions** drop-down is disabled if the AP is offline.

Blocking a Wireless Client

Blocking a client automatically denies association for wireless clients that breach a rule or policy. Client blocking excludes a client from an AP in the network. Excluding a client from the network can be performed for various reasons, few of them being security and intrusion detection.

Client blocking can be performed when the client is . Wireless clients can be excluded from the network only when the client blocking option is enabled for the SSID under the AP configuration. Client blocking can be performed manually or dynamically. Manual blocking adds the MAC address of a client to the blocked list. These clients are added into a permanent blocked list. The clients can be blocked dynamically when they exceed the authentication failure threshold or when a blocking rule is triggered as part of the authentication process. For details, see Denylisting Instant AP Clients.

To block a wireless client, ensure that the Instant AP is running one of the following firmware versions:

- Aruba Instant 8.5.0.7 firmware version or later versions
- Aruba Instant 8.6.0.3 firmware version or later versions
- ArubaInstant 10.1.0.0 firmware version or later versions

To block a wireless client, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.
   The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network, enter the client name in the **Client Name** column, and click the client name.
5. From the **Actions** drop-down list, click **Block Client**.
   The clients gets blocked from the network.

The parameter values available for a blocked client is displayed in the clients **List** view and **Client Details** pages. The available values are based on the type of blocking.

The following table consists of the available parameters corresponding to the block type.

Table 328: *Parameters of a Blocked Client*

Available Parameters	Applies To
Client Name—MAC address	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.

Table 328: *Parameters of a Blocked Client*

Available Parameters	Applies To
Status	Client blocked in the connected state.
IP Address	Client blocked in the connected state.
VLAN	Client blocked in the connected state.
Connected To	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
SSID	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
AP Role	Client blocked in the connected state.
Usage	Client blocked in the connected state.
Group Name	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
Site Name	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
MAC Address	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
Host Name	Client blocked in the connected state.
User Name—For an authenticated network	Client blocked in the connected state.
Key Management—For an authenticated network	Client blocked in the connected state.
Authentication—For an authenticated network	Client blocked in the connected state.
IPv6 (**Link Local** or **Global Unicast**)	Client blocked in the connected state.
Capabilities	Client blocked in the connected state.
Client OS	Client blocked in the connected state.
Last Seen	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
AP NAME	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
AP MAC Address	Client that is manually or dynamically blocked or blocked in the offline, failed, or connected state.
Channel	Client that is manually or dynamically blocked or blocked in the offline or failed state.
Channel/Band	Client blocked in the connected state.

Table 328: *Parameters of a Blocked Client*

Available Parameters	Applies To
Switch Name—If switch is present	Client blocked in the connected state.
Port—If switch is present	Client blocked in the connected state.
Switch Role—If switch is present	Client blocked in the connected state.
Gateway Role—If gateway is present	Client blocked in the connected state.
Gateway Name—If gateway is present	Client blocked in the connected state.

Unblocking a Wireless Client

To unblock a wireless client, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The clients overview page is displayed in **List** view. By default, the **Clients** table displays a unified list of clients.
3. To filter the Blocked clients, click **Blocked** in the **All Clients** page.

   The list of blocked clients is displayed.
4. Click the name of the wireless client to open the corresponding **Client Details** page.
5. Enter the client name in the **Client Name** column, and click the client name.
6. From the **Actions** drop-down list, click **Remove Block**.

   The client is unblocked from the network.

Client Live Monitoring

Click **Go Live** to start live monitoring of the client. Live monitoring is supported only if the Instant AP is running 8.4.0.0 firmware version. Live monitoring stops after 15 minutes. At any point, you can click **Stop Live** to go back to the historical view.

The following data gets updated every 5 seconds after you start the live monitoring:

- **Throughput**
- **Signal to Noise Ratio (SNR)**

Live Health Bar

The **Live Health Bar** is present in the **Summary** page only for a wireless client. It provides live data every 5 seconds for a session duration of 15 minutes.

To launch the Live Health Bar:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients.

4. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
5. Enter the client name in the **Client Name** column and then click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the client status icon next to the client name, the **Health Bar** pop-up appears. It displays the latest values that is updated every 5 seconds.

   The **Live Health Bar** session is for 15 minutes only, after that time period, the refresh icon appears. If you click the refresh icon, the **Live Health Bar** session restarts.
7. Click the pin icon to pin the **Health Bar** to the **Summary** page for the constant view.

The parameters available in the **Live Health Bar** are:

- **Connection status icon**
- **Device Health**
- **Signal Quality**
- **Tx | Rx Rate**
- **Connected To**

Client Live Troubleshooting

Aruba Central allows you to troubleshoot issues related to a wireless client connected to an access point or a wired client connected to a switch.

To troubleshoot a wired client connected to a switch, the switch firmware version must be 16.09.0001 or a later version and the model should be one of the following:

- Aruba 2930F Switch Series
- Aruba 2930M Switch Series
- Aruba 3810 Switch Series
- Aruba 5400R Switch Series (V3 mode)

You can troubleshoot a wired client connected to both a standalone switch or stack.

Live troubleshooting is supported only if the wireless client is connected to the access point running Aruba Instant 8.4.0.0 or a later version. You can also enable targeted packet capture during live troubleshooting and download the PCAP file if the access point is running Aruba Instant 8.6.0.5 or a later version.

Live troubleshooting can be performed on a wired client only when the access point is running Aruba Instant 8.5.0.0 or a later version.

Troubleshooting a Client

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis.

To troubleshoot a client at a site level, perform the following steps:

1. In the **Network Operations** app, set the filter to a **Site** that contains at least one device. The dashboard context for the selected site is displayed.
2. Under **Analyze**, click **Live Events**.The **Live Events** page is displayed.
3. Enter the MAC address of the client and click **Start Troubleshooting**.

To troubleshoot a wireless or wired client, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired** to filter the clients connected to the wireless or wired client respectively.
5. Enter the client name in the **Client Name** column, and click the client name.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.

The client live troubleshooting starts automatically for the selected client.

The status of the troubleshooting is displayed every minute. The troubleshooting session runs for a duration of 15 minutes. You can stop live troubleshooting at any point by clicking **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Device Name**—Displays the name of the device the client is connected to. Set the filter to select a specific device under **Site**.
- **Device Type**—Displays the type of device the client is connected to.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

Packet Capture

Aruba Central allows you to interact and launch a targeted packet capture on a client connected to a specific access point or a switch. After you start packet capture from the UI, Aruba Central notifies the access point and the switch. The default packet capture duration is 15 minutes. After you start packet capture, use the toggle button to stop packet capture, or go back to the **Client Overview** page.

For packet capture, for a wired client connected to an Aruba 5400R Switch Series (V3 mode), ensure that "no-allow v2 modules" is set for the switch.
Packet capture for stack switches works only if the client is connected to the commander of the stack.

Starting Packet Capture

You can start packet capture from the wireless or wired clients page. Packet capture can be done at a site level (wireless client only) or for a selected client.

To start packet capture at a site level, perform the following steps:

1. In the **Network Operations** app, set the filter to a **Site** that contains at least one device. The dashboard context for the selected site is displayed.
2. Under **Analyze**, click **Live Events**.The **Live Events** page is displayed.

3. Enter the MAC address of the client.

At a site level, Aruba Central does not support packet capture for a wired client connected to a switch.

4. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
5. Click **Start Troubleshooting**.

To start packet capture for a wireless or wired client, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired** to filter the clients connected to the wireless or wired client respectively.
5. Enter the client name in the **Client Name** column, and click the client name.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed. The client live troubleshooting starts automatically for the selected client.
7. Click **Stop Troubleshooting** to stop live troubleshooting.
8. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
9. Click **Start Troubleshooting** to live troubleshoot the selected client. Live packet capture starts for the selected client.

   The live troubleshooting session runs for a duration of 15 minutes. After the live troubleshooting session ends, a **Download PCAP** text appears above the live events table. Click **Download PCAP** to download the generated pcap file on your local system.

Clients > Wired Client > Overview

The overview page displays the client summary details and client sessions details for the selected wired client.

The section includes the following topics:

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network.
5. Enter the client name in the **Client Name** column, and click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details

For a visual representation of the procedure, click here.

Overview

The wired client overview tab displays the wireless client summary, AI insights, location, sessions, and profile details for each client.

Wired Client Health Bar

The wired client health bar displays the connection status, the connected port, and the name of the gateway the client is connected to. For more information, see The Health Bar.

The **Health** bar displays the following information:

Table 329: *Wired Client Health Bar*

Field	Description
Connection status icon	Displays the icons with the connection status of the client. Connection status is updated immediately on state change. The available statuses are: ■ **Connecting**—Displays a list of client connections that are in progress. ■ **Connected**—Displays a list of clients that are successfully connected to the network. ■ **Failed**—Displays a list of all failed client connections. ■ **Offline**—Displays a list of all offline clients. ■ **Blocked**—Displays a list of all blocked clients.
Connected Port	Name of the port through which the is connected.
Connected To	Name of the Gateway to which the client is connected. Click the name of the Gateway to view the device details page.

Summary

The wired **Client Details** page displays the information about the type of data path that the client uses, the network, and basic client details such as IP address, type of encryption, and so on. The client details page refreshes automatically to display real time data and graphs. To refresh the page manually, click the refresh icon.

The following table describes the information displayed in each section.

Table 330: *Wired Client Details*

Section	Description
Data Path	Displays the data path of the client in the network. Click the device icon to view the corresponding device details page. The data path can be one of the following: ■ **Client** > **Wired Profile** > **AP** ■ **Client** > **Wired Profile** > **AP** > **Switch** ■ **Client** > **Wired Profile** > **AP** > **Switch** > **Gateway** ■ **Client** > **Wired Profile** > **AP** > **Gateway** ■ **Client** > **Switch** ■ **Client** > **Switch** > **Gateway** ■ **Client** > **Gateway**
Client Info	Displays the following information: ■ **Username**—User name of the client. ■ **Hostname**—Hostname of the client. ■ **Client Type**—Type of the client device. ■ **IP Address**—IP address of the client. ■ **MAC Address**—MAC address of the client. ■ **Global Unicast IPv6 Address**—Global unicast IPv6 address of the client. ■ **Link Local IPv6 Address**—Link local IPv6 address of the client. ■ **Client Category**—Category of the profiled device. For example, Access Points, Computer, Smart Device, VoIP phone, and so on. For details, see Classifying Clients. ■ **Client Family**—Displays the type of operating system or vendor. For example, if the client category is Computer, the client family can be Windows, Linux, or Apple Mac. For details, see Classifying Clients. ■ **Client OS**—Displays the operating system that the device runs on. For example, if the client category is Computer and the client family is Windows, the client OS can be Windows or Windows 8/10. For details, see Classifying Clients. ■ **Connected Since**—Date and time since when the client was last connected. ■ **Manufacturer**—Manufacturer of the client device.
Network Info	Displays the following information: ■ **VLAN**—Displays the VLAN ID on which the client is connected to the AP. ■ **Gateway Role**—Displays the role assigned to the client by the Gateway. ■ **Switch Role**—Displays the role assigned to the client by the Switch. ■ **Segmentation**—Displays the type of dynamic segmentation configured for the client. Supported values are UBT, PBT, Underlay, or Overlay. **NOTE:** To view the details about dynamic segmentation, a gateway must be licensed in Aruba Central and connected to the switch. ■ **Tunneled**—Displays whether the client is tunneled or not. ■ **Tunnel ID**—Displays the tunnel ID the client is connected to. ■ **Port**—Displays the port type used by the client.
Throughput	Displays the incoming and outgoing throughput traffic for the client during a specific time range. By default, the graph on the **Throughput** pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the **Time Range Filter** link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months.

AI Insights

The **AI Insight** tab displays information about client performance and connectivity issues such as, excessive 2.4 GHz dwell and low SNR links. AI Insights are displayed for a selected time period based on the time selected in **Time Range Filter**. The user can select 3 hours, 1 week, 1 day, or 1 month to view the insight data. Each AI Insight type displays the AI Insight label, AI Insight graph, and AI Insight chart. Further, the Insights include categories of information present in form of tabs like, reason, band, channel, SNR and so on. These tabs are clickable and display the detailed information found in that section of the Insight. For more information on AI Insights, see The AI Insights Dashboard.

Sessions

The client sessions page consists of the firewall session details for the client connected to a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. The **Sessions Summary** pane displays the device the client is connected to, total number of sessions, and the time stamp of when the page was last refreshed. The sessions details page refreshes automatically, to refresh the page manually, click the refresh icon after the timestamp.

The **Sessions** table lists the details of each session. By default, the table displays the following columns: **Application**, **Source IP**, **Destination IP**, **Source Port**, **Destination Port**, **Action**, **Flags**, **Packets**, and **State**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each session:

Table 331: *Sessions Tab*

Section	Description
Application	Displays the list of applications.
Source IP	Displays the source IP address.
Destination IP	Displays the destination IP address.
Protocol	Displays the communication protocol used.
Source Port	Displays the source port number.
Dest Port	Displays the destination port number.
Action	Displays the application specific action.
Flags	Displays the active flags
Packets	Displays the number of packets.
State	Displays the connection state of the application. The state can either be Denied, Active, or Inactive.
Start Time	Displays the start time.
Receive Time	Displays the receive time.

Table 331: *Sessions Tab*

Section	Description
WebCC Category	Displays the WebCC category.
WebCC Reputation	Displays the WebCC reputation.
WebCC Score	Displays the WebCC score.
Application Category	Displays the application category.

Client **Sessions** is supported only if the Instant AP is running Aruba Instant 8.6.0.0 firmware version or later versions.

For details on the Branch Gateway client sessions refer, Gateway > Overview > Sessions.

Wired Client > Applications

The **Applications** page consists of client details that are connected to a wired network.

The section includes the following topics:

- Viewing Clients Connected to Wired Networks
- Applications
  - Visibility

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network.
5. Enter the client name in the **Client Name** column, and click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details

Applications

The **Application** page displays the **Visibility** tab.

Visibility

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see Application Visibility.

Wired Client > Live Events

The **Live Events** page consists of information required to troubleshoot issues related to a client or a site in real time for detailed analysis.

The section includes the following topics:

- Viewing Clients Connected to Wired Networks
- Live Events

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network.
5. Enter the client name in the **Client Name** column, and click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details

Live Events

You can live troubleshoot clients connected to a wired network. For more information on live troubleshooting a client, see Client Live Troubleshooting.

Wired Client > Events

The **Events** page displays the details of events generated by the AP and client association.

The section includes the following topics:

- Viewing Clients Connected to Wired Networks
- Events

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network.
5. Enter the client name in the **Client Name** column, and click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details

Events

The **Events** page consists of the table that displays the following columns: **Occurred On**, **Event Type**, and **Description**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each event:

Table 332: *Events Tab*

Section	Description
Occurred On	Displays the time at which the event occurred.
Event Type	Displays the type of the event.
Description	Displays the detailed description of the event.
Device MAC	Displays the MAC address of the device.
BSSID	Displays the BSSID.

To download events into a CSV format, click the download button. Aruba Central generates the CSV report of all the events for the selected client.

You can also filter the events based on the type of events, click the **Click here for Advance Filtering**. Select the type of events from the list and click **Filter**. The events under the selected categories get listed in the **Events** table. For more information on Events, see Alerts & Events

Wired Client > Tools

The **Tools** page aids the administrator users to monitor connections.

The section includes the following topics:

- Viewing Clients Connected to Wired Networks
- Tools

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network.
5. Enter the client name in the **Client Name** column, and click the client name.

   The contextual dashboard for the selected client is displayed and opens the **Summary** page by default.
6. Click the required tab name to navigate and view the details

Tools

The **Tools** page is automatically filtered based on the client you select. This enables network administrators to perform checks on the client and debug client connectivity issues. For more information on Tools, see Using Troubleshooting Tools.

Clients > Remote Client > Overview

The remote clients are clients that are connected to the network through VPN. The in-house wireless and wired clients can also be authenticated using the VPN (VIA). The overview page displays the summary, AI insights, location, sessions, and security details for the selected remote client.

The section includes the following topics:

- Viewing Clients Connected to VPN
- Overview
- Applications
- Tools

Viewing Clients Connected to VPN

To view the details of a client connected to the VPN:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.

4. Click the name of the remote client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Remote** to filter the clients connected to the network.
5. Enter the client name in the **Client Name** column, and click the client name. The client **Summary** page is displayed.
6. Click the required tab name to navigate and view the details.

Overview

The remote client overview tab displays the remote client summary, AI insights, location, sessions, and profile details for each client.

Remote Client Health Bar

The remote client health bar displays the connection status, the connected port, and the name of the gateway the client is connected to. For more information, see The Health Bar

The **Health** bar displays the following information.

Table 333: *Remote Client Health Bar*

Field	Description
Connection status icon	Displays the icons with the connection status of the client. Connection status is updated immediately on state change. The available statuses are: ■ **Connecting**—Displays a list of client connections that are in progress. ■ **Connected**—Displays a list of clients that are successfully connected to the network. ■ **Failed**—Displays a list of all failed client connections. ■ **Offline**—Displays a list of all offline clients. ■ **Blocked**—Displays a list of all blocked clients.
Connected To	Name of the Gateway to which the client is connected. Click the name of the Gateway to view the device details page.

Summary

The remote **Client Details** page displays the information about the type of data path that the client uses, the network details, and basic client details such as IP address of the client, type of encryption, and so on. The **Client Details** page refreshes automatically to display real time data and graphs. To refresh the page manually, click the refresh icon.

The following table describes the information displayed in each section.

Table 334: *Remote Client Details*

Section	Description
Data Path	Displays the data path of the client in the network. Click the device icon to view the corresponding device details page. The data path may be one of the following: ■ **Client** > **Wired Profile** > **Gateway** ■ **Client** > **Wireless Profile** > **Gateway**
Client Info	Displays the following information: ■ **Username**—User name of the client. ■ **Hostname**—Hostname of the client.

Table 334: *Remote Client Details*

Section	Description
	■ **Client Type**—Type of the client device. ■ **Local IP Address**—Link local IP address of the client. ■ **IP Address**—IP address of the client. ■ **MAC Address**—MAC address of the client. ■ **Client OS**—Displays the operating system that the device runs on. For example, if the client category is Computer and the client family is Windows, the client OS can be Windows or Windows 8/10. For details, see Classifying Clients. ■ **Connected Since**—Date and time since when the client was last connected.
Network Info	Displays the following information: ■ **Gateway Role**—Displays the role assigned to the client by the Gateway. ■ **Authentication Type**—Displays the authentication method as VIA VPN.
Throughput	Displays the incoming and outgoing throughput traffic for the client during a specific time range. By default, the graph on the **Throughput** pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the **Time Range Filter** link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months.

AI Insights

The **AI Insight** tab displays information about client performance and connectivity issues such as excessive 2.4 GHz dwell and low SNR links. AI Insights are displayed for a selected time period based on the time selected in **Time Range Filter**. The user can select 3 hours, 1 week, 1 day, or 1 month to view the insight data. Each AI Insight type displays the AI Insight label, AI Insight graph, and AI Insight chart. Further, the Insights include categories of information present in form of tabs like, reason, band, channel, SNR and so on. These tabs are clickable and display the detailed information found in that section of the Insight. For more information on AI Insights, see The AI Insights Dashboard.

Location

The **Location** tab displays the current physical location of the client device on the floor map.

Sessions

The client sessions page consists of the firewall session details for the client connected to a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. The **Sessions Summary** pane displays the device the client is connected to, total number of sessions, and the time stamp of when the page was last refreshed. The sessions details page refreshes automatically, to refresh the page manually, click the refresh icon after the timestamp.

The **Sessions** table lists the details of each session. By default, the table displays the following columns: **Application**, **Destination IP**, **Protocol**, , **Dest Port**, **DSCP**, **Flags**, **Packets**, **State** and **Action**.

Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each session:

Table 335: *Sessions Tab*

Section	Description
Application	Displays the list of applications.
Source IP	Displays the source IP address.
Destination IP	Displays the destination IP address.
Protocol	Displays the communication protocol used.
Source Port	Displays the source port number.
Dest Port	Displays the destination port number.
DSCP	Displays the DSCP value.
Flags	Displays the active flags
Packets	Displays the number of packets.
Bytes	Displays the total number of bytes.
State	Displays the connection state of the application. The state can either be Denied, Active, or Inactive.
Action	Displays the application specific action.
VLAN	Displays the VLAN the client is connected to.
Start Time	Displays the start time.
Receive Time	Displays the receive time.
WebCC Category	Displays the WebCC category.
WebCC Reputation	Displays the WebCC reputation.
WebCC Score	Displays the WebCC score.
Application Category	Displays the application category.
Priority	Displays the priority value.

For details on the Branch Gateway client sessions refer, Gateway > Overview > Sessions.

Remote Client > Applications

The **Applications** page provides you the client details for passive monitoring of the remote client. The section includes the following topics:

- Viewing Clients Connected to VPN
- Applications
  - Visibility

Viewing Clients Connected to VPN

To view the details of a client connected to the VPN:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the remote client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Remote** to filter the clients connected to the network.
5. Enter the client name in the **Client Name** column, and click the client name. The client **Summary** page is displayed.
6. Click the required tab name to navigate and view the details.

Applications

The **Application** page displays the **Visibility** tab.

Visibility

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see Application Visibility.

Remote Client > Tools

This section includes the following topics:

Viewing Clients Connected to VPN

To view the details of a client connected to the VPN:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site or device.
4. Click the name of the remote client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Remote** to filter the clients connected to the network.

5. Enter the client name in the **Client Name** column, and click the client name. The client **Summary** page is displayed.
6. Click the required tab name to navigate and view the details.

Tools

The **Tools** page is automatically filtered based on the client you select. This enables network administrators to perform checks on the client and debug client connectivity issues. For more information on Tools, see Using Troubleshooting Tools.

Classifying Clients

If the Aruba Central account is registered in the US-2 or EU-1 regional cluster, Aruba Central classifies the client connected to an AP. This section includes the following topics:

- Clients Page
- Insights

Clients Page

The **Clients** page provides a list view of all the clients connected to the network. The page displays key client details and also allows you to view a specific client detail page. For more information about clients, see All Clients.

The following details are displayed in the **Clients** > **List** view and the **Client Details** page:

- **Client Category**—Displays the category of the profiled client. For example, Computer, Smart Device, VoIP phone, and so on.
- **Client Family**—Displays the type of operating system or vendor. For example, if the client category is *Computer*, the client family can be Windows, Linux, or Apple Mac.
- **Client OS**—Displays the operating system that the client runs on. For example, if the client category is *Computer* and the client family is *Windows*, the client OS can be Windows or Windows 8/10.

  The following figure shows the **Client** section in the **Client Details** page:

Insights

The **Client** card in insights display the number of clients impacted. From the **Client** card, you can drill-down to the **Top 50 Clients Impacted** table. In this table, the **OS** column displays the client family and the operating system of the client. If Aruba Central is unable to classify the client, **Unclassified** is displayed.

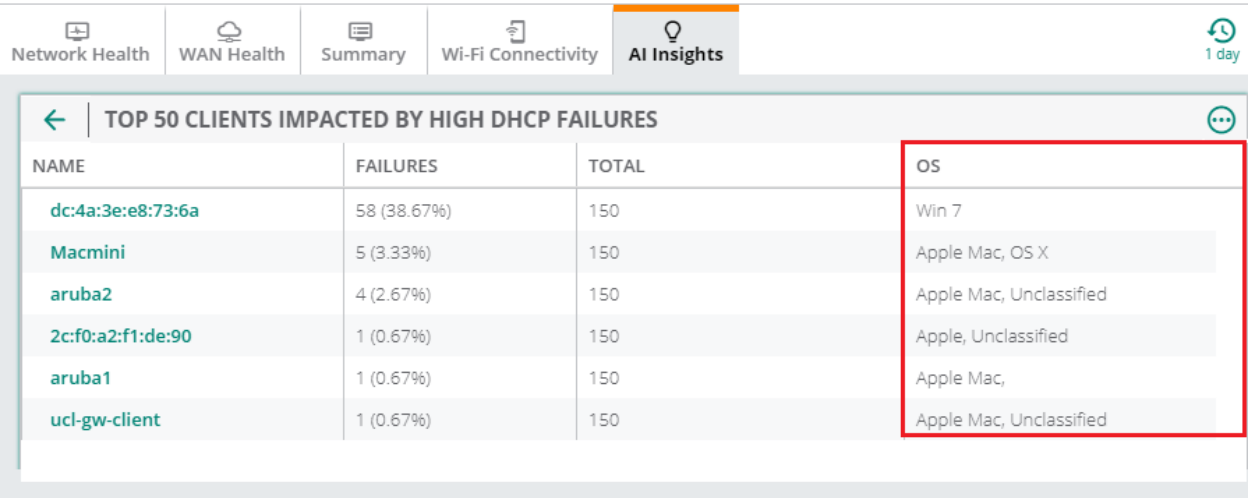
NOTE

The access point must be running Instant AP 6.4.4.8 or a later version.

The following connectivity and roaming insights display the client family and client OS:

- Clients with High MAC Authentication Failures
- Clients with High Wi-Fi Security Key-Exchange Failures
- Clients with High 802.1X Authentication Failures
- Clients with DHCP Server Connection Problems
- Clients with Low SNR Minutes
- Dual-band (2.4/5 GHz) Clients Primarily using 2.4 GHz

The following figure shows the **Top 50 Clients Impacted** table for the **High DHCP Failures** insight:



Related Topics:

- Clients > Wireless Client > Overview
- Clients > Wired Client > Overview
- Clients > Remote Client > Overview
- The AI Insights Dashboard

The **Manage** > **Applications** tab provides detailed information on data usage by the clients connected to APs and Branch Gateways in the network. The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications and websites. Click the **List** and the **Summary** icons on the **Application** and **Websites** sections to toggle between the dashboard views.

- Application Visibility is supported on Instant APs running software versions 6.4.3.1-4.2.0.0 or later. Aruba Central supports Application visibility monitoring, DPI configuration, and web filtering for IAP-103, RAP-108/109, IAP-114/115, RAP-155, IAP-224/225, IAP-274/275, IAP-228, IAP-277, IAP-205, IAP-214, IAP-324/325, and IAP-304/305, IAP-207, IAP-334,IAP-314/315, IAP-344/345, IAP-504/505, IAP-514/515, IAP-535/534 and IAP-555.
- Instant AP-104/105, Instant AP-134/135, RAP3WNP, and Instant AP-175 devices only support web policy enforcement.

Viewing Visibility Dashboard

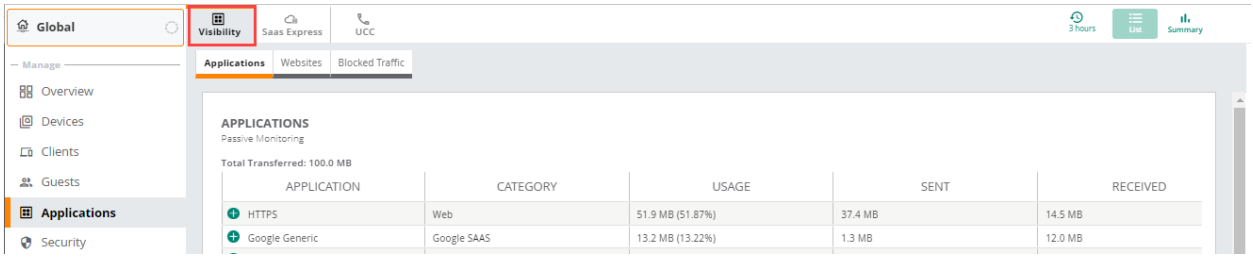
To view the **Visibility** dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups** or **Sites**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Applications**. The visibility dashboard is displayed.

The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**
- **Blocked Traffic**

Figure 507 ***Visibility*** *dashboard at the global level*



To view client traffic details, ensure that the DPI access rules are enabled on the Instant AP device.

Applications

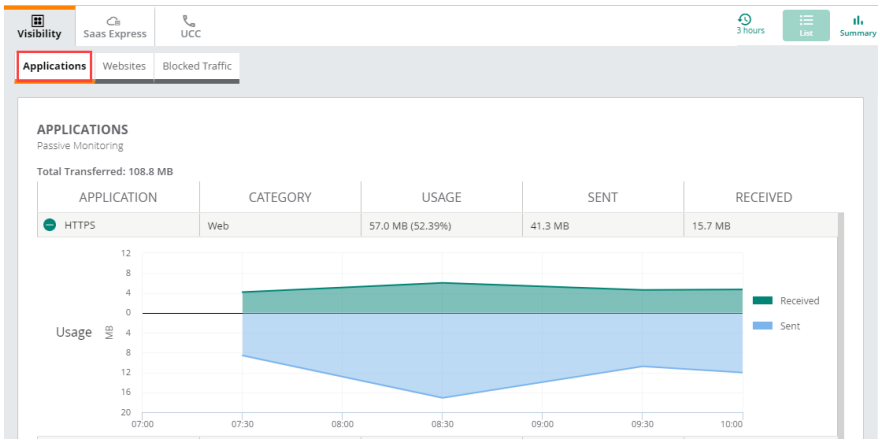
The **Applications** tab includes a table view and a graph view related to the client traffic flow to and from various applications. These graphs are displayed for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in last three hours.

Table View in Application Section

Click the **List** icon in the **Applications** tab to display a table with the following columns:

- **Application**—Name of the application.
- **Category**—The category to which the application belongs. The application can belong to any of the categories, such as **Unclassified**, **Standard**, **Social Networking**, **Streaming**, **Web**, **Cloud File Storage**, **Instant Messaging Network Service** and so on.
- **Usage**—Data consumed by an application.
- **Sent**—The size of data sent from the application.
- **Received**—The size of data received by the application.

Figure 508 *Application Dashboard List View*

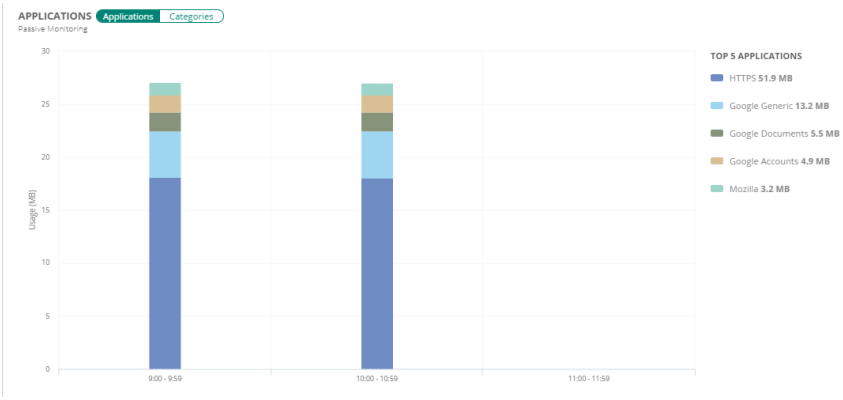


Graph View in Applications Section

Click the **Summary** icon in the Applications tab to display bar graphs indicating the traffic flow in the following tabs:

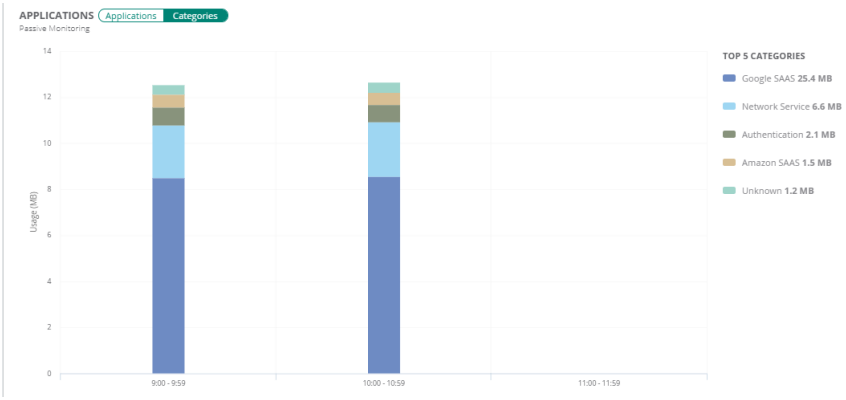
- **Applications**—The stacked bar graph in this tab displays details of the client traffic flowing to or from the top five classified applications listed in the **Applications** table. The legend beside the bar graphs displays the list of applications to which the traffic flow is detected. By hovering the mouse on the bar graph, you can view the size of data flowing to and from the application same as displayed in legend.

Figure 509 *Graphical View with Applications*



- **Categories**—The stacked bar graph in this tab displays details of the client traffic flowing to or from the top five classified application categories listed in the **Applications** table. By hovering the mouse on the bar graph, you can view the size of data flowing to and from the application categories same as displayed in legend.

Figure 510 *Graphical View with Categories*



For more information about configuring applications and application categories, see Configuring Aruba Gateways for Application Visibility and Control.

Websites

The **Websites** tab includes a table view and a bar graph view related to the client traffic flow and their data usage by various websites. These graphs are displayed for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in last three hours.

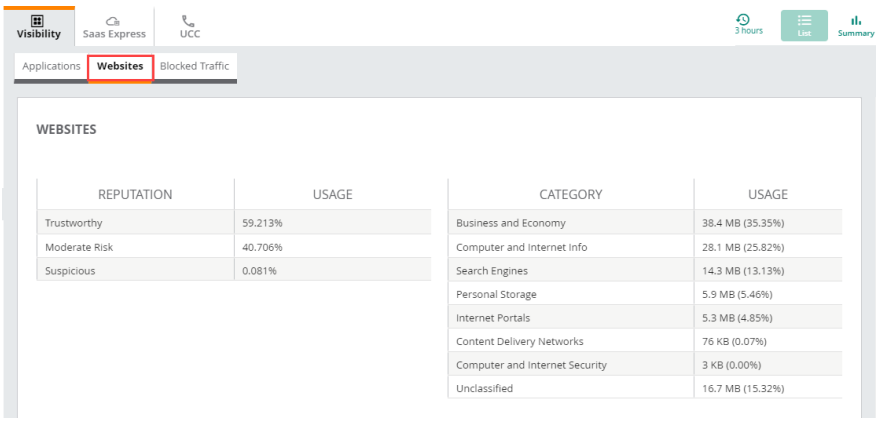
Table View in Websites Section

The **Websites** tab displays the following details:

- **Reputation**—The reputation of the application categories, for example, **Trustworthy**, **Incomplete**, **Moderate Risk**, **Low Risk**, **High Risk** and so on. The reputations are set based on the risk levels exhibited by the application categories.
- **Usage**—The percentage of data usage by application categories based on their reputation.

- **Category**—The category of the client traffic that sends and receives data, for example, **Unclassified**, **Social Networking**, **Streaming**, **Web**, **Cloud File Storage**, **Instant Messaging** and so on.
- **Usage**—The size and percentage of data usage by the corresponding categories.

Figure 511 *Websites Dashboard View*

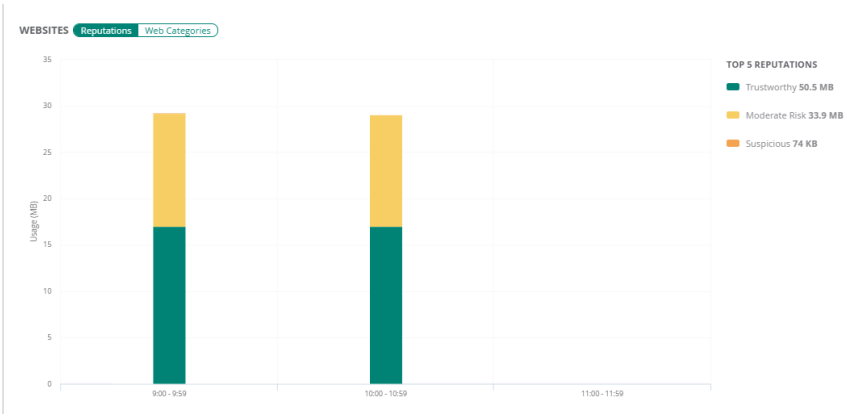


Graph View in Websites Section

Click the **Summary** icon in the **Websites** section to display bar graphs for the following tabs:

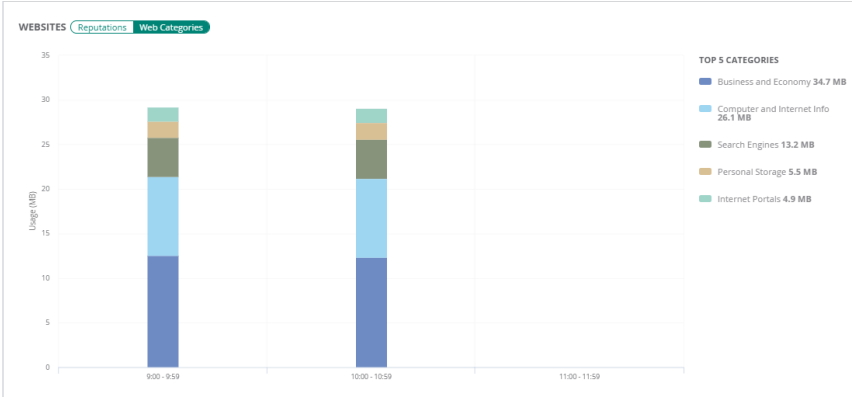
- **Reputation**—The stacked bar graph displays details of client traffic flow for the top five reputations listed in the **Websites** table.

  Figure 512 *Websites with Reputations*



- **Web Categories**—The stacked bar graph displays details of client traffic flow for the top five web categories listed in the **Websites** table. You can view the size of data flowing to and from each of the web categories by hovering the mouse on the bar graph. The legend beside the bar graphs displays the list of websites based on its reputation, to which the traffic flow is detected.

Figure 513 *Websites with Web Categories*



- The Applications (Apps) and Web Categories charts are also displayed in the **Applications** pages for the Group, Site, APs, and Gateways levels.
- Application Visibility data is updated every 0th minute of every hour. The data population on the **Applications > Visibility** dashboard may be delayed by an hour when compared to the Application Visibility data displayed in the **Applications** pages for the Group, Site, APs, and Gateways levels.

Blocked Traffic

Based on the group selection from the **Blocked Traffic** drop-down list, the **Blocked Traffic** section of the **Application > Visibility > Blocked Traffic** dashboard allows you to view the following information:

- Blocked devices of the selected group as CSV file.
- The number of user sessions that are blocked.

- The blocked traffic details are shown only for the APs on which Application Visibility or DPI ACLs are enabled.
- The **Blocked Traffic** tab is only displayed in **Global** level in the **Network Operations> Manage > Applications** page.

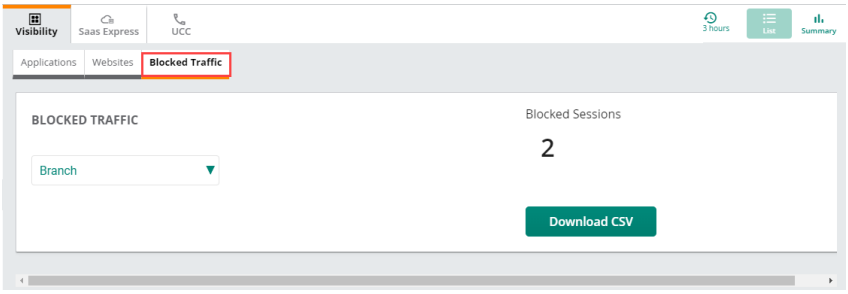
Downloading Blocked Session Details

To download blocked session details in the CSV format, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Applications**. The **Visibility** dashboard is displayed.
3. Click **Blocked Traffic** tab.
4. To download the blocked sessions report, select the device group from the **Select Group** drop-down.

5. Click **Download CSV**. Aruba Central generates the CSV report with data from the last 7 days.

Figure 514 *Blocked Traffic Dashboard view*



NOTE

The CSV file shows up to 50000 blocked sessions for a single Instant AP cluster.

Chapter 37
Using Troubleshooting Tools

In the **Network Operations** app, use the filter to select a group, label, site, or a device and then, select **Tools** menu option under **Analyze**. The **Tools** menu allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. Users with admin role and custom roles that allow edit access to the troubleshooting module can troubleshoot network and device issues. For more information on user roles, see Configuring User Roles.

The **Tools** menu option is not visible to users who do not have troubleshooting permission.
Aruba Central does not support performing diagnostic checks on offline devices.

The **Tools** page is divided into the following tabs:

- **Network Check**—Allows you to run diagnostic checks on networks and troubleshoot client connectivity issues. You must have admin privileges or read-write privileges to perform network checks.
- **Device Check**—Allows you to run diagnostic checks and troubleshoot switches. You must have admin privileges or read-write privileges to perform device checks.
- **Commands**—Allows you to perform network health check on devices at an advanced level using command categories. Read-only users can also perform advance checks.

This section includes the following topics:

Troubleshooting Network Issues

Network check aims to identify, diagnose, and debug issues detected in an Aruba Central-managed network. The **Network Check** tab on the **Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection.

To perform a diagnostic check on the Aruba Central-managed network, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.

c. Click a device listed under **Device Name**.

The dashboard context for the device is displayed.

2. Under **Analyze** > **Tools**, click the **Network Check** tab.

   The **Network Check** page is displayed.

3. Select a device. You can run diagnostic checks on the following types of devices managed by Aruba Central:
   - Access Points
   - Switches
   - Gateways

Table 336 lists the tests available for each device type:

Table 336: *Tests and Devices*

Test	Access Point	Switch	Gateway
Ping Test	Available	Available	Available
Ping Sweep Test	Not Available	Not Available	Available
Traceroute	Available	Available	Available
HTTP Test	Available	Not Available	Available
HTTPS Test	Available	Not Available	Available
TCP Test	Available	Not Available	Not Available
Speed Test (iPerf)	Available	Not Available	Available

Devices that are already running commands shall not execute newly added commands.

Troubleshooting AP Connectivity Issues

The following tests are available to diagnose issues pertaining to WLAN network connections:

Ping Test

Sends ICMP echo packets to the hostname or IP addresses of the selected devices to check for latency issues.

To perform a ping test on APs:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
   - The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

     A list of access points is displayed in the **List** view.

c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

The dashboard context for the access point is displayed.

2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Sources** drop-down list, select source(s). You can select multiple APs.
5. From the **Test** drop-down list, select **Ping Test**.
6. From the **Destination Type** drop-down list, select one of the following:
   - **Hostname/IP Address**—Enter the hostname or IP address.
   - **Client**—Select a client.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:

Show Additional Test Settings is not displayed when a **Test** type is not selected.

   a. In the **Packet Size** field, enter the packet size in order to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 65507 bytes.
   b. In the **Count** field, enter the count. The value should be between 1 to 2147483647.
   c. Select **Port** from the **Source Interface** drop-down list and select the port number.

8. Click **Run**. The output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on APs:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. Click **Run**. The output is displayed in the **Device Output** section.

HTTP Test

Sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.

To perform an HTTP test on APs:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTP URL for which you want to perform the HTTP test, in the **URL** field, For example, http://*hostname* or http://*ipaddress*.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
   The value should be from 1 to 10 seconds. The default timeout value is 1 second.

Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Important Points to Note

- HTTP test is supported only for APs residing on AOS version 8.3.0.0 or above.
- The test supports only IPv4 address or domain name in the **URL** field.

HTTPS Test

Sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device. HTTPS is a performance test to identify the time taken to load a web page.

To perform an HTTPS URL test on APs:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.

- To select a device in the filter:
  a. Set the filter to **Global**.
  b. Under **Manage**, click **Devices** > **Access Points**.
     A list of access points is displayed in the **List** view.
  c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
     The dashboard context for the access point is displayed.

2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTPS URL for which you want to perform the HTTPS test, in the **URL** field, For example, https://*URL* or https://*IPv4*.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
   The value should be from 1 to 10 seconds. The default timeout value is 1 second.

Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Important Points to Note

- HTTPS test is supported only for APs residing on AOS version 8.4.0.0 or above.
- The test supports only IPv4 address or domain name in the **URL** field.

TCP Test

Sends packets to the host, for example, FTP server, and tries to establish a connection and exchange data. If the FTP server returns a response, the issue could be isolated to the client device.

To perform a TCP test on APs:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.
     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.
        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.

4. From the **Test** drop-down list, select **TCP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter a valid IPv4 address in the **Host** field. Hostname is not supported.
7. Enter the port number., in the **Port** field. The port number should be between 1 to 65535.
8. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
   The value should be from 1 to 10 seconds. The default timeout value is 5 seconds.

Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Important Point to Note

- TCP test is supported only for APs residing on AOS version 8.3.0.0 or above.

Speed Test (iPerf)

Performs a speed test to measure network speed and bandwidth. The speed test diagnostic tool is available only for Instant AP. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on APs:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.
     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.
     c. A list of access points is displayed in the **List** view.
     d. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Speed Test (iPerf)**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.

While performing troubleshooting on APs, a maximum of 20 APs are listed in the drop-down list. If there are more than 20 APs, use the **Search** option to search for an AP on which you would like to perform diagnostic checks.
If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

6. In the **Host** field, enter a valid hostname.
7. From the **Protocol** drop-down list, select the protocol. The available options are **TCP** or **UDP**.

8. To use additional parameters, click **Show Additional Test Settings** and in the **Options** field, enter an option.
   For example, bandwidth.

Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**. The test output is displayed in the **Device Output** section.

Troubleshooting Switch Connectivity Issues

The following tests are available to diagnose issues related to wired network connections:

Ping Test

Sends ICMP echo packets to the IP address of the selected switch to check for latency issues.

To perform a ping test on switches, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.
        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name** for which you want to perform diagnostic test.
        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down, select **Switch**.
4. From the **Test** drop-down, select **Ping Test**.
5. From the **Sources** drop-down, select source(s). You can select multiple switches.

You can select Aruba Switch or Mobility Access Switch from the **Sources** drop-down.

6. From the **Destination Type** drop-down, select one of the following:
   - **Hostname/IP Address**—Enter the hostname or IP address in the **Hostname/IP Address** field.
   - **Client**—Select a client from the **Client** drop-down.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:

Show Additional Test Settings is not displayed when a **Test** type is not selected.

   a. In the **Repetitions** field, enter the repetition value. The value should be between 1 to 500.
   b. In the **Data Size** field, enter the data size. The value should be between 0 to 65399.

Mobility Access Switches do not support repetition and data size.

8. Select the **Use Management Interface** option if you want to use VRF Management interface. To use VRF Default interface, clear this option, which is the default.

Use Management Interface option is available only for AOS-CX switches.

9. Click **Run**. The test output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on switches, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, **Network Check**.
3. From the **Device Type** drop-down, select **Switch**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down, select source(s). You can select multiple switches.
6. Enter the hostname or IP address in the **Hostname/IP Address** field.
7. To use additional parameters, click **Show Additional Test Settings** and select the **Use Management Interface** option, if you want to use the VRF Management interface. To use the VRF Default interface, clear this option.

Show Additional Test Settings is disabled when no Test type is selected.

Use Management Interface option is available only for AOS-CX switches

8. Click **Run**. The output is displayed in the **Device Output** section.

   For information about viewing and downloading the output, see Viewing the Device Output.

If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

Troubleshooting Gateway Connectivity Issues

The following tests are available to diagnose issues pertaining to WAN or SD-WAN network connections:

Ping Test

Sends ICMP echo packets to the IP addresses of the selected devices to check for latency issues.

To perform a ping test on Gateways:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the gateway is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Ping Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. From the **Destination Type** drop-down list, select one of the following:
   - **Hostname/IP Address**—Enter the hostname or IP address.
   - **Client**—Select a client.
   - **VPNC**—Select the VPN Concentrator.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:

Show Additional Test Settings is not displayed when a **Test** type is not selected.

   a. In the **Packet Size** field, enter the packet size to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 2000 bytes.
   b. In the **Count** field, enter the count. The value should be between 1 to 1000.
   c. In the **Time to Live** field, enter the time range. The value should be between 1 to 225 seconds.
   d. In the **DSCP** field, enter the packet header value. The value should be between 0 to 63.
   e. From the **Source Interface** drop-down list, select one of the following:
      - **Loopback**—Select loopback to verify if ping functionality is working when the source address is set as logical address. It is a logical interface.
      - **Management Interface**—Select management interface to verify if ping functionality is working when the source address is set as management interface. It is a physical interface which is dedicated to configuration and management operation in the network.
      - **VLAN Interface**—Select VLAN interface to verify if ping functionality is working when the source address is set as VLAN interface. It is a virtual LAN used to avoid broadcast domain in a switch or gateway.
   f. Optionally, you can select the **Don't Fragment** toggle button. This option is used when the packet size is more than the Maximum Transmission Unit (MTU) size of the interface.
8. Click **Run**. The output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on Gateways:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the gateway is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. Enter the hostname or IP address.
7. To use additional parameters, click **Show Additional Test Settings**, and from the **Source Interface** drop-down list, select **VLAN Interface**.
8. From the **VLAN Interface** drop-down list, select the required VLAN ID displayed along with the IP address.
9. Click **Run**. The output is displayed in the **Device Output** section.

If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

Ping Sweep Test

Performs a more advanced check on host reachability and network connectivity. Sends different sizes of ICMP echo packets to the IP addresses of selected devices based on start packet size, end packet size and sweep interval field values.

To perform a ping sweep test on Gateways:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.

c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.

   The dashboard context for the gateway is displayed.

2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Ping Sweep Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. From the **Destination Type** drop-down list, select one of the following:
   - **Hostname/IP Address**—Enter the hostname or IP address.
   - **Client**—Select a client.
   - **VPNC**—Select the VPN Concentrator.
7. In the **Start Packet Size** field, enter the start packet size to capture and store the range of data packet to analyze network issues at a later stage. The range is from 10 to 1999 bytes.
8. In the **End Packet Size** field, enter the end packet size. The range is from 11 to 2000 bytes.
9. In the **Sweep Interval** field, enter the sweep interval size to set the sweep threshold for the transactions. The range is from 1 to 1990 bytes.
10. In the **Count** filed, enter the count. The value should be between 1 to 1000.
11. Click **Run**. The test output is displayed in the **Device Output** section.

Speed Test (iPerf)

Performs a speed test to measure network speed and bandwidth. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on Gateways:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.
     c. A list of access points is displayed in the **List** view.
     d. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Speed Test (iPerf)**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. In the **Host** field, enter a valid hostname or IP address.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:

Show Additional Test Settings is not displayed when a **Test** type is not selected.

a. **Port**—Select the port.
b. **VLAN Interface**—Select the VLAN ID from the drop-down list.

8. Click **Run**. The test output is displayed in the **Device Output** section.

HTTP Test

Sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, it indicates that the web server is up and reachable. If the HTTP website does not return a response, it indicates that the server is down and did not return a response.

To perform an HTTP test on Gateways:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **HTTP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. Enter the HTTP URL for which you want to perform the HTTP test, in the **URL** field, For example, http://*hostname* or http://*ipaddress*.
7. Click **Run**. The test output is displayed in the **Device Output** section.

The test supports only IPv4 address or domain name in the **URL** field.

HTTPS Test

Sends packets to the HTTPS URL and tries to establish a connection and exchange data.If the HTTPS website returns a response, it indicates that the web server is up and reachable. If the HTTPS website does not return a response, it indicates that the server is down and did not return a response.

To perform an HTTPS URL test on Gateways:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Group**, **Label**, or **Site**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.

- To select a device in the filter:
    a. Set the filter to **Global**.
    b. Under **Manage**, click **Devices** > **Gateways**.
       A list of access points is displayed in the **List** view.
    c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.
       The dashboard context for the access point is displayed.

2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. Enter the HTTPS URL for which you want to perform the HTTPS test, in the **URL** field, For example, https://*URL* or https://*IPv4*.
7. Click **Run**. The test output is displayed in the **Device Output** section.

The test supports only IPv4 address or domain name in the **URL** field.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and target. It also shows the status of the tests as, in progress, complete, and the buffer time. If there are multiple devices, select the device for which you want to view the output.

Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the **Download** icon to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Enabling Gateway Logs

Logs is supported in this release as a selectively available feature. Contact your Aruba SE or Account Manager to enable it in your Aruba Central account.

Logs aims to help users diagnose and debug issues detected in an Aruba Central-managed network. The **Logs** tab on the **Tools** page of a gateway dashboard provides the user with an option to enable **On-Demand data collection**. The **On-Demand data collection** enables you to download TAR logs and crash logs related to gateways.

To enable logs collection for a gateway on the Aruba Central-managed network, complete the following procedure::

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the selected option contains at least one gateway. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the gateway is displayed.
2. Under **Manage** > **Devices**, click the **Gateways** tab.

   A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**.

   The dashboard context for the gateway is displayed.
4. Under **Analyze** > **Tools**, click the **Logs** tab.
5. In the **Logs** tab, turn on the **Enable On-Demand data collection** toggle to download TAR logs and crash logs.
6. To upload TAR log or crash log, click **+** in the **Log Files** table. The Upload Log File panel opens.
7. Configure the following parameters as per your requirements:

Table 337: *Upload Log File Configuration Parameters*

Parameter	Description
File type	Select one of the log file types listed here: ■ TAR log ■ Crash log
Tar log	The following options are displayed when the **File Type** is configured as **TAR log**. You can select one of the options listed here: ■ **Upload existing file**—Allows you to upload an existing TAR log file. ■ **Generate & upload new file now**—Allows you to generate and upload a new TAR log file now.

Parameter	Description
	▪ **Generate & upload new file at a scheduled time**—Allows you to generate and upload a new TAR log file at a later date and time.
Crash Log	The following options are displayed when the **File Type** is configured as **Crash log**. You can select one of the options listed here: ▪ **Upload existing file**—Allows you to upload an existing Crash log file. ▪ **Prepare & upload new file now**—Allows you to prepare and upload a new Crash log file now. ▪ **Prepare now & upload new file at a scheduled time**—Allows you to prepare a Crash log file now and upload it at a later date and time.
Scheduled Time	If you chose to upload a TAR or Crash log file at a later date and time, configure the parameters listed here: ▪ **Select Zone**—Allows you to configure the time zone. ▪ **Select Date**—Allows you to select a date within the range of a week. ▪ **Hours**—Allows you to configure hour ranging from 0 to 23. ▪ **Minutes**—Allows you to configure minutes ranging from 0 to 59.

8. Click **Save**.
9. The **Log Files** table displays the information in the table below:

Table 338: *Log Files Parameters*

Parameter	Description
File type	Displays the name of the generated log file.
Type	Displays the type of the generated log file: ▪ TAR file ▪ Crash file
Status	Displays the status of the generated log file. ▪ Scheduled—Displays this status when an existing log file is scheduled for upload. ▪ In progress—Displays this status when a new log file is generated and it is scheduled for upload now or for a later date.
Collection Time	Displays the time when the log file was created.
Size	Displays the size of the log file.
User	Displays the User ID of the user who generated the log file.

10. To download a log, select the respective log listed in the Log Files table and click the download icon.
11. To delete a log, select the respective log listed in the Log Files table and click the delete icon.

Troubleshooting Device Issues

Device check aims to identify, diagnose, and debug issues on your device. The **Device Check** tab in the **Tools** page can be used to perform troubleshooting check for Gateways, Aruba Switches and Aruba CX

switches. When a troubleshooting operation is initiated, Aruba Central establishes a session with the switch or gateway selected for the troubleshooting operation and displays the output in the **Device Output** section.

To perform a device check on gateways and switches, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Switches** or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
2. Under **Analyze** > **Tools**, click the **Device Check** tab.

   The **Device Check** page is displayed.
3. Select a device. You can run diagnostic checks on the following types of devices managed by Aruba Central:
   - Troubleshooting Switch Issues
   - Troubleshooting Gateway Issues

Troubleshooting Switch Issues

To perform a device check on switches, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, click the **Device Check** tab.

   The **Device Check** page is displayed.
3. From the **Sources** drop-down, select a switch.
4. From the **Test** drop-down, select one of the following tests to perform diagnostic checks on the selected switch:
   - **Cable Test**—Enables testing of the electrical connections in the switch cable. It checks whether the cabling is conformed to the cabling plans and is of expected quantity. It is useful for production and maintenance.

NOTE

Cable Test is supported in Aruba Switches only from version 16.05.000 or above.
Cable Test is not supported in Aruba CX switches.

- **Interface Bounce**—Restarts the port interface and forces a client to re-initiate a DHCP request. This option is available only for Aruba Switches.
- **PoE Bounce**—Restarts the PoE port and the device that is either connected to the PoE port or powered by it. This option is available only for Aruba Switches.

NOTE

If you select **Cable Test**, **PoE Bounce**, or **Interface Bounce**, you must enter the port number or the port number range as mentioned in the example text.
If you navigate to the **Tools** page from the **Clients** page, under **Device Check** the client context is already set and the port number is auto filled based on the client selected.

- **Chassis Locate**—Activates the Switch locator LED. The locator LED indicates the physical location where an Aruba Switch is currently installed.

  Important Point to Note

NOTE

Interface Bounce, PoE Bounce, and Chassis Locate tests are supported only from the following versions in switches:

- Aruba Switches: 16.04.0000 or above
- Aruba CX: See Supported AOS-CX Platforms.

5. Click **Run**. The output is displayed in the **Device Output** section.

   For information about viewing and downloading the output, see Viewing the Device Output.

   Unlike the other tests, for Cable Test, the output is displayed in a tabular format, and you cannot download, email, or export the output.

Troubleshooting Gateway Issues

To perform a device check on gateways, complete the following procedure:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click a gateway under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the gateway is displayed.
2. Under **Analyze** > **Tools**, click the **Device Check** tab.

   The **Device Check** page is displayed.
3. From the **Sources** drop-down, select a gateway.

4. From the **Test** drop-down, select one of the following tests to perform the diagnostic check:
   - **Interface Bounce**—Restarts the port interface and forces a client to re-initiate a DHCP request.
   - **PoE Bounce**—Restarts the PoE port and the device that is either connected to the PoE port or powered by it.

If you select **PoE Bounce** or **Interface Bounce**, you must enter the port number or the port number range as mentioned in the example text.
If you navigate to the **Tools** page from the **Clients** page, under **Device Check** the client context is already set and the port number is auto filled based on the client selected.

5. Click **Run**.

   The output is displayed in the **Device Output** section. For information about how to view and download the output, see Viewing the Device Output.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and target. It also shows the status of the tests as, in progress, complete, and the buffer time. If there are multiple devices, select the device for which you want to view the output.

Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the **Download** icon to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Advanced Device Troubleshooting

Advanced device check aims to identify, diagnose, and debug issues on your device at an advanced level using commands. The **Commands** tab on the **Tools** page lists commands specific to a particular device to test the device entity and collect results based on your selection. When a troubleshooting operation is initiated, Aruba Central establishes a session with the devices selected for the troubleshooting operation and displays the output in the **Device Output** section.

To perform advanced troubleshooting on devices, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
2. Under **Analyze** > **Tools**, click the **Commands** tab.

   The **Commands** page is displayed.
3. Select a device. Network administrators can perform advanced troubleshooting on the following types of devices managed by Aruba Central:
   - Access Points
   - Switches
   - Gateways

Devices which are already running will not execute newly added commands.

Troubleshooting Access Points

To troubleshoot APs at an advanced level:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Access Point**.
4. From the **Available Devices** drop-down list, select the AP. You can select multiple APs.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box.

   For more information on filtering commands, see Filtering Commands.

8. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
   a. Click the **Repeat** check box.
   b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
   c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**. The output is displayed in the **Device Output** section.

To perform advanced troubleshooting on APs, the minimum software version required on Instant APs is 6.4.3.1-4.2.0.3.
To perform advanced troubleshooting on Mobility Access Switches, the minimum supported version is 7.4.0.6.
If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

Troubleshooting Switches

To troubleshoot switches at an advanced level:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name** for which you want to run a diagnostic test.

        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, click **Commands**.

   The **Commands** page is displayed.
3. From the **Device Type** drop-down, select **Switch**.
4. From the **Available Devices** drop-down, select the switch. You can select multiple switches.
5. Select any command category in the **Categories** pane and the **Commands** pane displays the associated commands.

Aruba CX switches support only the `show tech` and `show running-config` commands.

6. Click **Add >** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box.

   For more information on filtering commands, see Filtering Commands.
8. (Optional) Select command(s) and click **< Remove** to remove selected command(s) or click **< Remove All** to clear the **Selected Commands** pane.

9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
   a. Click the **Repeat** check box.
   b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
   c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**. The output is displayed in the **Device Output** section.

    For information about viewing and downloading the output, see Viewing the Device Output.

Troubleshooting Gateways

To troubleshoot Gateways at an advanced level:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Gateways**.

        A list of gateways is displayed in the **List** view.
     c. Click a gateway listed under **Device Name** for which you want to perform diagnostic test.

        The dashboard context for the gateway is displayed.
2. Under **Analyze** > **Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Gateway**.
4. From the **Available Devices** drop-down list, select the gateway. You can select multiple gateways.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. If you have selected a command marked with either '*' or '+', enter the filtration parameters as displayed in the **Additional Filters** dialog box.

   For more information on filtering commands, see Filtering Commands.
8. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
   a. Click the **Repeat** check box.
   b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
   c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**. The output is displayed in the **Device Output** section.

Gateway Diagnostic Tests

Aruba Central provides troubleshooting utilities to test SD-WAN overlay network connections. Users experiencing device connectivity issues at the branch site at a specific location, can select the device and specify an IP address to test the network connectivity. SD-WAN diagnostic tests allow users to view the

routing path and forwarding rules that are used to forward or drop packets in an SD-WAN orchestrated network.

Diagnostic tests identify the routing or forwarding issues in the overlay network path, if any. Following are two types of diagnostic tests:

- **Control plane** test
- **Data plane** test

SD-WAN diagnostic tests do not trace underlay routing network paths.

The minimum firmware version required for performing SD-WAN diagnostic tests is ArubaOS 8.5.0.0-2.1.0.0.

This section includes the following topics:

Control Plane

The control plane builds and maintains the network topology and makes decisions on the traffic flow in an SD-WAN network. Control plane tracing is based on the active routing table entries.

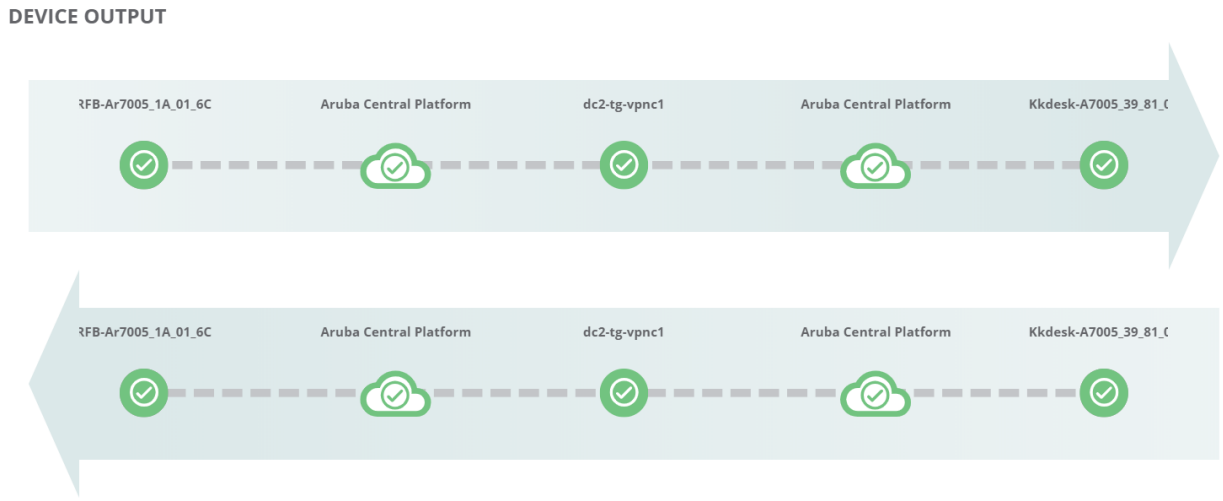
In the **Control plane** test, the diagnostic framework traces all the nodes and the forward route details in the orchestrated path from the selected gateway to the destination IP. It also traces all the nodes and the forward route detail in the reverse path, from the last gateway in the overlay path to the source IP. The last gateway in the path tracing output is the gateway in which the packet gets routed through the underlay routes, but not through the tunnels.

To perform a **Control plane** test, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**.The dashboard context for the selected filter is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Diagnostics**.
5. From the **Diagnostic Type** drop-down list, select **Control plane**.
6. From the **Sources** drop-down list, select the source.
7. In the **Source IP Address** field, enter the IP address for which you want to perform the test.
8. In the **Destination IP Address** field, enter the IP address for which you want to perform the test.
9. Click **Run**.

The output is displayed in the **Device Output** section.

Figure 515 *Control Plane—Device Output*



Control Plane—Node Details

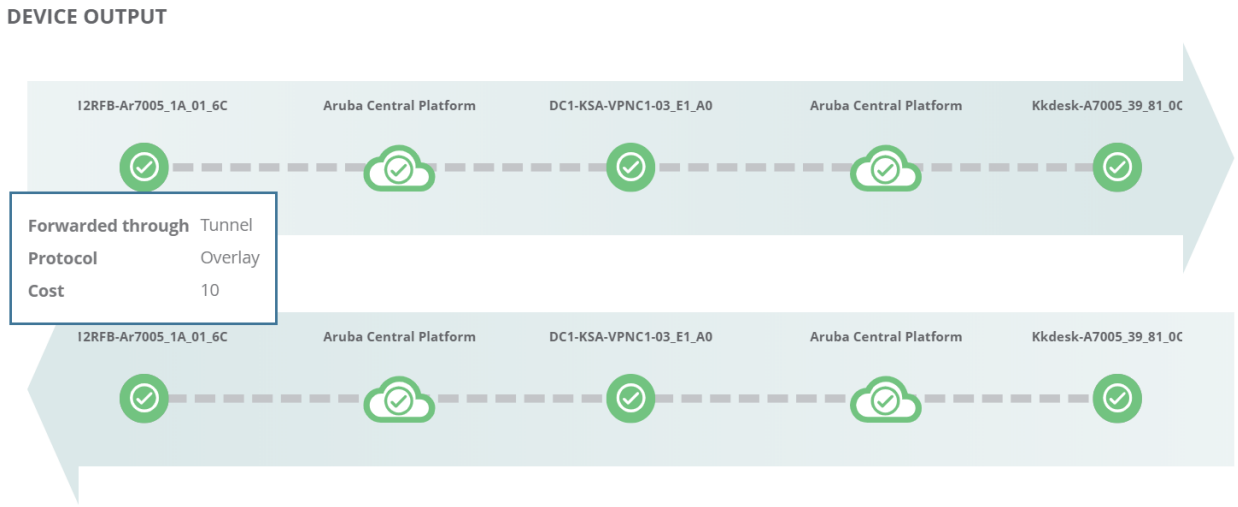
When you click on a node, a pop-up displays information that allows the user to analyze the data at every node in the forward and reverse path.

Gateway and VPNC—Node Details

When you click a Gateway node or a VPNC node in a forward or reverse path, the pop-up displays the following information:

- **Forwarded through**—Displays the name of the network path.
- **Protocol**—Displays the type of protocol.
- **Cost**—Displays the metric value of the path cost.

Figure 516 *Gateway and VPNC—Node Details*

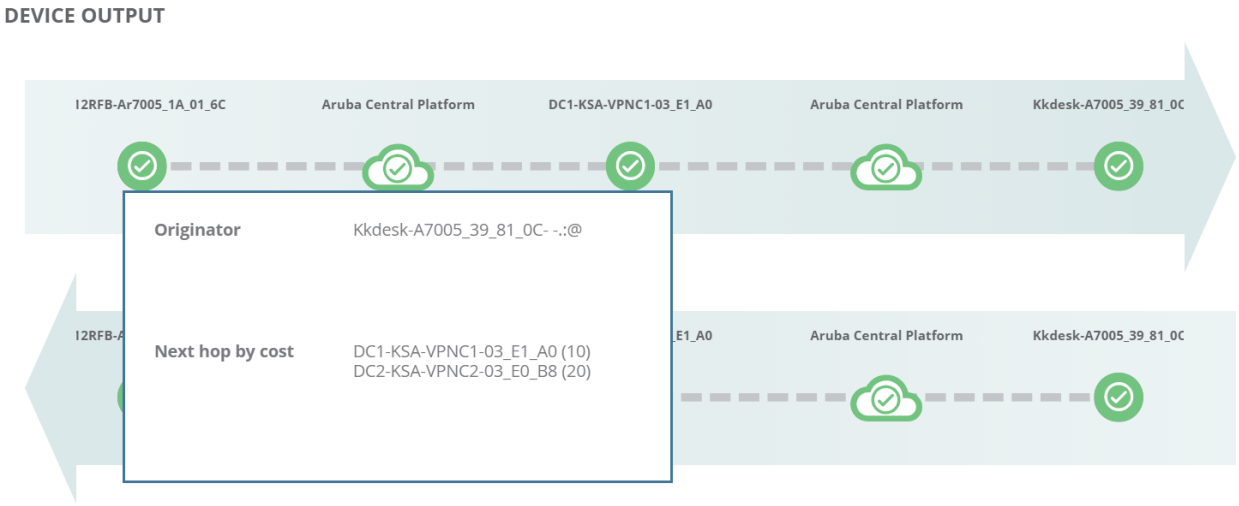


Aruba Central Platform—Node Details

When you click an Aruba Central Platform node in a forward or reverse path, the pop-up displays the following information:

- **Originator**—Displays the name of the devices which originated the particular route prefix in the overlay topology. It is the destination IP for the forward path and the source IP for the reverse path.
- **Next hop by cost**—Displays the list of next hops in an order of increasing value of cost.

Figure 517 *Aruba Central Platform—Node Details*



Data Plane

The data plane is responsible for forwarding the packets based on the decisions from the control plane in an SD-WAN network. Data plane tracing is based on the current datapath session table entries. Data path sessions are created when traffic flows through the gateways. When the data traffic flow stops, data path sessions are cleared after the age-out interval of the session. The test output is valid when you execute the test within the age-out interval of the data path session, and there are data path session entries in the gateway matching your input for the diagnostics test.

For most effective data plane test results, live traffic flow must be available matching your input for the diagnostics test.

In the **Data plane** test, the diagnostic framework traces all the nodes and the datapath session status for the selected flow in the overlay path from the selected gateway to the destination IP or port. It also traces all the nodes and the datapath session status for the reverse traffic from the last gateway in the overlay path to the source IP. The last gateway in the data plane tracing output is the gateway in which the packet gets routed through the underlay routes or gets dropped because of the configured firewall rules, but not through the tunnels.

To perform a **Data plane** test, complete the following steps:

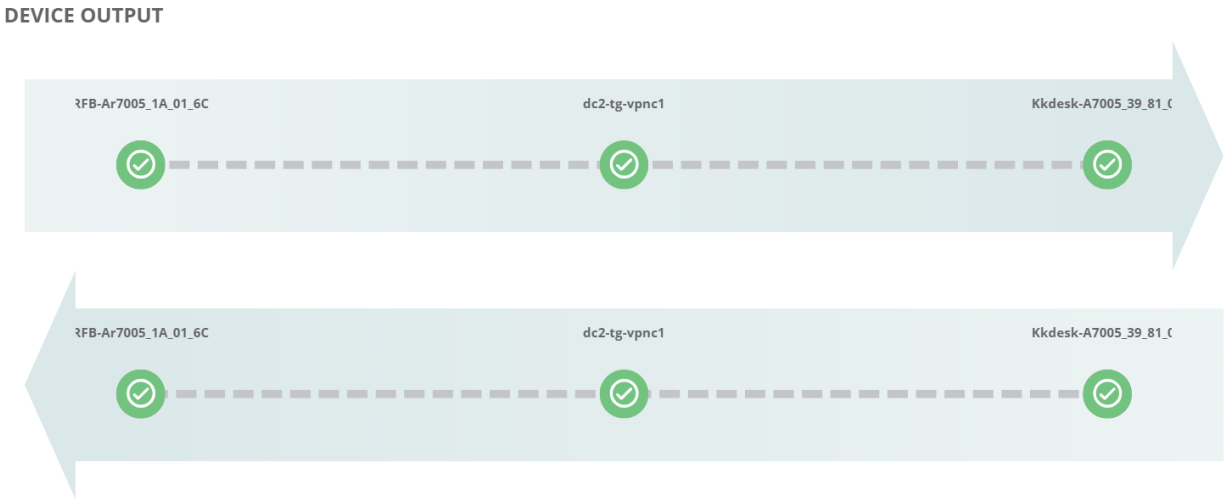
1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the filter selection contains at least one gateway. For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Diagnostics**.
5. From the **Diagnostic Type** drop-down list, select **Data plane**.
6. From the **Protocol** drop-down list, select the protocol. The protocols supported are **ICMP**, **IGMP**, **IPv4_ENCAP**, **TCP**, **UDP**, **IPv6_ENCAP**, **RSVP**, **GRE**, **IPSEC_ESP**, **IPSEC_AH**, and **L2TP**.

7. From the **Sources** drop-down list, select the source.
8. In the **Source IP Address** field, enter the IP address for which you want to perform the test.
9. In the **Port** field, enter the port number.
10. In the **Destination IP Address** field, enter the IP address for which you want to perform the test.
11. In the **Port** field, enter the port number.
12. Click **Run**.

The output is displayed in the **Device Output** section.

In the **Data plane** test, the **Port** fields are optional. When you select the **ICMP** protocol, the **Port** fields are disabled.

Figure 518 *Data Plane—Device Output*



Data Plane—Node Details

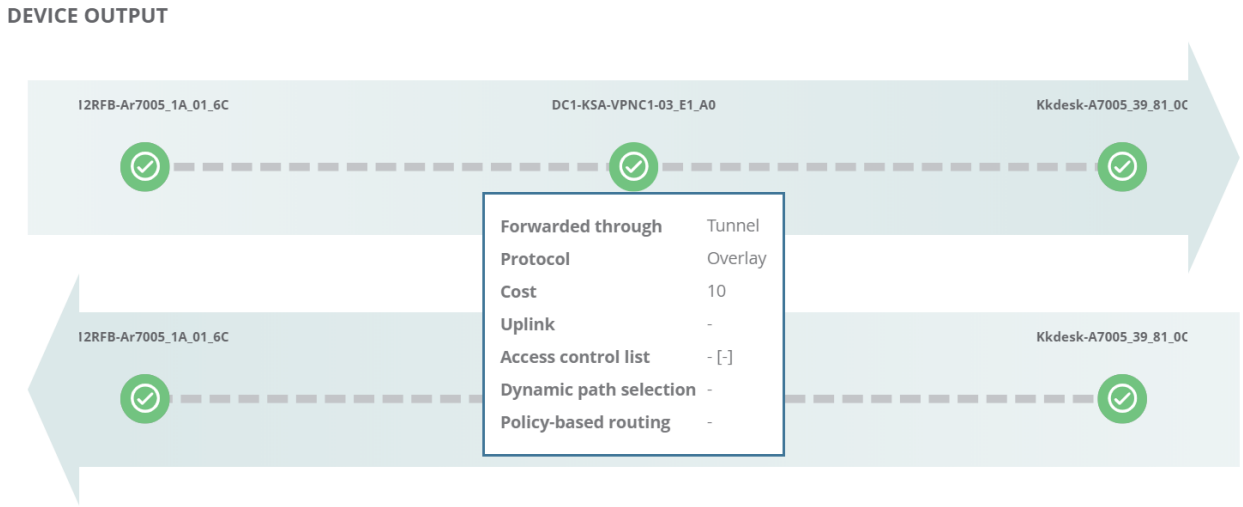
When you click on a node, a pop-up displays information that allows the user to analyze the data at every node in the forward and reverse path.

Gateway and VPNC—Node Details

When you click a Gateway node or a VPNC node in a forward or reverse path, the pop-up displays the following information:

- **Forwarded through**—Displays the name of the network path.
- **Protocol**—Displays the type of protocol.
- **Cost**—Displays the metric value of the path cost.
- **Uplink**—Displays the name of the uplink.
- **Access control list**—Displays the firewall ACL/ACE rules applied for the session.
- **Dynamic path selection**—Displays the SD-WAN DPS policy applied for the session.
- **Policy-based routing**—Displays the PBR policy applied for the session.
- **Error description**—Displays the error message associated with a specific error.

Figure 519 *Gateway and VPNC—Node Details*



Node-Specific Error Messages

In the diagnostic tests, when an error occurs, the **Error description** parameter appears in the pop-up of that specific node. The icon for that specific node changes to an error icon.

The following are few error messages:

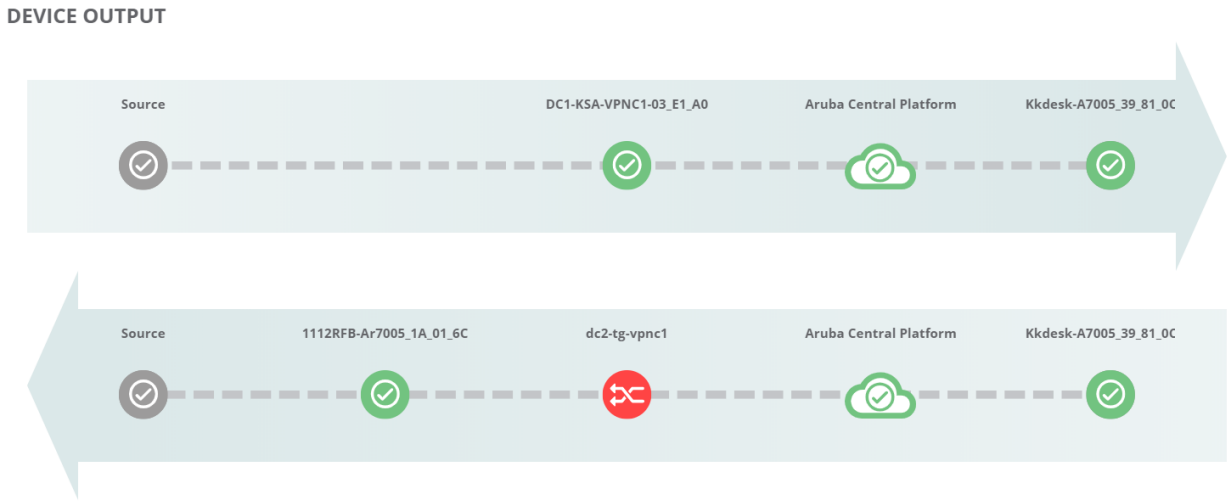
- **Session not found**—Error message states that the device does not have any session entry for the specified parameters, such as source IP, destination IP, protocol, source port, or destination port, and the packet flow did not reach the device.
- **ACL denied**—Error message states that the session has hit a firewall ACL/ACE deny rule and the packets are dropped by the device.
- **Reverse packet not seen**—Error message states that the device has forwarded the packets to the next hop in the forward direction but is yet to receive any packets from that next hop device.
- **Connection test stopped here due to incompatible device firmware**—Error message states that the device firmware is incompatible to run the diagnostic tests.

Asymmetric Routing

Asymmetric routing occurs when the forward traffic traverses from a source to a destination in one path but the reverse traffic follows a different path from the destination to source. For example, forward traffic from Branch B1 traverses via VPNC A and the reverse traffic traverses via VPNC A to reach Branch B1. Asymmetric path is when the reverse traffic traverses via VPNC B to reach Branch B1.

The diagnostic tests detect asymmetric routing in a control plane path and data plane path.

Figure 520 *Asymmetric Routing*



Routing Loop

Routing Loop is a network failure in which the traffic is continuously routed back and forth between two hops rather than reaching the destination host.

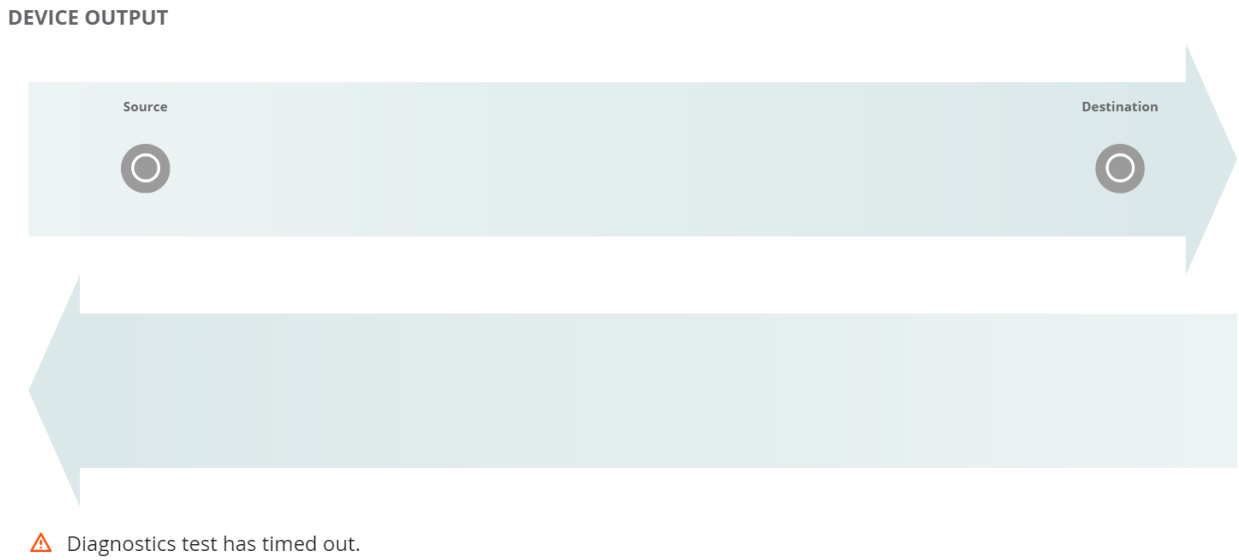
The diagnostic tests detect routing loop issues in a control plane path and data plane path.

Error Notifications

The following are a few error notifications:

- **Diagnostics test has timed out**—Error message states that the diagnostic test is not completed within the expected delay of 60 seconds. The reason for the time out can be one of the following:
  - The back-end is still querying a gateway.
  - The device fails to answer for a reason.
  - Occurs even after partial path data is collected and displayed.
- **Diagnostics test request cannot be fulfilled**—Error message states that the diagnostic test request is not fulfilled. The reason for the failure of the request can be because invalid parameters are entered in the diagnostic test request or while querying for the diagnostic test result.
- **Diagnostics test is unavailable**—Error message states that the test cannot be completed and indicates that the back-end or the source gateway is down.
- **Diagnostics test has failed**—Default error message to indicate errors other than mentioned above.

Figure 521 *Error Message*



Filtering Commands

In order to streamline the debug process and avoid huge data generation while troubleshooting, few commands enable Client MAC address, IP Address, and Port filtration.

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices**, and then click **Access Points**, **Switches**, or **Gateways**.

        A list of devices is displayed in the **List** view.
     c. Click a device listed under **Device Name**.

        The dashboard context for the device is displayed.
2. Under **Analyze** > **Tools**, click **Commands**.

   The **Commands** page is displayed.
3. Select the device type, **Access Point**, **Switch**, or **Gateway** as required from the drop-down list.
4. Select any command category and the **Commands** pane displays the associated commands.

If you navigate from the device details page, the **Tools** page appears, where the device context is already set and the **Source** field is automatically populated based on your selection.

Mandatory filters— Commands marked with '*'

1. Select a command marked with '*' and click **Add**.

   The **Additional Filters** dialog box appears.

2. Enter the parameters such as, Client MAC address, IP address, port number, port list, or policy name as required.

   The parameters are generated based on the commands selected.
3. Click **Apply**.

In case of mandatory filter commands, if you do no enter the filtering parameters in the additional filters dialog box, the command does not get added to the selected command pane and you cannot perform the troubleshooting.

4. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

Optional filters— Commands marked with '+'

1. Select a command marked with '+' and click **Add**.

   The **Additional Filters** dialog box appears.
2. (Optional) Enter the parameters such as, Client MAC address, IP address, port number, port list, or policy name as required.

   The parameters are generated based on the commands selected.
3. Click **Apply**.

In case of optional filter commands, if you do no enter the filtering parameters in the additional filters dialog box, the command still gets added to the selected command pane and you can perform your troubleshooting.

4. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

If there are multiple devices, select the device for which you want to view the output. It shows the status of the tests as, in progress, complete, and the buffer time.

Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the **Download** icon to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Proximity Tracing

Aruba has introduced a new feature, proximity tracing, to perform queries for contact and location tracing. Proximity tracing complements a host of other tools or techniques geared towards enabling customers to understand their users' movements and interactions, specifically with a focus on combating the COVID-19 pandemic. To increase the scope and help as many people as possible, proximity tracing is offered to both Aruba Central customers (Instant AP) and AirWave customers (Campus AP and Instant AP) including NetInsight campus customers.

Proximity tracing tracks wireless client devices (stations) and associated stations they come into contact with, either directly or through connections to neighboring access points, as well as location tracing. Proximity tracing jobs from NetInsight process wireless client data connected to Instant AP through Aruba Central and wireless client data connected to AP through AirWave connection (AW8).

Proximity tracing efforts work best when devices have a static MAC address and are required to have a unique username. A random MAC address or a constantly changing username complicate the ability to locate an individual user or device and the users they may have come into contact with and may lessen the impact of this tool.

Proximity tracing can be done at global or customer (CID) level for duration of 14 days within the last 21 days. Customer can download the contact username list in a CSV file. The file downloaded shows additional details with username, MAC address, AP, duration, site, and date. To trace contact clients and location, see Contact and Location Tracing.

The Opt-Out feature allows to ignore specific users from being traced. To ignore a set of users, add their MAC address in a TXT file and upload the file. User needs to specifically upload a latest list of MAC addresses which should be ignored. The latest list of MAC addresses should include the complete new set of updated entries including new entries, updated entries, or removed entries. When new file is uploaded, the opt-out clients is updated to a new list. To opt-out clients, see Opt-Out Clients.

Pre-requisites

Proximity tracing has the following pre-requisites for data coming from AirWave Server:

- AirWave Server connection signup should happen through Aruba Central account by creating a new customer account which does not have any Instant AP on-boarded. To signup AirWave Server connection through Aruba Central by creating a new customer account, see AirWave Server Connection Signup Through Aruba Central.
- Devices (AP and wireless clients) should be present in customer network coming through AirWave.
- If duplicate usernames exist, an imputed username is derived by taking the MAC address.
- If a username has more than 5 wireless clients connected during the same hour, an imputed username derived by taking the MAC address is used instead.
- If the device generates random MAC address, it is mapped to the same username if it remains unique.
- If a user inputs both username and MAC address, the search results is based on the username.

- If a username keeps changing in a network, the results are processed with the username that is used most in the day.

Contact and Location Tracing

To trace contact clients and location:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Tools > Proximity Tracing**.
3. Enter the values for the parameters listed in the following table.

Enter either the username or MAC address.

Table 339: *Contact Tracing*

Mode	Description
Username	Client name.
MAC Address	MAC address of the client.
Start Date	Start date within the last 21 days.
End Date	End date within the last 21 days. End date cannot be more than 14 days from start date.

4. Click **Trace Contacts/Locations**.

   The traced contacts are listed under **Contact Usernames** table and the location under **Locations** table.

If the username does not return any result, enter the MAC address. Contact and location tracing work best when devices have a static MAC address and are required to have a unique username. A random MAC address or a constantly changing username complicate the ability to locate an individual user or device and the users they may have come into contact with and may lessen the impact of this tool.

5. Optionally, click **Download** to download the traced contacts or locations as a CSV file.

The CSV file contains additional information than what is displayed in the **Contact Usernames** table and **Locations** table and can be used for advanced analysis.

Opt-Out Clients

To opt-out specific clients from being traced, save the MAC address of the clients as a TXT file and upload it to Aruba Central.

The uploaded opt-out list will overwrite the previous list of opt-out entries. The latest list of MAC addresses should include the complete new set of updated entries including new entries, updated entries, or removed entries.

In the opt-out clients TXT file, enter each MAC address on a new line in the following format:

xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx, where x is a case-insensitive hexadecimal number.

For example:

```
00:1B:44:11:3A:B7
30-65-EC-6F-C4-58
f0c3717d06d1
```

To upload the opt-out clients file:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Tools > Proximity Tracing**.
3. Click the configuration icon.
4. In the **Opt-out Clients** tab, click **No file uploaded (text file only)** and select the TXT file.
5. Click **Upload**.

NOTE

To download the current opt-out list, click **Download**.

AirWave Server Connection Signup Through Aruba Central

To complete AirWave Server connection signup through Aruba Central:

1. Navigate to **Sign Up for Aruba Central** site.
2. Under **Account Details**, enter an email address and password. Under **Customer Details**, enter the requisite details. If you are already a Aruba Central user, it is recommended to use the same account. If you are a Aruba Central user and an AirWave user for Data center, create a new account for AirWave as both data sources are different.
3. Select an Aruba Central Server based on your region.
4. Select **Network Operations** for **Interested Apps**.
5. Click **I agree to the Terms and Conditions**.
6. Click **Sign Up**.
7. An email is sent to the registered email address. In that email, click **Activate your account here** or click the URL provided to activate the account.
8. After the account is verified, you will be redirected to the **Aruba Central Login** site. Log in with the registered credentials.
9. In the **Welcome to Aruba Central** page, select **Evaluate Now**.
10. Click **Exit Workflow**.
11. In the **Exit Workflow** pop-up, click **Exit Now**.
12. In the **Network Operations** app, set the filter to **Global**.
13. Under **Analyze**, click **Tools > Proximity Tracing**.
14. Click the configuration icon.
15. Click **AirWave Connection** tab. Under **Status**:
    - **Provision** shows **Not Provisioned**
    - **Connection** shows **Not Connected**
    - **Data Access** shows **Enabled**

    These parameters cannot be modified while provisioning.

NOTE

If you signed-in using a TID loaded with Instant AP, the **AirWave Connection** tab is not available.

16. Under **Connection Settings**, both **Customer ID** and **Email Address** are auto-filled and cannot be edited. The values for both are obtained from the logged in user. For **Secret**, enter a value or click **Generate**.

17. After a secret is entered or generated, click Copy to Clipboard. Paste and save the secret along with customer ID and email address securely. These are required during AW8 configuration.
18. Click **Save**. The page automatically refreshes and under **Status**:
    - **Provision** shows **Provisioned**
    - **Connection** shows **Not Connected**
    - **Data Access** shows **Enabled**

The **Secret** is hashed and cannot be viewed after it is saved.

19. After provisioning is completed, under **Status**:
    - **Provision** shows **Provisioned**
    - **Connection** shows **Connected**
    - **Data Access** shows **Enabled**

AirWave Configuration

To configure AirWave to send information to Aruba Central:

1. Log in to AirWave.
2. Select 3.

```
AirWave Management Platform 8.2.11.1.20200628.0336 on localhost.localdomain
1  Files >
2  Backups >
3  Configuration >
4  System >
5  Users >
6  Support >
7  Security >
8  Advanced >
q  >> Quit
Your choice:3
```

3. Select 6.

```
Configuration
1  Configure Network Settings
2  Set Hostname
3  Set Timezone
4  Certificates >
5  SSHD >
6  CLT >
b  >> Back
Your choice:6
```

4. Select 1.

```
CLT1  Configure CLT
2  Reconfigure CLT
3  Remove CLT
4  Test CLT GW connectivity
b  >> Back
```

```
Your choice:1
Running Configure CLT
Before configuring AW8 for CLT, you are required to Sign Up on Central first.
You will require Customer ID, Email and Secret used on Central during SignUp.
You will also need to allow access from AW8 to
https://nookgw.netinsight.arubanetworks.com/ on tcp-port 443.
https://cltanalytics.s3-us-west-2.amazonaws.com on tcp-port 443
For more details, please refer to Installation Documents or contact your local
SE.
Would you like to continue? (y/N) :  y
nter your Customer ID: <enter customer ID copied from Aruba Central>
Enter your CLT email ID: <enter email address copied from Aruba Central>
secret: <enter secret copied from Aruba Central>
CLT configured successfully.
Hit return to continue ...
```

Removing AirWave Connection

When you remove a AirWave connection, the original provisioning information will be available for a maximum of 24 hours before it is removed. If the AirWave Server was accidentally removed, it is recommended to wait for at least 24 hours before provisioning the AirWave Server again and completing AirWave configuration.

To remove AirWave connection from Aruba Central:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Tools > Proximity Tracing**.
3. Click the configuration icon.
4. Click **AirWave Connection** tab.
5. Under **Remove AirWave Connection**, click **Remove AirWave Connection**.
6. In the **Remove AirWave Connection** pop-up, click **Remove AirWave Connection**.

Disabling Data Access

To disable access to proximity data:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Tools > Proximity Tracing**.
3. Click the configuration icon.
4. Click **AirWave Connection** tab.
5. Slide the **Enable Data Access** toggle to the left.

Density Tracing

Density tracing jobs from the NetInsight process collects details of Instant AP data connected through Aruba Central and Campus AP through AirWave Connection (AW8) which have users or devices that are densely populated.

Density tracing takes the location tracing one step further. The location tracing information is aggregated across all users for each customer and converted to a heatmap of 5 minute usage for all access points. To save space, the data is compacted and uploaded once a day. The user can download the data and perform further analysis. The data could be delayed at the most by 24 hours (Aruba Central) or 48 hours (AirWave).

Access points and wireless clients should be present in the network coming through AirWave. No Instant AP devices should be part of Central Customer account. AirWave Server connection or signup should happen through Aruba Central which does not have any on-boarded Instant AP.

Density tracing is available Aruba Central in the Global view under Tools > Proximity Tracing. Density tracing can be done at global or customer account level in Aruba Central for duration of 5 days within the last 21 days.

To enable density tracing:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Tools > Proximity Tracing**.
3. Click **Density Tracing**.
4. Search for Density Tracing IAP List by selecting a time period between two dates.
5. Click **File Download** to download the list of APs which are densely populated.

The downloaded CSV file contains columns based on density tracing schema.

- time_epoch = ts in epoch_seconds
- access_point_mac = apmac
- bin_<N> = buckets of density count, Nth 5-minute block relative to ts
  - 1 day = 1440 minutes / 5 = 288
  - Hence the range for bin is 0 to 287
  - Example: bin_3 = count for 5 minutes starting (ts + (5 minutes * 3))

Drop Username for AirWave Data

You may drop username for AirWave data and usernames will not be stored or uploaded to Aruba Central for tracing. You will be able to trace devices using the MAC Address.

To drop usernames for AirWave data:

1. In the **Network Operations** app, set the filter to **Global**.
2. Under **Analyze**, click **Tools > Proximity Tracing**.
3. Click the configuration icon.
4. Click **AirWave Connection**.
5. Click **Drop Username**.

In the next hour, after the job runs successfully, usernames will not be collected anymore from the devices for proximity tracing. You will not be able to search based on Usernames. Proximity tracing works using MAC address and the username of the devices is not displayed.

Aruba Central allows you to access various device and network management applications, and services from the portal. The app selector on the left navigation pane shows the application services that you have subscribed for and the device management applications for the devices you have provisioned in Aruba Central.

This section includes the following topics:

Guest Access

The guest management feature allows guest users to connect to the network and at the same time, allows the administrator to control guest user access to the network.

Aruba Central allows administrators to create a splash page profile for guest users. Guest users can access the Internet by providing either the credentials configured by the guest operators or their respective social networking login credentials. For example, you can create a splash page that displays a corporate logo, color scheme and the terms of service, and enable logging in from a social networking service such as Facebook, Google, Twitter, and LinkedIn.

Businesses can also pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

To enable logging using Facebook, Google, Twitter, and LinkedIn credentials, ensure that you create an application (app) on the social networking service provider site and enable authentication for that app. The social networking service provider will then issue a client ID and client secret key that are required for configuring guest profiles based on social logins.

Guest operators can also create guest user accounts. For example, a network administrator can create a guest operator account for a receptionist. The receptionist creates user accounts for guests who require temporary access to the wireless network. Guest operators can create and set an expiration time for user accounts. For example, the expiration time can be set to 1 day.

Cloud guest feature runs on the AP Foundation License. For more information, see Aruba Central License Feature Details.

Guest Access Dashboard

The **Summary** page in the **Manage > Guest Access** application provides a dashboard displaying the number of guests, guest SSID, client count, type of clients, and guest connection for the selected group.

Table 340 describes the contents of the **Guest Access Overview** page:

Table 340: *Guest Access Overview Page*

Data Pane Item	Description
Time Range	Time range for the graphs and charts displayed on the **Overview** pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month.
Guests	Number of guests connected to the SSIDs with Cloud Guest splash page profiles.
Guest SSID	Number of guest SSIDs that are configured to use the Cloud Guest splash page profiles.
Avg. Duration	The average duration of client connection on the SSIDs with Cloud Guest splash page profiles.
Max Concurrent Connections	Maximum number of client devices connected concurrently on the guest SSIDs.
Guest Connection (graph)	Time stamp for the client connections on the cloud guest for the selected time range.
Guest Count by Authentication	Number of client devices based on the authentication type configured on the cloud guest SSIDs.
Guest Count by SSID	Number of guest connections per SSID.
Client Type	Type of the client devices connected on the guest SSIDs.

Creating Apps for Social Login

The following topics describe the procedures for creating applications to enable the social login feature:

- Creating a Facebook App
- Creating a Google App
- Creating a Twitter App
- Creating a LinkedIn App

Creating a Facebook App

Before creating a Facebook app, ensure that you have a valid Facebook account and you are registered as a Facebook developer with that account.

To create a Facebook app, complete the following steps:

1. Visit the Facebook app setup URL at https://developers.facebook.com/apps.
2. From **My Apps**, select **Add a New App**.
3. Enter the app name and your email address in the **Display Name** and **Contact Email** text boxes, respectively.
4. Click **Create App ID**.
5. Hover the mouse on **Facebook Login** and select **Setup**.
6. Click **Web** (that is, the WWW platform).
7. Enter the website URL in the **Site URL** box.

   This URL is the same as the server URL mapped in the splash page configuration.
8. Click **Save**.

9. Read through the Next Steps section for further information on including Login Dialog, Access Tokens, Permissions, and App Review.
10. Go to **PRODUCTS > Facebook Login > Settings** from the left navigation menu.
11. Click the **Client OAuth Login** toggle switch to turn to **Yes**.
12. Enter the OAuth URI in the **Valid OAuth redirect URIs** box.

    The URI is the server URL mapped in the splash configuration with **/oauth/reply** appended to it. To get the valid Oauth redirect URL, go to the **Guest Access > Splash Pages** path and click the eye ( ) icon available against the specific splash page name in the **Splash Pages** table.

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://example1.cloudguest.arubanetworks.com/oauth/reply.

13. From the left navigation menu, select **App Review**.
14. Select the **Make <App Name> Public** toggle switch to make your app available to public.
15. Click **Category**.
16. In the **Choose a Category** pop-up window, select a category.
17. Click **Confirm**.
18. Select other extra permissions you want to provide for the users of your app.

    There are 41 permissions available for you to select from.
19. Click **Add xx Items**, where x represents the number of permissions you selected.
20. Enter the reason for providing specific permissions and click **Save**.
21. Click **Submit for Review**.
22. On the left navigation pane, click the **Settings** icon.

    Note the app ID and app secret key. Use the app ID and secret key when configuring Facebook login in the Aruba Central UI.
23. Under **App Domains**, enter the server URL.

Creating a Google App

Before creating a an app for Google based login, ensure that you have a valid Google account.

To create a Google app, complete the following steps:

1. Access the Google Developer site at https://code.google.com/apis/console.
   a. To select an existing project, click **Select a project** and select the desired project. If the project is not created, click **Create a project**, enter the project name and click **Create**.
   b. Click **APIs & Services**.
   c. Click **Enable APIs and Services**.
   d. Navigate to **Social** category, and then click **Google API**. The **Google API** window opens.
   e. To enable the API, click **Enable**.
   f. Click **Create Credentials**. If the credentials are already created, click **Go to credentials**.
   g. In the **Credentials** pane, perform the following actions:
      i. Under the **Where will you be calling the API from** section, select **Web Browser**.
      ii. Under the **What data you will be accessing** section, select **User Data**.
      iii. Click **What Credentials do I need**.
2. Under **Create an OAuth 2.0 client ID**. Enter the **OAuth 2.0 Client ID Name**.

3. Under **Authorized JavaScript Origins**, enter the base URL with FQDN of the cloud guest instance that will be hosting the captive portal. For example, https://%hostname%/.
4. Under **Authorized Redirect URIs**, enter the cloud server OAuth reply URL that includes the FQDN of the cloud server instance with /oauth/reply appended at the end of the URL.

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://example1.cloudguest.examplenetworks.com/oauth/reply.

5. Click **Create Client ID**.

   Under **Set up the OAuth 2.0 consent screen**, provide your **Email Address** and product name, and then click **Continue**. The client ID is displayed.
6. Click **Done**. A page showing the OAuth Client IDs opens.
7. Click the **Oauth client ID** to view the client ID and client secret key.

   Use this client ID and client secret key when configuring Google login in the Aruba Central UI.

Creating a Twitter App

Before creating a Twitter app, ensure that you have a valid Twitter accosunt.

To create a Twitter app, complete the following steps:

1. Visit the Twitter app setup URL at https://apps.twitter.com.
2. Click **Create New App**. The **Create an application** web page is displayed.
3. Enter the application name and description.
4. For OAuth 2.0 Redirect URLs, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source, and append /oauth/reply at the end of the URL.

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://exa.example.com/oauth/reply.

5. Select **Yes, I agree** to accept the Developer Agreement terms.
6. Click **Create a Twitter application**.
7. Click **Manage Keys and Access Tokens**.

   The **Keys and Access Tokens** tab opens. The consumer key (API key) and consumer secret (API key) are displayed.
8. Note the ID and the secret key. The consumer key and consumer secret key when configuring Twitter login in Aruba Central UI.

Creating a LinkedIn App

Before creating a LinkedIn app, ensure that you have a valid LinkedIn account.

To create a LinkedIn app, complete the following steps:

1. Visit the LinkedIn app setup URL at https://developer.linkedin.com.
2. Click **My Apps**. You will be redirected to https://www.linkedin.com/secure/developer/apps.
3. Click **Create Application**. The **Create a New Application** web page is displayed.
4. Enter your company name, application name, description, website URL, application logo with the specification mentioned, application use, and contact information.
5. Click **Submit**. The **Authentication** page is displayed.

6. Note the client ID and client secret key displayed on the **Authentication** page.
7. For **OAuth 2.0 Redirect URLs**, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source and append /oauth/reply at the end of the URL.
8. Click **Add** and then click **Update**. The API and secret keys are displayed.
9. Note the API and secret key details. Use the API ID and secret key when configuring LinkedIn login in the Aruba Central UI.

Configuring a Guest Splash Page Profile

This topic describes the following procedures:

- Adding a Guest Splash Page Profile
- Customizing a Splash Page Design
- Previewing and Modifying a Splash Page Profile
- Localizing a Guest Portal
- Associating a Splash Page Profile to an SSID

Adding a Guest Splash Page Profile

To create a splash page profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Guests** to display the **Splash Pages**.
   You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the **+** icon.
   The **New Splash Page** pane is displayed.
4. On the **Configuration** tab, configure the parameters described in the following table:

Table 341: *Splash Page Configuration*

Data Pane Content	Description
Name	Enter a unique name to identify the splash profile. **NOTE:** If you attempt to enter an existing splash profile's name, Aruba Central displays a message stating that **Splash page with this name already exists**.
Type	Configure any of the following authentication methods to provide a secure network access to the guest users and visitors. ■ **Anonymous** ■ **Authenticated** ■ **Facebook Wi-Fi**
Anonymous	Configure the **Anonymous** login method if you want to allow guest users to log in to the Splash page without providing any credentials. For anonymous user authentication, you can also enable a pre-shared key to allow access. To enable a pre-shared key based authentication, set the **Guest Key** to ON and specify a password.

Table 341: *Splash Page Configuration*

Data Pane Content	Description
Authenticated	Configure authentication and authorization attributes, and login credentials that enable users to access the Internet as guests. You can configure an authentication method based on sponsored access and social networking login profiles. The authenticated options available for configuring the guest splash page are described in the following rows.
Username/Password	The **Username/Password** based authentication method allows pre-configured visitors to obtain access to wireless connection and the Internet. The visitors or guest users can register themselves by using the splash page when trying to access the network. The password is delivered to the users through print, SMS or email depending on the options selected during registration. To allow the guest users to register by themselves: 1. Enable **Self-Registration**. 2. Set the **Verification Required** to **ON** if the guest user account must be verified. 3. Enable the **Bypass Apple Captive Network Assistant (CNA)** to bypass the CNA on the iOS devices. Enabling CNA bypass allows users to bypass the Apple Captive Network Assistant pop-up on their iOS devices. However, users still need to verify their credentials with a browser. When the CNA bypass is disabled, the iOS clients have to enter the credentials in the CNA pop-up on their devices. The **Bypass Apple Captive Network Assistant (CNA)** toggle button is displayed only when **Verification Required** is enabled. Users can either enable or disable CNA bypass based on their requirement. 4. Specify a verification criteria to allow the self-registered users to verify through email or phone. ▪ If email-based verification is enabled and the **Send Verification Link** is selected, a verification link is sent to the email address of the user. The guest users can click the link to obtain access to the Internet. ▪ If phone-based verification is enabled, the guest users will receive an SMS. The administrators can also customize the content of the SMS by clicking on **Customize SMS**. 5. Specify the duration within the range of 1-60 minutes, during which the users can access free Wi-Fi to verify the link. The users can log in to the network for the specified duration and click the verification link to obtain access to the Internet. By default, the expiration date for the accounts of self-registered guest users is set to infinite during registration. The administrator or the guest operator can set the expiration date after registration.
Social Login	**Social Login**—Enable this option to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google, or LinkedIn and sign into a third-party website. When a social login based profile is configured, a new login account to access the guest network or third-party websites is not required.

Table 341: *Splash Page Configuration*

Data Pane Content	Description
	■ **Facebook**— Allows guest users to use their Facebook credentials to log in to the splash page. To enable Facebook integration, you must create a Facebook app and obtain the app ID and secret key. For more information on app creation, see Creating a Facebook App. Enter the app ID and secret key for client ID and client Secret respectively to complete the integration. ■ **Twitter**—Allows guest users to use their Twitter credentials to log in to the splash page. To enable Twitter integration, you must create a Twitter app and obtain the app ID and secret key. For more information, see Creating a Twitter App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. ■ **Google**—Allows guest users to use their Google credentials to log in to the splash page. To enable Google integration, you must create a Google app and obtain the app ID and secret key. For more information, see Creating a Google App. ◦ Enter the app ID and secret key for client ID and client secret respectively. ◦ To restrict authentication attempts to only the members of a Google hosted domain, enter the domain name in the **Gmail for Work Domain** text box. Ensure that you have a valid domain account licensed by Google Domains or Google Apps. For more information see: • https://apps.google.com/intx/en_in/ • https://domains.google.com/about/ ◦ Specify a text for the Sign-In button. ■ **LinkedIn**—Allows guest user to use their LinkedIn credentials to log in to the splash page. To enable LinkedIn integration, you must create a LinkedIn app and obtain the app ID and secret key. For more information, see Creating a LinkedIn App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration.
Facebook Wi-Fi	If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the **Facebook Wi-Fi** option. The Facebook Wi-Fi feature allows you to pair your network with a Facebook business page, thereby allowing the guest users to log in from Wi-Fi hotspots using their Facebook credentials. If the Facebook Wi-Fi business page is set up, when the users try to access the Internet, the browser redirects the user to the Facebook page. The user can log in with their Facebook account credentials and can either check in to access free Internet or skip checking in and then continue.
Facebook Wifi Configuration	After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration. 1. Click the **Configure Now** link. 2. Sign in to your Facebook account. 3. If you do not have a business page, click **Create Page**. For more information on setting Facebook Wi-Fi service, see **Setting up Facebook Wi-Fi for Your Business** at https://www.facebook.com/help/126760650808045.

Table 341: *Splash Page Configuration*

Data Pane Content	Description
	NOTE: Instant AP devices support Facebook Wi-Fi services on their own, without Aruba Central. However, for enabling social login based authentication, the guest splash pages must be configured in Aruba Central. For more information on Facebook Wi-Fi configuration on an Instant AP, see the *Aruba Instant User Guide*.
Allow Internet In Failure	To allow users access the Internet when the external captive portal server is not available, click the **Allow Internet In Failure** toggle switch. By default, this option is disabled.
Override Common Name	To override the default common name, click the **Override Common Name** toggle switch and specify a common name. The common name is the web page URL of the guest portal. By default, the common name is set to **securelogin.arubanetworks.com**. The guest users can override this default name by adding their own common name. If your devices are managed by AirWave and you want to use your own certificate for the captive portal service, ensure that the captive portal certificate is pushed to the Instant AP from the AirWave management system. When the appropriate certificate is loaded on the AP, perform the following actions: 1. Run the **show captive-portal-domains** command at the Instant AP command prompt. 2. Note the common name or the internal captive portal domain name. 3. Add this domain name in the **Override Common Name** field on the **Splash Page** configuration page. 4. Save the changes.
Guest Key	To set password for anonymous users, enable the Guest Key and enter a password.
Sponsored Guest	Enable the **Sponsored Guest** option to provide authorization control to a guest sponsor for allowing and denying a guest from accessing the network.
Allowed Sponsor Domains	Enter accepted company domain names. The domain name must match the suffix of the sponsor's email address. The domain names must be company names and not any public domain names such as Gmail, Yahoo, and so on. To add more domain names, click the add icon and enter the domain name. This is a mandatory field.
Allowed Sponsor Emails	Enter the allowed email addresses. If you leave this field empty, all emails that correspond to the allowed domains list are permitted to sponsor guests. To add more sponsor emails, click the add icon and enter the sponsor's email address. This is an optional field.
Authentication Success Behavior	If **Anonymous** or **Authenticated** option is selected as the guest user authentication method, specify a method for redirecting the users after a successful authentication. Select one of the following options: ▪ **Redirect to Original URL**— When selected, upon successful authentication, the user is redirected to the URL that was originally requested. ▪ **Redirect URL**— Specify a redirect URL if you want to override the original request of users and redirect them to another URL.

Table 341: *Splash Page Configuration*

Data Pane Content	Description
Authentication Failure Message	If the **Authenticated** option is selected as the guest user authentication method, enter the authentication failure message text string returned by the server when the user authentication fails.
Session Timeout	Enter the maximum time in Day(s): Hour(s): Minute(s) format for which a client session remains active. The default value is 0:8:00. When the session expires, the users must re-authenticate. If MAC caching is enabled, the users are allowed or denied access based on the MAC address of the connective device.
Share This Profile	Select this check box if you want to allow the users to share the Splash Page profile. The Splash Page profiles under All Devices can be shared across all the groups. **NOTE:** When you clone an existing group, the unshared splash page profile in the existing group is not cloned to the new group. In the existing group, if an unshared splash page is associated with a guest network, then the splash page value is empty in the guest network of the new group.
Daily Usage Limit	Use this option to set a data usage limit for authenticated guest users, anonymous profiles, and Facebook Wi-Fi logins. By default, no daily usage limit is applied. To set a daily usage limit, use one of the following options: ▪ **By Time**— Specify the time limit in hours and minutes for data usage during a day. When a user exceeds the configured time limit, the device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified time zone. ▪ **By Data**— Specify a limit for data usage in MB. You can set this limit to either **Per User**, **Per Session**, or **Per Device**. When the data usage exceeds the configured limit, the user device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified time zone. ◦ **Per User**— This option applies the data usage limit based on authenticated user credentials. ◦ **Per Session**—This option applies the data usage limit based on user sessions. ◦ **Per Device**—This option applies the data usage limit based on the MAC address of the client device connected to the network. **Important Points to Note** ▪ The values configured for this feature do not serve as hard limits. There might be a slight delay in enforcing daily usage limits due to the time required for processing information. ▪ For anonymous and Facebook Wi-Fi logins, the daily usage limit is applied per MAC address of the client device connected to the network.
Allowlist URL	To allow a URL, click + and add the URL to the allowlist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the allowlist, so that the users can access the required web pages.

Customizing a Splash Page Design

To customize a splash page design, complete the following steps:

1. In the **Network Operations** app, set the filter to a group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Guests** to display the **Splash Pages**.
   You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the **+** icon.
   The **New Splash Page** pane is displayed.
4. To customize a splash page design, on the **Guest > Splash Page > New Splash Page > Customization** pane, configure the parameters described in the following table:

Table 342: *Splash Page Customization*

Data Pane Content	Description
Layout	To customize the page layout based on the device type. Specify a layout by selecting one of the following options: ▪ **Horizontal, better for computers** ▪ **Vertical, better for phones** The horizontal layout is selected by default. To change the layout, click the drop-down list and select the required layout type.
Background color	To change the color of the splash page, select a color from the **Background Color** palette.
Button color	To change the color of the sign in button, select a color from the **Button Color** palette.
Header fill color	Select the fill color for the splash page header from the **Header fill color** palette.
Page font color	To change the font color of the text on the splash page, select a color from the **Page font color** palette.
Page font Color	Select the font color of the splash page from the palette.
Logo	To upload a logo, click **Browse**, and browse the image file. Ensure that the image file size does not exceed 256 KB.
Background Image	Click **Browse** to upload a background image. Ensure that the background image file size does not exceed 512 KB.
Page Title	Add a suitable title for the splash page.
Welcome Text	Enter the welcome text to be displayed on the splash page. Ensure that the welcome text does not exceed 20,000 characters.
Terms & Conditions	Enter the terms and conditions to be displayed on the splash page. Ensure that the terms and conditions text does not exceed 20000 characters. The text box also allows you to use HTML tags for formatting text. For example, to highlight text with italics, you can wrap the text with the HTML tag. Specify an acceptance criteria for terms and condition by selecting any of the following options from the **Display "I Accept" check box**: ▪ **No, Accept by default** ▪ **Yes, Display check box** If the **I ACCEPT** check box must be displayed on the Splash page, select the display format for terms and conditions.

5.

Data Pane Content	Description
	Ensure that **Display Option For Terms & Conditions** has the Inline Text option auto-selected and displayed as an uneditable text.
Ad Settings	If you want to display advertisements on the splash page, enter the URL in the **Advertisement URL**. For **Advertisement Image**, click **Browse** and upload the image.

Localizing a Guest Portal

To localize a guest portal, complete the following steps:

1. In the **Network Operations** app, set the filter to a group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Guests** to display the **Splash Pages**.
   You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the **+** icon.
   The **New Splash Page** pane is displayed.
4. To localize or translate the Guest portal content, on the **Guest > Splash Page > New Splash Page > Localization** pane, configure the parameters described in the following table:

These are optional settings unless specified as a required parameter explicitly.

Table 343: *Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Login Section		
Login button title	Enter the custom label text to be localized for the **Login** button.	1–255 characters
Network login title	Enter the custom title text that you want to localize for the **Network Login** page.	1–255 characters
Login page title	Enter the custom text for title in the **Login** page.	1–255 characters
Access denied page title	Enter the custom title text for the **Access Denied** page.	1–255 characters
Logged in title	Enter the custom **Logged in** title text for the page that allows access.	1–255 characters
Username label	Enter the custom text for **Username** lable.	1–255 characters

5.

Table 343: *Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Username placeholder	Enter the custom text to show in in the **Username** placeholder.	1–255 characters
Password placeholder	Enter the custom text to show in in the **Password** placeholder.	1–255 characters
Email address placeholder	Enter the custom text to show in in the **Email Address** placeholder.	1–255 characters
Register button title	Enter the custom title text for **Register** button.	1–255 characters
Network login button title	Enter the custom title text for **Network Login** button.	1–255 characters
Terms and Conditions title	Enter the custom text to show in the **Terms and Conditions** title.	1–255 characters
I accept the Terms and Conditions' text	Enter the custom text to show for the **'I accept the Terms and Conditions'** text adjacent to the check box.	Up to 20000 characters
Welcome Text	Enter a custom Welcome text to the guest portal user.	Up to 20000 characters
Login failed message	Enter a custom text to show for the **Login Failed** message when a user's login attempt gets denied or fails.	Up to 20000 characters
Logged in message	Enter a custom text to show for the **Logged in** message in the access allowed page.	Up to 20000 characters
Register Section		
Phone help message	Enter a custom help message to show for the **Phone** help field.	Up to 20000 characters
Phone number placeholder	Enter the custom placeholder text for the **Phone Number** input UI control.	1–255 characters
'Back' button text	Enter the custom text label to show for the **Back** button control.	1–255 characters
'Continue' button text	Enter the custom text label toshow for the **Continue** button control.	1–255 characters
Email radio button	Enter a custom text label for the **Email** option.	—
Phone radio button	Enter a custom label text for the **Phone** option.	—
Register page title	Enter a custom title text for the **Register** page.	1–255 characters

Table 343: *Guest Portal Localization*

Data Pane Content	Description	Allowed Length of Text
Accept button title	Enter a custom title text for the **Accept** button.	1–255 characters
Register Page instructions	Enter a custom message to show in the **Register** page.	Up to 20000 characters
Verification Section		
Verification code label	Enter a custom text to show for the **Verification code** label.	1–255 characters
Verification code placeholder	Enter a custom text to show for the **Verification code** placeholder.	1–255 characters
Verification email check message	Enter a custom text for the **Verification Email Check** message. This is shown in the verification pending page.	Up to 20000 characters
Verification email notice message	Enter a custom text for the **Verification Email Notice** message. This is the message notifying the user when the email will be sent.	Up to 20000 characters
Verification email sent message	Enter a custom text for the **Verification Email Sent** message.	Up to 20000 characters
Verification phone notice message	Enter a custom text for the **Verification Phone Notice** message. This is the message notifying the user that an SMS has been sent.	Up to 20000 characters
Verified account message	Enter a custom text for the **Verified Account** message. This is the message that will be shown in the Verified page.	Up to 20000 characters
Verify account message	Enter a custom text for the **Verify Account** message. This is the message that will be shown in the Verify page.	Up to 20000 characters
Verify button title	Enter a custom label text for the **Verify** button.	1–255 characters
Verify title	Enter a custom text for **Verify** title.	1–255 characters
Network login message	Enter a custom text message to show in the **Network Login** page.	Up to 20000 characters

6. Click **Preview** to preview the localized guest portal page or click **Finish**.

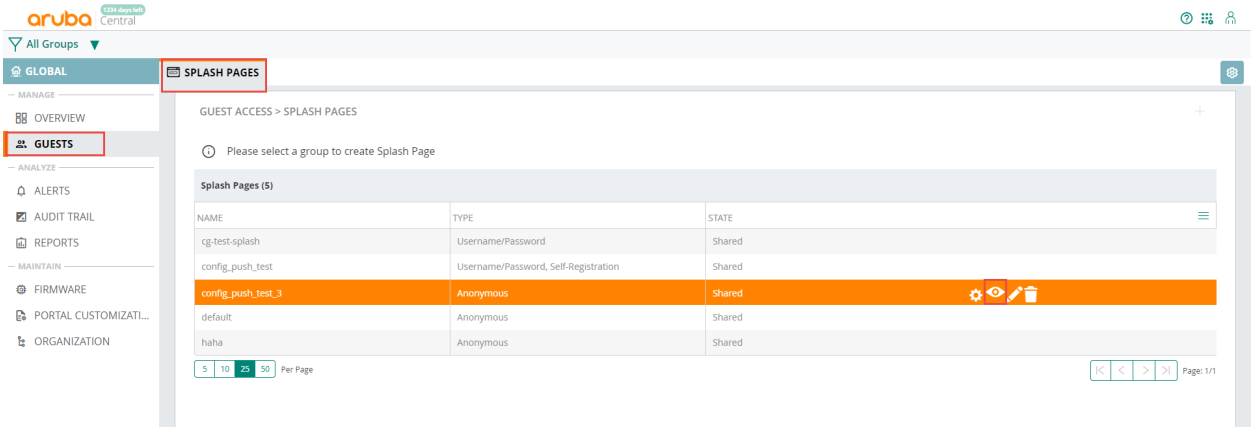
Previewing and Modifying a Splash Page Profile

To preview a splash page profile, complete the following steps:

1. In the **Network Operations** app, set the filter to a group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Guests** to display the **Splash Pages**.
   A list of splash page profiles is displayed.

3. Ensure that the pop-up blocker on your browser window is disabled.
4. Hover over the splash profile you want to preview and click the preview icon. The Splash Page is displayed in a new window.

Figure 522 *Splash Pages Tab*



The **Splash Pages** page also allows you to perform any of the following actions:

- To view the Splash Page configuration text in an overlay window, click the settings icon next to the profile. You can copy the configuration text and apply it to AirWave managed APs using configuration templates.
- To modify a splash page profile, click the edit icon ext to the profile form list of profiles displayed in the Splash Page Profiles pane.
- To delete a profile, select the profile and click the delete icon next to the profile.

Associating a Splash Page Profile to an SSID

To associate a splash page profile with an SSID, complete the following steps:

1. In the **Network Operations** app, set the filter to a group.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Device** > **Access Points**.
3. Click the **Config** icon.
4. Under **WLANs**, click **+Add SSID**.
5. The **Create a New Network** pane is displayed.
6. Refer to the AP configuration page for Aruba Central Online Help for more detailed information on how to create the network at .

Creating a WiFi4EU Guest Network

Aruba Central allows administrators to create splash page profile specifically for WiFi4EU. The below workflow describes how to set up a WiFi4EU splash page profile.

To create a WiFi4EU splash page, complete the following steps:

1. In the **Network Operations** app, set the filter to a group.
   The dashboard context for the group is displayed.

2. Under **Manage**, click **Guests**.

   The **Guest Access > Splash Pages** page is displayed.
3. Click the + icon to create a new splash page.
4. On the **Configuration** tab, configure the parameters based on your requirement. Ensure that the name of the splash page is **WiFi4EU**. Refer Adding a Guest Splash Page Profile for details on creating a new splash page.

To associate a splash page profile with an SSID, complete the following steps:

1. Under **Manage**, click **Guests**.
2. Click the **Config** icon.

   The **Guest Access > Guest Network** page is displayed.
3. Click **Create Guest Network**.

   The **Create Guest Network** page is displayed.
4. In **SSID**, enter **WiFi4EU**.
5. In the **Security** option, select **Open** or **WPA2-PSK**.

   If you selected the WPA2-PSK option, enter a password in **Passphrase** to access the guest network.
6. Select **WiFi4EU** splash page profile from the **Splash page** drop-down-list.
7. Click **Add** to enter the required time settings.
8. Click **Save** in the **Create Guest Network** pane. The guest network profile is created and is available for the specified time frame.

To associate the WiFi4EU API with the WiFi4EU splash page, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

   The **API Gateway** page is displayed.
2. To view the **Swagger** interface, click the link in the **Documentation** column.

   The documentation is displayed in a new window.
3. In **URL**, select **Guest** from the drop-down list.
4. In **API Reference**, select **WiFi4EU**.
5. Under **Parameters**, enter the network ID provided by the WiF4EU organization and enter the required two letter language code.
6. Click **Try**.

   The WiFi4EU settings get pushed to the WiFi4EU Splash page. Refer Viewing Swagger Interface for details.

Configuring Visitor Accounts

The **Visitors** pane displays information on the session and account details of the visitors who access the splash page. It helps you monitor the guest sessions.

The MSP does not support creating or modifying guest visitor accounts. To configure visitors for WLAN networks and view visitor connection details, the administrators must drill down to the customer account and access it.

Adding a visitor

To add a new visitor, perform the following steps:

1. From the MSP view, drill down to a customer account.
2. In the **Network Operations** app, navigate to **Manage > Guests > Visitors.**
   The **Guest Access > Visitors** page is displayed.
3. Click on the **Account** tab, and then click **Add Visitor**.
   The **Add Visitor** pane is displayed.
4. Configure the parameters described in the following table:

Table 344: *Adding Visitors*

Data Pane Content	Description
Name	Enter a unique name to identify the visitor.
Company	Enter the company name of the visitor.
Email	Enter the email ID of the visitor.
Phone	Enter the phone number of the visitor.
Password	■ Click **Generate**. The automatically generated password is displayed in the **PASSWORD** text box. ■ Select **Send Access Code** to send the access code by email or SMS.
Valid Till	Specify the duration for the visitor account to expire in Day(S): Hour(s): Minute(s) format. To allow users to access the network for unlimited period of time, select **Unlimited**.
Enable	Select this check box to activate the user account.

5. Click **Save**.
6. Click **Save and Print** to print the details of the visitor.

To view the guest or visitor sessions, perform the following steps:

1. From the MSP view, drill down to a customer account.
2. In the **Network Operations** app, navigate to **Manage > Guests > Visitors.**
   The Guest Access > Visitors page is displayed.
3. From the **Show visitors for network** drop-down list, select a network.

The following table displays the session details of the visitor:

Table 345: *Visitor Sessions Pane*

Data Pane Content	Description
Visitors	Displays the name of the visitor.
Login Type	Displays the login type of the client (**Anonymous**, **Username/Password**, **Self-Registration**, **Facebook Wi-Fi**).

Data Pane Content	Description
Browser	Displays the type of browser that the client is connected.
MAC Address	Displays the MAC address of the connected client device.
Device Type	Displays the type of the device.
OS Name	Displays the OS on the client device.
Login Time	Displays the login time of the client.
Session Time (Secs)	Displays the duration for which the client is connected.

The following table displays the account details of a visitor:

Table 346: *Visitor Accounts Pane*

Data Pane Content	Description
Name	Displays the name of the visitor.
Email	Displays the email ID of the visitor.
Phone	Displays the contact number of the visitor.
Company	Displays the company name of the visitor.
Status	Indicates if the user account is in active or inactive state.
Creation	Displays the date and time on which the visitor account is created.
Expiration	Displays the date and time on which the visitor account expired.
Actions	Allows you to edit a specific visitor account.

You can filter the visitors displayed in the **Account List** by visitor status. Select **Active**, **Inactive**, or **Show All** from the drop-down list.

Deleting Visitors

To delete one or more visitors, perform the following steps:

1. Select the visitor or visitors you want to delete using the **Multiselect** box option.
2. Click **Delete**. The selected visitors get deleted.

Downloading Visitor Account Details

To download the visitor account details, click the **Download** option available in the **Accounts** tab.

Presence Analytics

Presence Analytics enables businesses to collect and analyze user presence data in public venues, enterprise environments, and retail hubs. Presence Analytics also enables businesses to collect real-time data on user

footprints within the wireless network range of Aruba Instant APs that are managed using Aruba Central. Using the Presence Analytics statistics, businesses can analyze user behavior and improve customer engagement, and thus maximize revenue opportunities, optimize workspace, and increase market presence.

Aruba Central supports Presence Analytics only on the APs running Aruba Instant 6.4.4.4-4.2.3.0 or a later version.
After Aruba Central is upgraded to 2.5.2, the Presence Analytics historical data is not retained and all the existing clients are considered as new clients.
To properly manage devices with Presence Analytics, ensure that the devices are associated with a particular site.

Enabling Presence Analytics

From Aruba Central 2.5.2 release onwards, **Presence Analytics** does not require a separate service subscription. If you had assigned a service subscription prior to Aruba Central 2.5.2 release, you can remove the service subscription and use the same subscription for either Cloud Guest or UCC.

Presence Analytics does not require a service token and is disabled by default.

To enable **Presence Analytics** on your Instant AP, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The **Global** dashboard is displayed.
2. Under **Manage**, click **Guests** > **Presence Analytics**.
3. Click the **Config** icon.
4. Turn on the **Enable all Access Points to collect data for sites analytics** toggle switch.
   The **Presence Analytics** license gets enabled on all devices for the particular account.

If Presence Analytics was enabled on any of the Instant APs before 2.5.2 upgrade, then after upgrade, Presence Analytics is enabled by default on all the Instant APs in the network. However, Presence and Loyalty statistics are displayed only for the Instant APs on which the Presence Analytics feature is enabled.

Using Presence Analytics

Presence Analytics displays data either for all sites or per site. A site in Aruba Central represents a physical location such as a venue or store. If your account does not have any sites configured, ensure that you create a site. For more information on creating sites and adding devices, see Managing Sites.

The **Presence Analytics** page displays the following menu options:

- **List**—Displays a list view of site analytics for all the sites in the account, or the selected site.
- **Summary**—Displays the graphical view of the Passerby metrics, the Loyal Visitors, Visit Frequency, and the Visit Status.
- **Configuration**—Allows you to enable data collection from access points.

List

The **Site Analytics** table lists the data for all sites connected to the network. To view analytics data for a specific site, in the **Network Operations** app, set the filter to a site. The specific site data is displayed. By default, the Site Analytics table displays the following columns: **Site**, **Unique Passerby**, **Unique Visitor**,

Draw Rate, **Visit**, **Loyal Visitor**, **Average Dwell Time**, and **Connected Visit**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

To download the site data into a CSV format, click the download icon. Aruba Central generates the CSV report of all the sites or the selected site in the network.

Table 347: *Site Analytics Data Metrics and Filters*

Dashboard View	Description
Time range filter	You can view the clients' presence data for a selected time range. Click the time range filter and select the **From** date and **To** date. Click **Apply**. The table displays the analytics data for the selected time range.
Site	Displays the name of the sites or site in the network.
Unique Passerby	Displays the aggregate count of unique passerbys for the selected time range.
Unique Visitor	Displays the aggregate count of unique visitors for the selected time range.
Draw Rate	Displays the percentage of passerby that is converted to visitors for the selected time range.
Visit	Displays the total number of visits made by clients for the selected time range. This includes the repeat visits made by a particular client.
Loyal Visitor	Displays the aggregate count of the visitors categorized as loyal. Visitors who have visited a site more than once in the last 1 month are referred to as loyal visitors.
Average Dwell Time	Displays the average time spent by visitors at a site for the selected time range.
Connected Visits	Displays the total number of visits connected to the Aruba SSID for the selected time range.

Summary

The **Summary** view provides a statistical analysis of the **Passerby**, **Loyal Visitors**, **Visit Frequency**, and **Visit Status** in a graphical representation. The graph can be populated for the following time range:

- Hourly—Data for the an hour, with the current time taken as the basis for calculation.
- Daily—Data for the last 24 hours, with 00:00 hour of the current day taken as the basis for calculation.
- Weekly—Data for the last 1 week, with 00:00 hour of the current week taken as the basis for calculation.

Select the specific time period from the time range filter. **Hourly** and **Daily** data is populated if the filter is set from 24 hours to 48 hours. **Daily** and **Weekly** data is displayed is the filter is set from 2 days till a month.

Passerby

An associated or unassociated client who is in the vicinity of a specific site and has an RSSI value greater than -90 dBm. You can customize the RSSI value for Passerby on the **Presence Analytics** > **Configuration**

page. The Passerby graph shows the aggregate count of passerby clients for the selected time range. The graph also shows the following details:

- The total count of visits versus the passerby details for the selected time range.

Loyal Visitors

Based on the engagement pattern and the time spent by the clients at the site, Aruba Central classifies clients as visitors. It also maintains a record of the number of repeat visits made by these clients over a specific duration. Based on these records, it plots the frequency at which the visitors return to the sites, and classifies these repeat visitors as loyal visitors.

The **Loyal Visitors** graph provides a statistical analysis of the clients classified as loyal visitors for a given time range. The graph also shows the following information:

- The total count of visitors versus the loyal visitors for the selected time range.

Visit Frequency

The visit frequency displays the total count of how many times a loyal visitor visited a site repeatedly. The graph displays the frequency distribution of visits made by visitors to the site. The graph also shows the following information:

- The number of loyal visitors versus their total visits in the last 3 months.

Visit Status

Visits are monitored when clients are either connected to an Aruba SSID or disconnected from it. These visits can either be an employee connected visit or a guest connected visit. The **Visit Status** displays a pie chart for the connected versus the not connected visits from the total number of visits for a specified time range. The total number of visits by all visitors (including loyal) for the selected time range is also displayed.

Configuration

The **Configuration** tab provides a collective data of all the traffic related to passerby and visitors from the APs connected to each site. The **Data Collection** table lists the data for all sites connected to the network. By default the table displays the following columns: **Site**, **Passerby Threshold**, **Visitors Threshold**, **Conversion Time**, and **Access Points**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

Table 348: *Data Collection Table*

Dashboard View	Description
Site	Displays the name of the sites or site in the network.
Passerby Threshold	Displays the set RSSI threshold for the passerbys in dBm.
Visitors Threshold	Displays the set RSSI threshold for the visitors in dBm.

Table 348: *Data Collection Table*

Dashboard View	Description
Conversion Time	Displays the dwell time in minutes set for each site.
Access Points	Displays the total number of Instant APs with Presence Analytics enabled on them versus the total number of Instant APs connected to the site. For example, if a certain site has 4 Instant APs and only 2 Instant APs have Presence Analytics enabled, the **Access Points** column displays **2/4**.

Setting RSSI Threshold and Dwell Time for a Site

The RSSI and dwell time configuration allows the administrators to perform the following actions:

- Classify the type of client.
- Analyze presence patterns.
- Determine if the usage has increased over a period of time.

To modify the default RSSI thresholds and dwell time configuration parameters for a site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Site**.
   The dashboard context for the selected site is displayed.
2. Under **Manage**, click **Guests** > **Presence Analytics**.
3. Click the **Config** icon.
4. In the **Data Collection** table, click the **Edit Threshold** icon.
   The **Thresholds** window is displayed.
5. Under **Visitors**, specify the value for **RSSI threshold**. By default, the RSSI threshold value is set to -65 dBm. You can specify a value within the range of -100 to 0.
6. Under **Passersby**, specify the values for **RSSI threshold**. By default, the RSSI threshold value is set to -90 dBm. You can specify a value within the range of -100 to 0.
7. Under **Conversion**, specify the values for **Dwell Time**. By default, the dwell time is set to 5 minutes.
8. Click **Save**.

Editing Multiple Site RSSI Threshold and Dwell Time

Aruba Central allows you to edit all site thresholds and dwell time simultaneously. Modifying thresholds and dwell time for all sites simultaneously overwrites all default and custom set values. To modify the RSSI thresholds and dwell time configuration parameters for all the sites in the network, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Guests** > **Presence Analytics**.
3. Click the **Config** icon.
4. In the **Data Collection** table, click the **Edit Default Thresholds**.
   The **Thresholds** window is displayed.
5. Select the check box to overwrite the customized sites threshold.

6. Under **Visitors**, specify the value for **RSSI threshold**. By default, the RSSI threshold value is set to -65 dBm. You can specify a value within the range of -100 to 0.
7. Under **Passersby**, specify the values for **RSSI threshold**. By default, the RSSI threshold value is set to -90 dBm. You can specify a value within the range of -100 to 0.
8. Under **Conversion**, specify the values for **Dwell Time**. By default, the dwell time is set to 5 minutes.
9. Click **Save**.

Editing Default RSSI Threshold and Dwell Time

To modify the default RSSI thresholds and dwell time configuration parameters, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Guests** > **Presence Analytics**.
3. Click the **Config** icon.
4. In the **Data Collection** table, click the **Edit Default Thresholds**.
   The **Thresholds** window is displayed.
5. Under **Visitors**, specify the value for **RSSI threshold**. By default, the RSSI threshold value is set to -65 dBm. You can specify a value within the range of -100 to 0.
6. Under **Passersby**, specify the values for **RSSI threshold**. By default, the RSSI threshold value is set to -90 dBm. You can specify a value within the range of -100 to 0.
7. Under **Conversion**, specify the values for **Dwell Time**. By default, the dwell time is set to 5 minutes.
8. Click **Save**.

Editing default thresholds and dwell time changes the default values only, custom set thresholds and dwell time do not change.
The applied configuration changes for the RSSI threshold and dwell time take a maximum of 2 hours to reflect in Aruba Central.
If Presence Analytics is disabled at a customer level, then all site level and customer level thresholds get cleared. Enabling Presence Analytics at customer level again resets the all threshold levels.

Enabling or Disabling Access Points for Each Site

To enable to disable APs associated with each site, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Guests** > **Presence Analytics**.
3. Click the **Config** icon.
4. In the **Data Collection** table, click the **Access Points** icon for the selected site.
   The **Devices Data Collection** window is displayed.
5. Select the APs you want to enable for the selected site. You can enable multiple APs for each site.
6. To disable APs for the selected site, uncheck the AP names from the list of APs. You can disable multiple APs for each site.
7. Click **Save**.

API Gateway

Aruba Central supports a robust set of REST APIs to enable users to build custom applications and integrate the APIs with their applications. The Aruba Central API framework uses OAuth protocol to authenticate and authorize third-party applications, and allows them to obtain secure and limited access to an Aruba Central service.

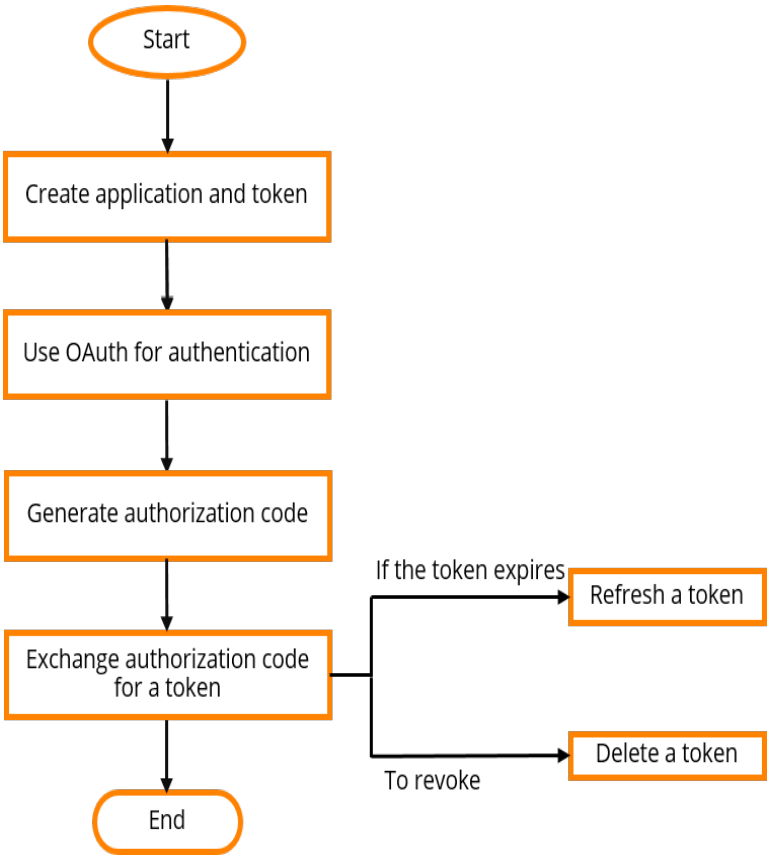
This section includes the following topics:

API Gateway and NB APIs

The **API Gateway** feature in Aruba Central supports the REST API for all Aruba Central services. This feature allows Aruba Central users to write custom applications, embed, or integrate the APIs with their own applications. The REST APIs support HTTP GET and POST operations by providing a specific URL for each query. The output for these operations is returned in the JSON format.

For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. The access tokens provide a temporary and secure access to the APIs. The access tokens have a limited lifetime for security reasons and the applications should use the refresh API to obtain new tokens periodically (every 2 hours).

The following figure illustrates the API gateway workflow for the users:



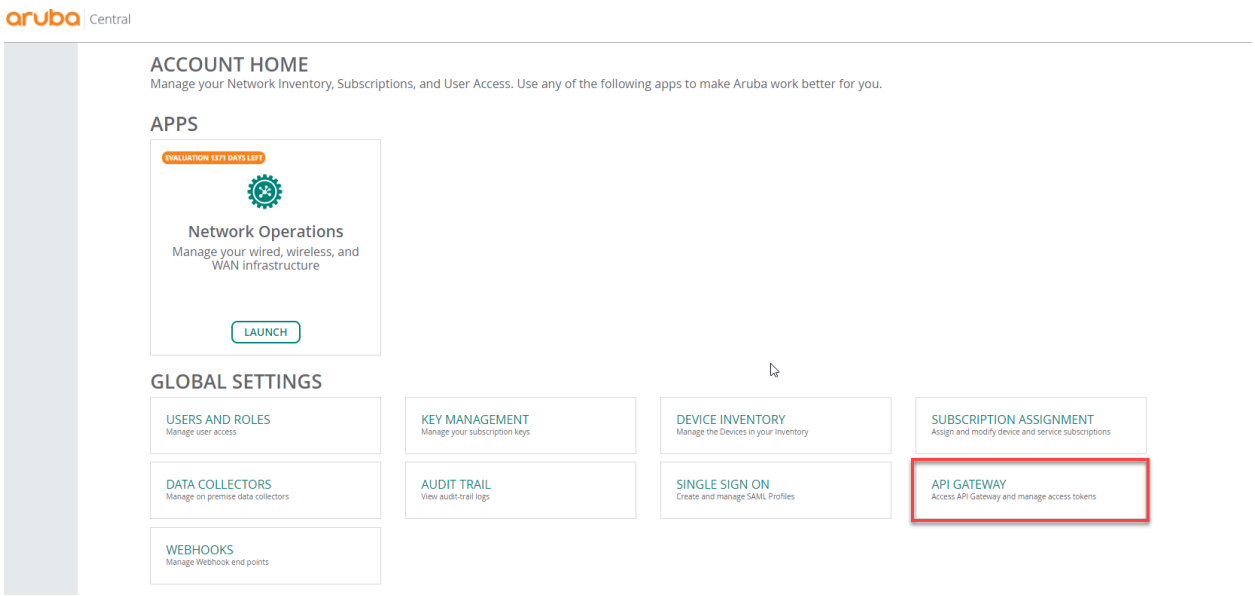
Accessing API Gateway

To access the API Gateway:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

   The **API Gateway** page is displayed. You can get new tokens and refresh old tokens. To obtain a new token application, you must set authentication parameters for a user session.

Figure 523 *Account Home Page with API Gateway Option Page*



Important Points to Note

- The admin user profile of MSP has **System Apps & Tokens** tab which displays all the apps and tokens generated locally in the admin user profile. This tab also displays all the apps created in the non-admin user profiles. Clicking these apps lists out all the associated tokens created for the non-admin user profile.
- Administrator role is specific to an app and hence the administrator account related RBAC library APIs and decorators must contain the application name as one of the parameters in the access verification query.
- The decorators associated with **Account Home**, **Network Operations**, or **ClearPass Device Insight** must contain **account_setting**, **central**, or **optik** as app names respectively, as one of the parameters.

Domain URLs

The following table shows the region-specific domain URLs for accessing API Gateway:

Table 349: *Domain URLs for API Gateway Access*

Region	Domain Name
US-1	app1-apigw.central.arubanetworks.com
US-2	apigw-prod2.central.arubanetworks.com
EU-1	eu-apigw.central.arubanetworks.com
Canada-1	apigw-ca.central.arubanetworks.com
China-1	apigw.central.arubanetworks.com.cn
APAC-1	api-ap.central.arubanetworks.com
APAC-EAST1	apigw-apaceast.central.arubanetworks.com
APAC-SOUTH1	apigw-apacsouth.central.arubanetworks.com

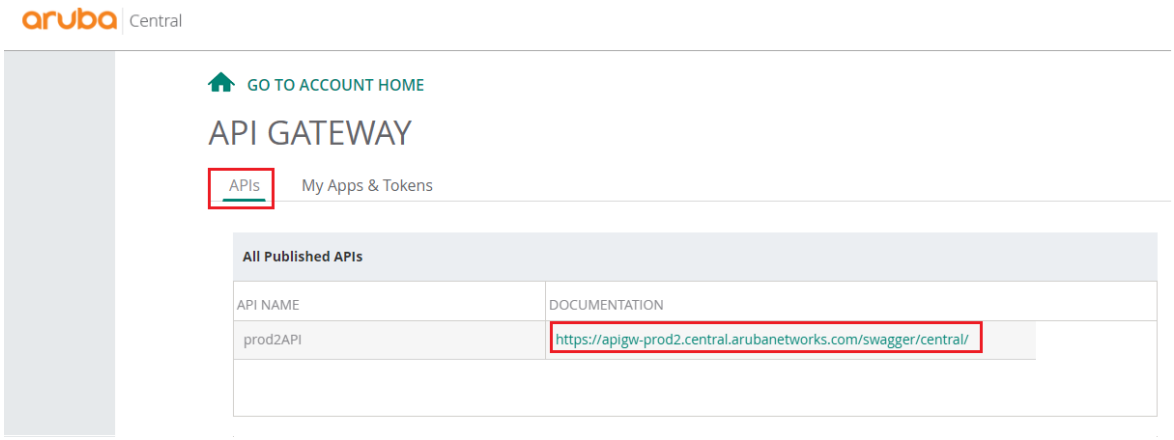
The procedures described in this article use app1-apigw.central.arubanetworks.com as an example. Ensure that you use the appropriate domain URL when accessing API Gateway or generating tokens.

Viewing Swagger Interface

To view the APIs managed through Aruba Central, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
   The **API Gateway** page with the list of published APIs is displayed.
2. To view the Swagger interface, click the link in the **Documentation** column next to the specific published API name. The documentation is displayed in a new window.

Figure 524 *API Gateway Dashboard*



List of Supported APIs

Aruba Central supports the following APIs for the managed devices.

Table 350: *APIs and Description*

API	Description
Monitoring	Gets network, client, and event details. It also allows you to manage labels and switches.
Configuration	Allows you to configure and retrieve the following: ■ Groups ■ Templates ■ Devices
AppRF	Gets Top N AppRF statistics.
Guest	Gets visitor and session details of the portal.
MSP	Allows you to manage and retrieve the following: ■ Customers ■ Users ■ Resources ■ Devices Aruba has enforced a request limit for the following APIs: ■ **GET /msp_api/v1/customers** ■ **GET /msp_api/v1/customers/{customer_id}/devices** ■ **GET /msp_api/v1/devices** ■ **PUT /msp_api/v1/customers/{customer_id}/devices** The maximum limit is set to 50 per API call. If you exceed this limit, the API call returns the HTTP error code 400 and the following error message: **LIMIT_REQUEST_EXCEEDED**.
User Management	Allows you to manage users and also allows you to configure various types of users with a specific level of access control.
Audit Event Logs	Gets a list of audit events and the details of an audit event.

Table 350: *APIs and Description*

API	Description
New Device Inventory	Gets device details and device statistics.
New Licensing	Allows you to manage and retrieve subscription keys.
Presence Analytics	Allows you to configure the Presence Analytics application. It also retrieves site and loyalty data.
Device Management	Allows you to manage devices.
Firmware	Allows you to manage firmware.
Troubleshooting	Gets a list of troubleshooting commands for a specific type of device.
Notification	Gets notification alerts generated for events pertaining to device provisioning, configuration, and user management.
Unified Communications	Retrieves data for all sessions for a specific period of time. It also retrieves the total number of clients who made calls in the given time range and gets the Lync/Skype for Business URL for the Aruba Central cluster that you are using.
Refresh API Token	Allows you to refresh the API token.
Reporting	Gets the list of configured reports for the given customer ID.
WAN Health	Allows you to the following: ■ Get list of configured WAN health policies. ■ Create a new WAN health policy. ■ Delete an existing WAN health policy. ■ Get the details of any specific WAN health policy. ■ Update an existing WAN health policy. ■ Get policy schedule details. ■ Create a schedule for a WAN health policy. ■ Get statistics for WAN health cookie generated for a site. ■ Get WAN health test results. ■ Get WAN health test results for a specific site.
Network Health	Allows you to get data for all the labels and sites.
Webhook	Allows you to add, or delete Webhooks, and get or refresh Webhook tokens. See Webhooks for further details on Webhook.
VisualRF	Allows you retrieve information on floor plans, location of APs, clients and rogue devices.
DPS Monitoring	Gets DPS compliance and session statistics for all the links of a device belonging to a specific policy.

For a complete list of APIs and the corresponding documentation, see https://app1-apigw.central.arubanetworks.com/swagger/central.

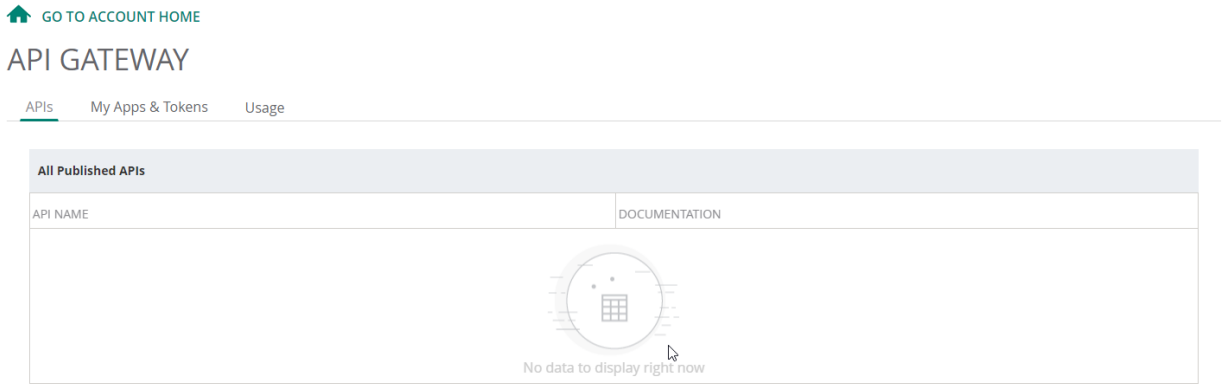
Creating Application and Token

To create an application, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

   The **API Gateway** page is displayed.

Figure 525 *API Gateway Dashboard*



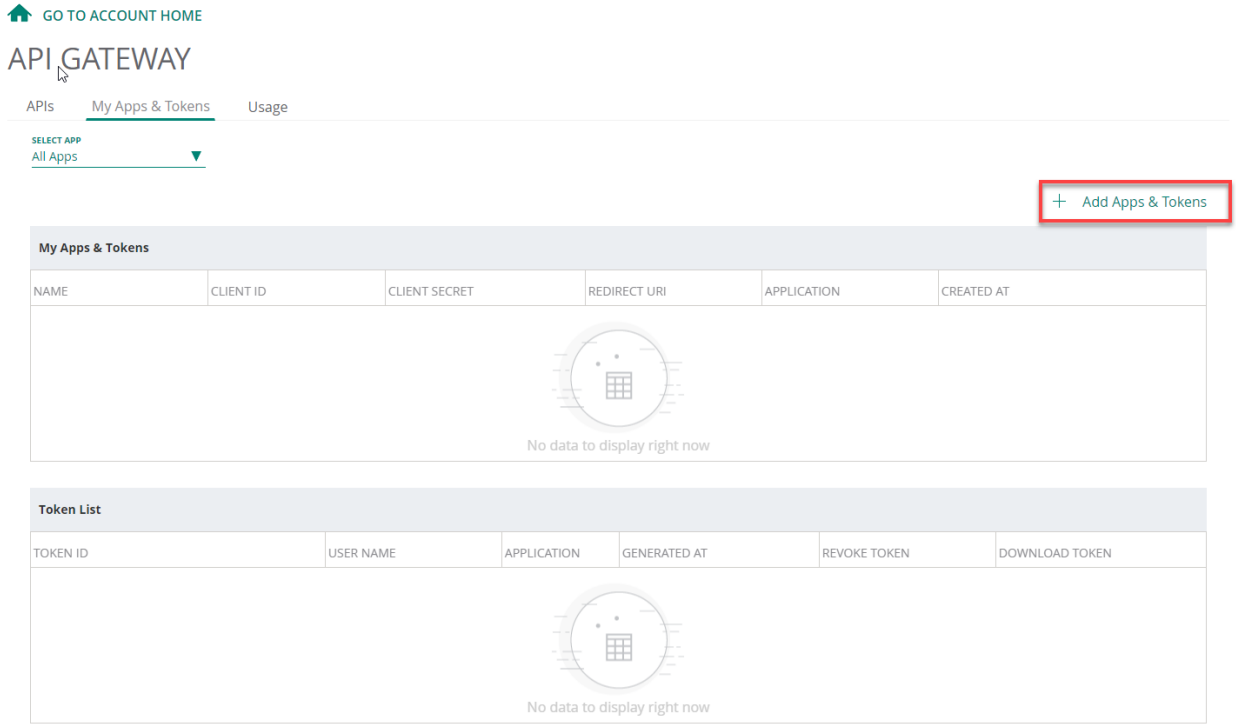
2. Click the **My Apps & Tokens** tab.

NOTE

The admin user will be able to create new apps for all the non-admin user by clicking **+ Add Apps & Tokens** in the **System Apps & Tokens** tab.

3. Click **+ Add Apps & Tokens**.

Figure 526 *Add Apps and Tokens Option Page*



4. In the **New Token** pop-up window, do the following:
    a. Enter the application name. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable.
    b. In the **Redirect URI** field, enter the redirect URL.
    c. From the Application drop-down list, select the application.
    d. Click **Generate**. A new application is created and added to the **My Apps & Tokens** table. The **My Apps & Tokens** table displays the following details:
        - **Name**—Name of the application. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable. Any new tokens generated in non-admin user profile is associated with the same application name.
        - **Client ID**—Unique ID for each application.
        - **Client Secret**—Unique secret ID for each application.
        - **Redirect URI**—Redirect URL.
        - **Application**—Name of the application. For example, Network Operations.
        - **Tokens**—Token created for the application. The option is available to admin user profile only.
        - **Created At**—Date on which the application was created.

To delete the added application, click delete icon on the row corresponding to an application and click **Yes** to delete that application.

Only admin users will be able to generate tokens with multiple application names. In non-admin user profile, the **Application Name** field contains the user name and is non-editable. Any new tokens generated in non- admin user profile is associated with the same application name. However, all the multiple application names and the associated tokens in non-admin user profiles from the earlier versions is retained in the **Token List** table.

Using OAuth 2.0 for Authentication

For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. OAuth 2.0 is a simple and secure authorization framework. It allows applications to acquire an access token for Aruba Central through a variety of work flows supported within the OAuth 2.0 specification.

All OAuth 2.0 requests must use the SSL endpoint available at https://app1-apigw.central.arubanetworks.com.

Access and Refresh Tokens

The access token is a string that identifies a user, app, or web page and is used by the app to access an API. The access tokens provide a temporary and secure access to the APIs.

The access tokens have a limited lifetime. If the application uses web server or user-agent OAuth authentication flows, a refresh token is provided during authorization that can be used to get a new access token.

If you are writing a long running applications (web app) or native mobile application you should refresh the token periodically. For more information, see Refreshing a token.

This section includes the following topics:

- Obtaining Access Token
- Accessing APIs
- Viewing and Revoking Tokens
- Adding a New Token

Obtaining Access Token

Users can generate the OAuth token using one of the following methods:

- Obtaining Token Using Offline Token Mechanism
- Obtaining Token Using OAuth Grant Mechanism

Accessing APIs

To access the API, use the following URL:

https://app1-apigw.central.arubanetworks.com/.

This endpoint is accessible over SSL and the HTTP (non-SSL) connections are redirected to the SSL port.

Table 351: *Accessing the API*

URL	Description
https://app1-apigw.central.arubanetworks.com/	The API gateway URL. All APIs can be accessed from this URL by providing a correct access token.

The parameters for the API are as follows:

Table 352: *Parameters for the API*

Parameter	Value	Description
`request_path`	URL Path	URL path of an API, for example, to access monitoring APIs, use the path */monitoring/v1/aps*.

Table 353: *Header for the API*

Header	Value	Description
Authorization	`Bearer ouzMaXEBbB6XqGtsWomK7MvaTuhrqDQ1`	Pass the access token in the header.

Example

Request Method: GET

https://app1-apigw.central.arubanetworks.com/monitoring/v1/aps

Request Header:

Authorization: Bearer ouzMaXEBbB6XqGtsWomK7MvaTuhrqDQ1

Response:


```
{
"aps": [
   {
   "firmware_version": "6.4.4.4-4.2.3.1_54637",
   "group_name": "00TestVRK",
   "ip_address": "10.29.18.195",
   "labels": [
   "Filter_242",
   "Ziaomof",
   "roster",
   "242455",
   "Diegso"
   ],
   "macaddr": "6c:f3:7f:c3:5d:92",
   "model": "AP-134",
   "name": "6c:f3:7f:c3:5d:92",
   "radios": [
   {
   "band": 0,
   "index": 1,
   "macaddr": "6c:f3:7f:b5:d9:20",
   "status": "Down"
   },
   {
   "band": 1,
   "index": 0,
   "macaddr": "6c:f3:7f:b5:d9:30",
   "status": "Down"
   }
   ],
   "serial": "AX0140586",
   "status": "Down",
   "swarm_id": "e3bf1ba201a6f85f4b5eaedeead5e502d85a9aef58d8e1d8a0",
   "swarm_master": true
   }
```

```
   ],
"count": 1
}
```

Viewing and Revoking Tokens

To view or revoke tokens, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**. The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**. The **Token List** table displays the following:
   - **Token ID**—Token ID of the application.
   - **User Name**—Name of the user to whom this token is associated to. An application can be associated to multiple users.
   - **Application**—Name of the application to which this token is associated to. For example, Network Operations.
   - **Generated At**—Date on which the token was generated.
   - **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
   - **Download Token**—Click **Download Token** to download the token.

In MSP mode, the admin user profile has **System Apps & Tokens** tab which displays all the apps and tokens generated in all non-admin user profiles in addition to the apps and tokens created in the admin user profile. To view all the tokens of admin and non-admin user, go to **Account Home > Global Settings > API Gateway > System Apps & Tokens**.

Adding a New Token

To add a new token, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.The API Gateway page is displayed.
2. Click **My Apps & Tokens**.

The admin user can create new tokens for all non-admin users by clicking **+ Add Apps & Tokens** in the **System Apps & Tokens** tab.

3. Click **+ Add Apps & Tokens** to add a new token.
4. Enter the application name in the **Application Name** box and click **Generate**.

If you have registered a custom URI when creating a new app under **System Apps and Tokens**, the **Redirect URI** option is disabled for you in the **My Apps and Tokens** tab **> Add Apps and Tokens > New Token** . In such cases, the **Redirect URI** option in **Add Apps and Tokens > New Token** under **My Apps and Tokens** populates your already registered URI.

Obtaining Token Using Offline Token Mechanism

To obtain tokens using the offline token method, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**. The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**.

In the MSP mode, the admin user profile can view the **System Apps & Tokens** tab which displays all the apps and tokens generated in all the non-admin user profiles in addition to the apps and tokens created in the admin user profile.

3. Click **+ Add Apps & Tokens**. The **New Token** pane is displayed.
4. Enter the application name and redirect URI in the **Application Name** and **Redirect URI** fields respectively.
5. Choose the application from the **Application** drop-down list and click **Generate** to generate a new token.
6. The **Token List** table displays the following:
   - **Token ID**—Token ID of the application.
   - **User Name**—Name of the user to whom this token is associated to. An application can be associated to multiple users.
   - **Application**—Name of the application to which this token is associated to. For example, Network Operations.
   - **Generated At**—Date on which the token was generated.
   - **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
   - **Download Token**—Click **Download Token** to download the token.

Obtaining Token Using OAuth Grant Mechanism

The following section describes the steps for obtaining the access token and refresh token using the authorization code grant mechanism:

- Step 1: Authenticate a User and Create a User Session
- Step 2: [Optional] Generating Client Credentials
- Step 3: Generate Authorization Code
- Step 4: Exchange Auth Code for a Token
- Step 5: Refreshing a Token
- Step 6: Deleting a Token

API calls are limited to 1 API per second. This rate-limit is applicable only to the APIs in the first 3 steps mentioned above.

Step 1: Authenticate a User and Create a User Session

The following API authenticates a user and returns a user session value that can be used to create future requests for a client with the specified username and password. It is assumed that you already have a client ID for your application. For more information on how to create an application and obtain tokens, see Creating Application and Token.

Domain URLs allow you to log in to the API gateway server and to establish the user session. This endpoint is accessible over SSL, and HTTP (non-SSL) connections are redirected to SSL port. The following table lists the region specific domain URLs for accessing the API gateway.

If user authentication is successful, the request will return HTTP code 200 and the response header will include the following attributes.

Table 354: *Authentication and User session Response Codes*

Header Key	Values	Description
https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/login?client_id=<client_id>	csrftoken=xxxx; session=xxxx	The server returns a CSRF token and identifies the user session, which must be used for all subsequent HTTP requests.

Example

Request Method: POST

URL: https://app1- apigw.central.arubanetworks.com/oauth2/authorize/central/api/login?client_id=<client_id>

Host: app1-apigw.central.arubanetworks.com

Request Header:

Accept: application/json

Content -Type: application/json

POST Request Body(JSON):

```
{
 "username": "xxxxx",
 "password": "xxxxx"
}
```

Error Response:

```
400: Bad Request
 Response Body (JSON):
 {
  "extra": {},
  "message": "<error string>"
 }
401: Auth failure
 Response Body (JSON):
 {
  "message": "Auth failure",
  "status": false
 }
429: API rate limit exceeded
```

Response Body (JSON):

```
{
 "message": "API rate limit exceeded"
}
```

Success Response:

```
200: OK
```

Response Body (JSON):

```
{
 "status": true
}
```

Response Header:

```
 Set-Cookie: csrftoken=xxxx;session=xxxx;
```

The **csrf token** value received in the successful response message must be used as a parameter for all subsequent POST/PUT requests. The **session** value must also be used for all subsequent requests to maintain the user session context.

Step 2: [Optional] Generating Client Credentials

The following API can be used to generate client credentials for a specific tenant using your Managed Service Provider (MSP) Client ID.

Table 355: *URL to Generate Client Credentials*

URL	Description
https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/client_credentials?client_id=<msp_client_id>	The **<msp_client_id>** variableis the client ID given from Central to that a Managed Service Provider that user registered the application.

Example

Request Method: POST

URI—https://app1-apigw.central.arubanetworks.coms/oauth2/authorize/central/api/client_credentials?client_id=<msp_client_id>

POST Request Body(JSON):

```
{
 "customer_id": "<tenant_id>"
}
```

Request Header: (Values from login API request)

```
 Set-Cookie: csrftoken=xxxx;session=xxxx;
```

Response Body(JSON):

```
{
 "client_id": "<new-client-id>",
 "client_secret": <new-client-secret>"
}
```

Error Response

```
429: API rate limit exceeded
```

Response Body (JSON):

```
{
 "message": "API rate limit exceeded"
}
```

Step 3: Generate Authorization Code

After the user is authenticated and you have a valid session for that user, use this API to get authorization code. The authorization code is valid only for 5 minutes and must be exchanged for a token within that time.

Table 356: *URL for to Generate an Authorization Code*

URL	Description
https://app1 apigw.central.arubanetworks.com/oauth2/authorize/central/api	The endpoint is a POST call to get an authorization code.

Query parameters for this API are as follows:

Table 357: *Query Parameters for the Auth Code API*

Parameter	Values	Description
client_id	**client_id** is a unique hexadecimal string	The **client_id** is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
response_ type	**code**	Use **code** as the response type to get the authorization code that can be exchanged for token
scope	**all** or **read**	Requested API permissions may be either **all** (for both read and write access) or **read** for read-only access.

Example

Request Method: POST

URL: https://app1 - apigw.central.arubanetworks.com/oauth2/authorize/central/api/?client_id=<client_id>&response_type=code&scope=all HTTP/1.1

Host: app1-apigw.central.arubanetworks.com

Request Header:

Accept: application/json Cookie: “session=xxxx” X-CSRF-Token: xxxx

Content -Type: application/json

POST Request Body(JSON):

```
{
 "customer_id": "xxxxx"
}
```

Error Response:

```
400: Bad Request
```

Response Body (JSON):

```
 {
  "extra": {},
  "message": "<error string>"
 }
401: Auth failure
```

Response Body (JSON):

```
 {
  "message": "Auth failure",
  "status": false
 }
```

```
429: API rate limit exceeded
```

Response Body (JSON):

```
{
 "message": "API rate limit exceeded"
}
```

Success Response:

```
200: OK
```

Response Body (JSON):

```
{
 " auth_code ": “xxxx”
}
```

Pass the **csrf-token** value you obtained in step one in the request header, otherwise the request will be rejected. Note the **auth_code** value in the response, as you will use this code to obtain an OAuth token.

Response Header:

```
Set-Cookie: csrftoken=xxxx;session=xxxx;
```

Step 4: Exchange Auth Code for a Token

Once you have an authorization code, you just use that code to request an access from the server. The exchanges should be done within 300 seconds of obtaining the auth code from the previous step, or the API will return an error.

Table 358: *URL for to Generate an Auth Token*

URL	Description
https:// app1- apigw.central.arubanetworks.com/oauth2/token	The endpoint is a POST call to get an access token using the authorization code obtained from the server.

Query parameters for this API are as follows:

Table 359: *Query Parameters for the Auth Code API*

Parameter	Values	Description
client_id	**client_id** is a unique hexadecimal string	The **client_id** is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
client_secret	**client_secret** is a unique hexadecimal string	The **client_secret** is a unique identifier provided to each developer at the time of registration. Application developers can obtain a client ID and client secret when they register with the API gateway admin.
grant_type	**authorization_code**	Use **code** to get the authorization code that can be exchanged for the token.
code	**auth_code** received from step 1	The authorization code received from the authorization server.
redirect_uri	string	The redirect URI must be the same as the one given at the time of registration. This is an optional parameter.

The response to this API query is a JSON dictionary with following values:

Table 360: *Auth Token Values*

Parameter	Values	Description
token_type	bearer	Identifies the token type. Central supports only the bearer token type (See https://tools.ietf.org/html/rfc6750)
refresh_ token	string	Refresh tokens are credentials used to renew or refresh the access_token when it expires without repeating the complete authentication flow. A refresh token is a string representing the authorization granted to the client by the resource owner.
expires_in	seconds	The lifetime, in seconds, of the access token.
access_ token	string	Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client.

Example

Request Method: POST

URL: https: //apigw-prod2.central.arubanetworks.com/oauth2/token?client_id=<Ccentral-API-app-clientid>&client_secret=xxxx&grant_type=authorization_code&code=xxxx \

Content -Type: application/json

Response:

```
{
 "refresh_token": "xxxx",
 "token_type": "bearer",
 "access_token": "xxxx",
 "expires_in": 7200
}
```

Step 5: Refreshing a Token

You can use the refresh token obtained in the previous step to update the access token without repeating the entire authentication process. A refresh token is only required once your access token is expired. You can only refresh a token for a new access token every 15 minutes. For example, when you refresh a new token, you can use the provided access token for 2 hours. If you want a new access token, you have to again refresh the token after 15 minutes from its last refresh.

Table 361: *URL to Refresh a Token*

URL	Description
https://app1-apigw.central.arubanetworks.com/oauth2/token	The endpoint is a POST call to refresh the access token using the refresh token obtained from the server

Query parameters for this API are as follows:

Table 362: *Query Parameters for Refresh Tokens*

Parameter	Value	Description
client_id	**client_id** is a unique hexadecimal string	The **client_id** is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.

Parameter	Value	Description
client_secret	**client_secret** is a unique hexadecimal string	The **client_secret** is a unique identifier provided to each developer at the time of registration. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
grant_type	**refresh_token**	Specify **refresh_token** as the grant type to request that an authorization code be exchanged for a token
refresh_ token	string	A string representing the authorization granted to the client by the resource owner.

The response to this API query is a JSON dictionary with following values:

Parameter	Value	Description
token_type	bearer	Identifies the token type. Only the bearer token type is supported. For more information, see https://tools.ietf.org/html/rfc6750.
refresh_ token	string	Refresh tokens are credentials used to renew or refresh the access token when it expires without going through the complete authorization flow. A refresh token is a string representing the authorization granted to the client by the resource owner.
expires_in	seconds	The expiration duration of the access tokens in seconds.
access_ token	string	Access tokens are credentials used to access the protected resources. An access token is a string representing an authorization issued to the client.

Example

Method: POST

https://apigw-prod2.central.arubanetworks.com/oauth2/token?client_id=<Central-API-app-clientid>&client_secret=xxxx&grant_type=refresh_token&refresh_token=xxxx

Response

```
{
 "refresh_token": "xxxx",
 "token_type": "bearer",
 "access_token": "xxxx",
 "expires_in": 7200
}
```

Step 6: Deleting a Token

To delete the access token, access the following URL:

Table 363: *URL to Delete a Token*

URL	Description
https://app1-apigw.central.arubanetworks.com/oauth2/token	This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to SSL port. Customer ID is a string.

Example

Method : DELETE

URL:https://app1-apigw.central.arubanetworks.com/oauth2/api/tokens

JSON Body:

```
{
 "access_token": "<access_token_to_be_deleted>",
 "customer_id": "<customer_id_to_whom_token_belongs_to>"
}
```

Headers:

Content-Type: application/json

X-CSRF-Token: <CSRF_token_obatained_from_login_API>

Cookie: "session=<session_obatained_from_login_API>"

Viewing Usage Statistics

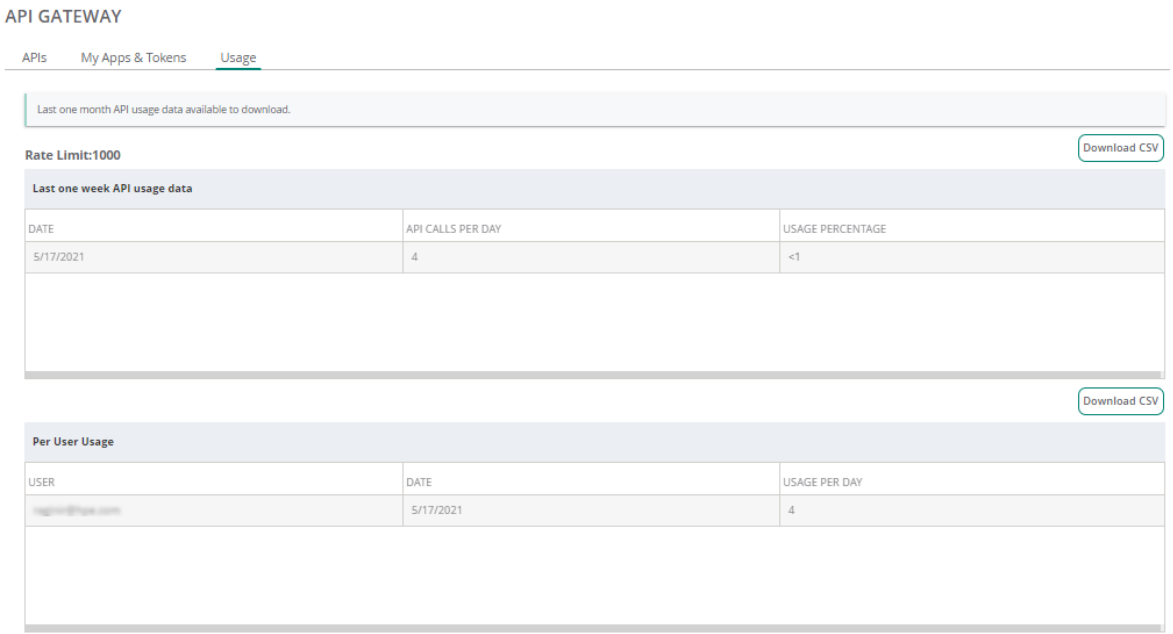
The **API Gateway** page includes the **Usage** tab that displays the API usage. The **Usage** tab is available only for administrators and the usage data is stored only for the previous 30 days. The following details are displayed:

- Assigned rate limit.
- Total usage.
- Per user usage.
- MSP and tenant usage if you are in MSP mode.

To view the usage statistics for users of API Gateway, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**. The **API Gateway** page is displayed.
2. Click **Usage**. The following details are displayed:

   Figure 527 *API Gateway Usage Page*



   a. **Rate Limit**—The total rate limit assigned for API calls for a day and other related details are available in the API response headers.

b. **Total Usage**:
   - **Date**—The date of usage.
   - **Usage Per Day**—Usage per day.
   - **Usage Percentage**—Usage percentage for a specific date.

c. **Per User Usage**:
   - **User**—The name of the user.
   - **Date**—The date on which the application was accessed.
   - **Usage Per Day**—The total usage by the user per day. This is derived based on the total number of API calls made on a per day basis. This is an aggregate across all customers.

d. If you are in MSP mode, the **MSP & Tenant Usage** table is displayed:
   - **Tenant ID**: ID of the tenant account.
   - **Date**: The date on which the application was accessed.
   - **Usage Per Day**: The total usage by the tenant account per day. This is derived based on the total number of API calls made on a per day basis.

The **Usage** tab is only available for administrators and the usage data is stored only for the previous 30 days.

Changes to Aruba Central APIs

This section lists the new APIs, deprecated APIs, alternative APIs, and APIs removed from Aruba Central:

Modified APIs

The following table lists the modified APIs:

Table 364: *Modified APIs*

Modified API	Description
Monitoring > Switch APIs	
▪ **[GET] /monitoring/v1/switch_stacks/{stack-id}/ports** ▪ **[GET] /monitoring/v1/switches/{serial}/ports**	Following fields are added in the response to ensure that the API call gets a list of ports, which includes: ▪ **out_errors** per port ▪ **in_errors** per port
▪ **[GET] /monitoring/v1/switches/{serial}** ▪ **[GET] /monitoring/v1/switch_stacks/{stack_id}**	The **switch_type** field is added to select the type of switch in the API endpoints. Following are the supported values: ▪ **ArubaCX** ▪ **ArubaSwitch** ▪ **MAAS**
▪ **GET /monitoring/v1/switches**	▪ **site** parameter is introduced to filter the switches by site name. ▪ **site** and **stack_id** fields are added to the response to get the site name and stack id details for the switches.

Table 364: *Modified APIs*

Modified API	Description
▪ **GET /monitoring/v1/switches/{serial}**	▪ **site** and **stack_id** fields are added to the response to get the site name and stack id details for the switches. ▪ **nae_aggr_status** field is added to the response that informs about the switch status either as Critical, Major, Minor, Normal, and Warning. This field is only applicable for CX switches.
▪ **GET /monitoring/v1/switch_stacks**	▪ **host_name** parameter is introduced to filter the switches by host name.
Audit Event Logs	
▪ **[GET] /auditlogs/v1/events** ▪ **[GET] /platform/auditlogs/v1/logs**	▪ The **limit** parameter has been enhanced to return 100 audit events. ▪ Following new parameters are introduced to filter audit events by time range: ◦ **start_time**—Start time in epoch seconds. If start time is not specified, current time minus 90 days is automatically filled in as the start time. ◦ **end_time**—End time in epoch seconds. If end time is not specified, current time is automatically filled in as the end time.
Monitoring > Client API	
▪ **[GET] /monitoring/v1/clients/wireless** ▪ **[GET] /monitoring/v1/clients/wired**	**site** parameter is introduced to filter the APIs by site name.
Monitoring > Gateway	
▪ **[GET] /monitoring/v1/gateways**	**site** parameter is introduced to filter the APIs by site name.
Monitoring > Access Points	
▪ **[GET] /monitoring/v1/aps/{serial}**	Following fields are added in the response to get the site and swarm name of the AP : ▪ **site_name** ▪ **swarm_name**
Monitoring > Swarm	
▪ **[GET] /monitoring/v1/swarms**	**swarm_name** parameter is introduced to filter the API by swarm name.
Topology	
▪ **[GET] /{site_id}**	Following fields are added in the response: ▪ **vlans**—lists the vlans configured on the device. ▪ **taggedVlans** and **untaggedVlan**—Lists the tagged and untagged vlan associated to the ports of the edge. This is applicable only for switches.

Deprecated APIs

The following table lists the APIs that have been deprecated. These APIs will continue to function but could be removed in a future release. Aruba strongly discourages the use of these APIs and recommends that you use the alternative API.

Table 365: *Deprecated APIs*

Deprecated API	Alternative API
User Management	
[GET] /accounts/v2/users	**[GET] /platform/rbac/v1/users**
[POST] /accounts/v2/users	**[POST] /platform/rbac/v1/users**
[POST] /accounts/v1/users/change_ password	**[POST] /platform/rbac/v1/users/{user_id}/password**
[POST] /accounts/v1/users/reset_password	**[POST] /platform/rbac/v1/users/{user_id}/password/reset**
[GET] /accounts/v2/users/{user_id}	**[GET] /platform/rbac/v1/users/{user_id}**
[PATCH] /accounts/v2/users/{user_id}	**[PATCH] /platform/rbac/v1/users/{user_id}**
[POST] /accounts/v1/bulk_users	**[POST] /platform/rbac/v1/bulk_users**
[PATCH] /accounts/v1/bulk_users	**[PATCH] /platform/rbac/v1/bulk_users**
[GET] /accounts/v1/status/{cookie_name}	**[GET] /platform/rbac/v1/status/{cookie_name}**
[GET] /accounts/v1/roles	**[GET] /platform/rbac/v1/roles**
[POST] /accounts/v1/roles	**[POST] /platform/rbac/v1/apps/{app_name}/roles**
[GET] /accounts/v1/roles/{rolename}	**[GET] /platform/rbac/v1/apps/{app_name}/roles/ {rolename}**
[DELETE] /accounts/v1/roles/{rolename}	**[DELETE] /platform/rbac/v1/apps/{app_name}/roles/ {rolename}**
[PATCH] /accounts/v1/roles/{rolename}	**[PATCH] /platform/rbac/v1/apps/{app_name}/roles/ {rolename}**
[GET] /accounts/v3/users	**[GET] /platform/rbac/v1/users**
[GET] /accounts/v1/users	**[GET] /platform/rbac/v1/users**
[POST] /accounts/v1/users	**[GET] /platform/rbac/v1/users**
[GET] /accounts/v1/users/{user_id}	**[GET] /platform/rbac/v1/users/{user_id}**
[PATCH] /accounts/v1/users/{user_id}	**[PATCH] /platform/rbac/v1/users/{user_id}**
[POST] /v2/subscriptions/assign	**[POST] /platform/licensing/v1/subscriptions/assign**
Presence Analytics	
[GET] /presence/v2/config/thresholds	**[GET] /presence/v3/config/thresholds**

Table 365: *Deprecated APIs*

Deprecated API	Alternative API
[POST] /presence/v2/config/thresholds	**[POST] /presence/v3/config/thresholds**
[GET] /presence/v2/analytics/aggregates	**NA**
[GET] /presence/v2/analytics/trends	**[GET] /presence/v3/analytics/trends/passerby_visitors**
[GET] /presence/v2/insights/top_sites	**NA**
[GET] /presence/v2/insights/bottom_sites	**NA**
[GET] /presence/v2/insights/sites/aggregates	**[GET] /presence/v3/insights/sites/aggregates**
[GET] /presence/v2/loyalty/aggregates	**NA**
[GET] /presence/v2/loyalty/trends	**[GET] /presence/v3/analytics/trends/loyal_visitors**
[GET] /presence/v2/loyalty/visits	**[GET] /presence/v3/visit_frequency**
▪ **[GET] /presence/v2/loyalty/aggregates/top_sites** ▪ **[GET] [/presence/v2/loyalty/aggregates/bottom_sites** ▪ **[GET] /presence/v2/loyalty/trends/top_sites** ▪ **[GET] /presence/v2/loyalty/trends/bottom_sites** **NOTE:** Expected to be slow for customers with large number of sites.	**NA**
[GET] /presence/v2/loyalty/sites/aggregates	**[GET] /presence/v3/insights/sites/aggregates**
Monitoring > VPN	
▪ **[GET] /monitoring/v1/vpn/usage** ▪ **[GET] /monitoring/v2/vpn/usage**	**[POST] /monitoring/v3/vpn/usage**
Monitoring > Access Points	
[GET] /monitoring/v1/aps	**[GET] /monitoring/v2/aps**
[GET] /monitoring/v2/aps/{serial}/rf_summary	**[GET] /monitoring/v3/aps/{serial}/rf_summary**
▪ **[GET] /monitoring/v1/aps/bandwidth_usage** ▪ **[GET] /monitoring/v2/aps/bandwidth_**	**[GET] /monitoring/v3/aps/bandwidth_usage**

Table 365: *Deprecated APIs*

Deprecated API	Alternative API
usage	
[GET] /monitoring/v1/aps/{serial}/uplink_history	NA
[GET] /monitoring/v1/aps/{serial}/neighbouring_clients	NA
[GET] /monitoring/v1/bssids	[GET] /monitoring/v2/bssids
[GET] /monitoring/v1/aps/bandwidth_usage/topn	[GET] /monitoring/v2/aps/bandwidth_usage/topn
Monitoring > Network	
[GET] /monitoring/v1/networks	[GET] /monitoring/v2/networks
[GET] /monitoring/v1/networks/{network_name}	[GET] /monitoring/v2/networks/{network_name}
[GET] /monitoring/v1/networks/bandwidth_usage	[GET] /monitoring/v2/networks/bandwidth_usage
Deprecated Licensing	
[GET] /subscriptions	[GET] /platform/licensing/v1/subscriptions
[GET] /subscriptions/stats	[GET] /platform/licensing/v1/subscriptions/stats
[GET] /services/enabled	[GET] /platform/licensing/v1/services/enabled
[GET] /subscriptions/assign	[POST] /platform/licensing/v1/subscriptions/assign
[POST] /subscriptions/unassign	[POST] /platform/licensing/v1/subscriptions/unassign
[GET] /services/config	[GET] /platform/licensing/v1/services/config
[DELETE] /subscriptions/devices/all	[DELETE] /platform/licensing/v1/subscriptions/devices/all
[POST] /subscriptions/devices/all	[POST] /platform/licensing/v1/subscriptions/devices/all
[DELETE] /msp/subscriptions/devices/all	[DELETE] /platform/licensing/v1/msp/subscriptions/devices/all
[POST] /msp/subscriptions/devices/all	[POST] /platform/licensing/v1/msp/subscriptions/devices/all
[GET] /autolicensing/services/{service}/status	[GET] /platform/licensing/v1/autolicensing/services/{service}/status
[DELETE] /customer/settings/autolicense	[DELETE] /platform/licensing/v1/customer/settings/autolicense

Table 365: *Deprecated APIs*

Deprecated API	Alternative API
[GET] /customer/settings/autolicense	**[GET] /platform/licensing/v1/customer/settings/autolicense**
[POST] /customer/settings/autolicense	**[POST] /platform/licensing/v1/customer/settings/autolicense**
[DELETE] /msp/customer/settings/autolicense	**[DELETE] /platform/licensing/v1/msp/customer/settings/autolicense**
[GET] /msp/customer/settings/autolicense	**[GET] /platform/licensing/v1/msp/customer/settings/autolicense**
[POST] /msp/customer/settings/autolicense	**[POST] /platform/licensing/v1/msp/customer/settings/autolicense**

Removed APIs

The following table lists the APIs that have been removed and the alternative APIs:

Table 366: *Removed and Alternative APIs*

Removed API	Alternative API
User Management	
[DELETE] /accounts/v1/users/{user_id}	**[DELETE] /platform/rbac/v1/users/{user_id}**
[DELETE] /accounts/v1/bulk_users	**[DELETE] /platform/rbac/v1/bulk_users**
Device Management	
[GET] /configuration/v1/devices/{device_serial}/mobility_master/	**[GET] /device_management/v1/mobility_master/{device_serial}**
[POST] /configuration/v1/devices/{device_serial}/mobility_master/{mm_name}	**[POST] /device_management/v1/mobility_master/{device_serial}/{mm_name}**
WIDS	
▪ **[GET] /monitoring/v1/wids/rogue_aps** ▪ **[GET] /monitoring/v1/wids/interfering_aps**	▪ **[GET] /rapids/v1/rogue_aps** ▪ **[GET] /rapids/v1/interfering_aps** **NOTE:** Rogue Detection is disabled, contact Aruba Support to enable this feature.
[GET] /monitoring/v1/wids/infrastructure_attacks	**[GET] /rapids/v1/wids/infrastructure_attacks**
[GET] /monitoring/v1/wids/client_attacks	**[GET] /rapids/v1/wids/client_attacks**
[GET] /monitoring/v1/wids/events	**[GET] /rapids/v1/wids/events**

Table 366: *Removed and Alternative APIs*

Removed API	Alternative API
Configuration	
▪ **[PUT] /configuration/v1/msp/templates**—This API updates the MSP customer level template to all template groups for the end customers. ▪ **[PUT] /configuration/v1/msp/templates/customer/{cid}**—This API updates the end customer-level template and applies the template to all template groups. **NOTE:** To achieve the functionality of **[PUT] /configuration/v1/msp/templates** API, it is recommended that you use the combination of 1, 3, and 4 numbered APIs from the alternate API column. **NOTE:** To achieve the functionality of **[PUT] /configuration/v1/msp/templates/customer/{cid}** API, it is recommended that you use the combination of 2 and 4 numbered APIs from the alternate API column.	1. **[PUT] /configuration/v2/msp/templates**—This API is used to update the template at MSP level. 2. **[PUT] /configuration/v2/msp/templates/customer/{cid}**—This API is used to update the template at end customer level. 3. **[POST] /configuration/v2/msp/templates/end_customers/{device_type}/{version}/{model}**—This API is used to apply the MSP level template to end customers. 4. **[POST]/configuration/v2/msp/templates/end_customers/{cid}/{device_type}/{version}/{model}/group**—This API is used to apply end customer-level templates to the end customer's template groups.

The following table lists the APIs that have been removed:

Table 367: *Removed APIs*

Removed APIs
ACP MSP
▪ **[GET] /platform/msp_api/v1/customers/{customer_id}** ▪ **[PUT] /platform/msp_api/v1/customers/{customer_id}** ▪ **[DELETE] /platform/msp_api/v1/customers/{customer_id}** ▪ **[GET] /platform/msp_api/v1/customers** ▪ **[POST] /platform/msp_api/v1/customers**
Clarity
▪ **[GET] /clarity/v1/overview/healthscore** ▪ **[GET] /clarity/v1/overview/healthscore/dns** ▪ **[GET] /clarity/v1/overview/network_stats** ▪ **[GET] /clarity/v1/ssid/names** ▪ **[GET] /clarity/v1/overview/reasons** ▪ **[GET] /clarity/v1/overview/attempts** ▪ **[GET] /clarity/v1/overview/device_attempts** ▪ **[GET] /clarity/v1/trend/healthscore** ▪ **[GET] /clarity/v1/trend/healthscore/dns** ▪ **[GET] /clarity/v1/trend/network_stats**

Table 367: *Removed APIs*

Removed APIs
■ **[GET] /clarity/v1/clients/search/partial** ■ **[GET] /clarity/v1/clients/search/absolute** ■ **[GET] /clarity/v1/clients/details** ■ **[GET] /clarity/v1/clients/stats** ■ **[GET] /clarity/v1/insights** ■ **[GET] /clarity/v1/insights/details** ■ **[GET] /clarity/v1/insights/distribution** ■ **[GET] /clarity/v1/license**
Attributes
■ **[GET] /monitoring/v1/attribute_values**
Presence Analytics
■ **[POST] /presence/v1/config/thresholds** ■ **[GET] /presence/v1/config/thresholds** ■ **[GET] /presence/v1/analytics/aggregates** ■ **[GET] /presence/v1/analytics/trends** ■ **[GET] /presence/v1/insights/top_sites** ■ **[GET] /presence/v1/insights/bottom_sites** ■ **[GET] /presence/v1/insights/sites/aggregates**

This section provides details on the typical issues you might face with the devices managed by Aruba Central network and the steps to help troubleshoot these issues.

For more information on the troubleshooting workflows, see the following topics:

Client Connectivity

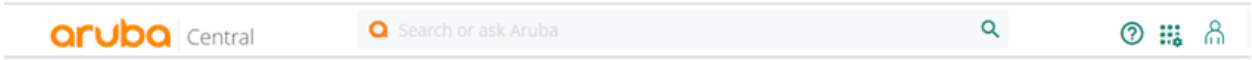
The following section provides details on the typical issues you might face while connecting to the clients in the Aruba Central network and the steps to help troubleshoot these issues.

Troubleshooting Made Easy Using the AI Search Bar

When there are many clients and devices in a network, it is difficult for a user to navigate and identify a particular client or a device to diagnose an issue. The search bar in the **Network Operations** app enables users to search for clients, devices, and infrastructure connected to the network. The search also retrieves relevant documentation to help users efficiently operate their networks. The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant search results.

The following figure illustrates the search bar option in Aruba Central.

Figure 528 *Search Bar*



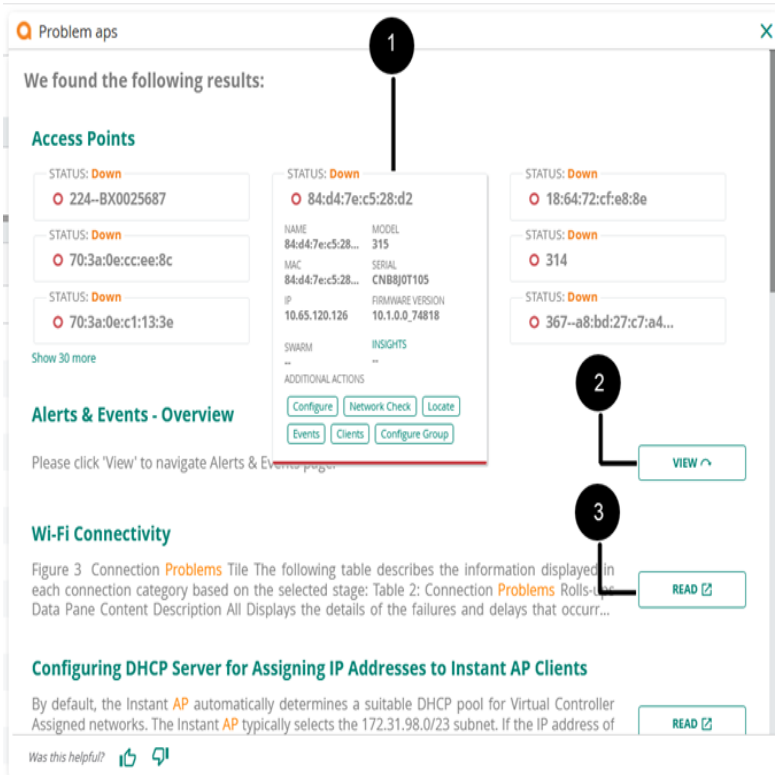
To start a search in the Aruba Central UI, click the search bar or press **/** (forward slash) on your computer keyboard.

When you click the search bar, you can see the search suggestions in the **Recent** and **Suggested Search** list.

- **Recent**—Shows the searches performed recently in the search bar. These suggestions help you quickly look at the previous searches.
- **Suggested Search**—Shows search suggestions corresponding to the workflow that you follow in the **Network Operations** app. The suggested search help you perform onboarding, monitoring, configuring, and troubleshooting tasks.

The following figure illustrates the sample search result in Aruba Central.

Figure 529 *Sample Search Result*



From the search results, you can navigate to:

- **Search Cards**—displays monitoring summary and links to configuration, monitoring, and troubleshooting pages in the **Network Operations** app.
- **View**—relevant links to the corresponding pages in the **Network Operations** app.
- **Read**—relevant links to the help pages in the Aruba Central Help Center.

For more information on the list of recommended search terms for different categories, see Using the Search Bar.

Datapath of a WLAN Client

Aruba Central automatically populates the datapath of a WLAN client.

To view the datapath of a WLAN client, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:

- **All**—Displays a list of all the clients connected to the network.
- **AP**—Displays a list of clients connected to the Instant AP.
- **Switch**—Displays a list of clients connected to the switch.
- **Gateway**—Displays a list of clients connected to the gateway.

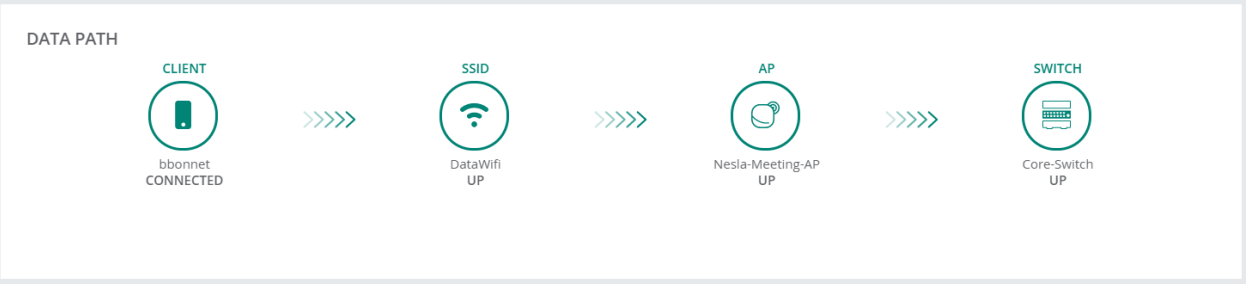
4. To filter the clients based on the state of connectivity, click the connectivity type from the **Client Summary** bar:
   - **Connecting**—Displays a list of client connections that are in progress.
   - **Connected**—Displays a list of clients that are successfully connected to the network.
   - **Failed**—Displays a list of all failed client connections.
   - **Offline**—Displays a list of all offline clients.
   - **Blocked** —Displays a list of all blocked clients.
5. In the **Clients Summary** bar, click **Wireless** to filter the clients connected to the wireless network.
6. In the **Clients** table, click a client listed under **Client Name**.

   The **Summary** tab is displayed.
7. In the **Client Details** page, the **Data Path** pane displays the datapath of the client in the network.

   Datapath can be one of the following:
   - **Client** > **SSID** > **AP**
   - **Client** > **SSID** > **AP** > **Switch**
   - **Client** > **SSID** > **AP** > **Switch** > **Gateway**
   - **Client** > **SSID** > **AP** > **Gateway**

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Figure 530 *Client—Datapath*



Client Health Issues

Client health is the efficiency at which an AP transmits downstream traffic to a particular client. This value is determined as the ratio of ideal airtime required for transmitting a packet from an AP to a client to the actual time taken for the packet transmission in percentage. Ideal air time assumes highest data rate without any retransmission.

A client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.

Viewing the Client Health

To view the client health, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the Instant AP.
   - **Switch**—Displays a list of clients connected to the switch.
   - **Gateway**—Displays a list of clients connected to the gateway.

The wired client will show up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Clients Summary** bar:
   - **All**—Displays a list of all the clients connected to the network.
   - **Wireless**—Displays a list of clients connected to the wireless network.
   - **Wired**—Displays a list of clients connected to the wired network.
   - **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the icon.
5. To filter the clients based on the state of connectivity, click the connectivity type from the **Clients Summary** bar:
   - **Connecting**—Displays a list of client connections that are in progress.
   - **Connected**—Displays a list of clients that are successfully connected to the network.
   - **Failed**—Displays a list of all failed client connections.
   - **Offline**—Displays a list of all offline clients.
   - **Blocked**—Displays a list of all blocked clients.
6. In the **Clients** table, click the **Health** column to view the health of the client. The value of the client health can be one of the following:
   - **Poor**—0-30
   - **Fair**—31-70
   - **Good**—71-100

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Offline Clients

Offline clients are the clients that were seen in a selected time duration, but are currently disconnected from the Aruba Central network. Aruba Central provides details of offline clients connected to the wireless and wired network. The **Clients** page provides a summary view of all the clients connected to the network.

To view the offline clients, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the Instant AP.
   - **Switch**—Displays a list of clients connected to the switch.
   - **Gateway**—Displays a list of clients connected to the gateway.

The wired client will show up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Clients Summary** bar:
   - **All**—Displays a list of all the clients connected to the network.
   - **Wireless**—Displays a list of clients connected to the wireless network.
   - **Wired**—Displays a list of clients connected to the wired network.
   - **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the icon.
5. In the **Clients Summary** bar, click **Offline** to view the offline clients.

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

The **Clients** table lists the details of each client. By default, **All** clients is selected and the table displays the following columns: **Client Name**, **Status**, **IP Address**, **VLAN**, **Connected To**, **SSID/Port**, **AP Role**, **Gateway Role**, and **Health**. The default columns displayed is different and contextual based on AP, switch, and gateway.

Click the ellipsis icon to perform additional operations:

- **Download CSV**—Downloads the client details in the .csv file format.
- **Select All**—Selects all columns.
- **Reset Columns**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click and enter the filter criteria or select a filter criteria. For example, to search a client, click the predefined filter criteria: **ConnectingConnected**, **Offline**, **Failed**, or **Blocked** from the **Client Summary** bar and in the **Client Name** column enter the name of the client. Aruba Central provides a near-instant refresh of the client status if the client is connecting or connected to an access point.

Table 368: *All Client Details*

Column Names	Applicability	Description
Client Name	▪ All ▪ AP ▪ Switch ▪ Gateway	Username, hostname, or MAC address of the client. Click the client name to view the **Summary** page.
Status	▪ All ▪ AP ▪ Switch ▪ Gateway	Client connection status. Use the filter option to view the following: ▪ Connecting—Applicable only for wireless clients. ▪ Connected—Applicable for all client types. ▪ Offline—Applicable for all client types. ▪ Failed—Applicable only for wireless clients. ▪ Blocked—Applicable only for wireless clients. Hover the cursor over the status column to view a pop-up summary based on the connection status. The status summary is populated based on the status type. Each status type and the summary is described below: ▪ **Connecting**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the client was last connected. ▪ **Connected**: ◦ **Client name**—Name of the client. ◦ **Authentication**—Type of authentication. Displays the authentication label only for authenticated clients. ◦ **IP address**—Client IP address. ◦ **Connected Since**—Date and time at which the client was connected. ◦ **Failure Stage**—Stage of the connection where the client failed to connect. It is not applicable for the wired clients, so displayed as NA. ◦ **Health Score**—Device health. ◦ **Connected Device Port**—The device port that the wired client is connected to. ▪ **Failed**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the client was last connected. ◦ **Failure Stage**—Stage of the connection where the client failed to connect. ◦ **Failure Reason**—Reason for the connection failure. ▪ **Offline**: ◦ **Client name**—Name of the client. ◦ **Authentication**—Type of authentication. Displays the authentication label only for authenticated clients. ◦ **IP address**—Client IP address ◦ **Connected Since**—Date and time at which the client was connected. ◦ **Last Seen Time**—Date and time the client was last connected.

Table 368: *All Client Details*

Column Names	Applicability	Description
		◦ **Failure Stage**—Stage of the connection where the client failed to connect. ◦ **Connected Device Port**—The device port that the wired client is connected to. ■ **Blocked**: ◦ **Client name**—Name of the client. ◦ **Last Seen Time**—Date and time the client was last connected.
IP Address	■ All ■ AP ■ Switch ■ Gateway	IP address of the client.
VLAN	■ All ■ AP ■ Switch ■ Gateway	VLAN of the device to which the client is connected.
Connected To	All	AP name, Switch name, or Gateway name. This is the first layer 2 hop for the client. If the device does not have a name, the MAC address is displayed.
AP Role	■ All ■ AP	Role assigned by the AP.
Gateway Role	■ All ■ Gateway	Role assigned by the Aruba Gateway.
Health	■ All ■ AP	Client health. The value can be one of the following: ■ **Poor**—0-30 ■ **Fair**—31-70 ■ **Good**—71-100
SSID/Port	■ All ■ AP ■ Switch ■ Gateway	Displays the SSID for wireless clients and the port number for wired clients. The column title displays **SSID** and **Port** interchangeably based on the device filters. For APs, the column title displays **SSID**. For switch and gateway, the column title displays **Port**.
Insights	■ All ■ AP	The total number of AI insights generated for the client.
Switch Role	■ All ■ Switch	Role assigned by the Aruba switch.
Failure Stage	■ All ■ AP	Failure status of the client that failed to connect. The failure reasons could be: ■ Association failure ■ MAC authentication failure

Table 368: *All Client Details*

Column Names	Applicability	Description
		■ 802.1X authentication failure ■ Key exchange failure ■ DHCP failure ■ Captive Portal failure
Group Name	■ All ■ AP ■ Switch ■ Gateway	Displays the name of the group that the device is connected to. The **Connected To** column displays the device name that the client is connected to.
Site Name	■ All ■ AP ■ Switch ■ Gateway	Displays the name of the site that the device is connected to. The **Connected To** column displays the device name that the client is connected to.
MAC Address	■ All ■ AP ■ Switch ■ Gateway	MAC address of the client.
Hostname	■ All ■ AP ■ Gateway	Host name of the client.
User Name	■ All ■ AP ■ Switch ■ Gateway	Username of the client.
Key Management	■ All ■ AP	Security mode used by the client.
Authentication	■ All ■ AP ■ Switch ■ Gateway	Authentication type used by the client to connect with the device.
Global Unicast IPv6 Address	■ All ■ AP ■ Gateway	When the IPv6 address is present for a client, you can view its Global Unicast IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Link Local IPv6 Address	■ All ■ AP ■ Gateway	When the IPv6 address is present for a client, you can view its Link Local IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed.
Capabilities	■ All ■ AP	Client 802.11 capabilities.

Table 368: *All Client Details*

Column Names	Applicability	Description
Usage	■ All ■ AP ■ Switch ■ Gateway	Total data usage for the selected time period.
Last Seen Time	■ All ■ AP ■ Switch ■ Gateway	Date and time when the client was last seen.
Connected Since	■ All ■ AP ■ Switch ■ Gateway	Date and time since when the client was connected.
AP Name	■ All ■ AP	Name of the AP.
AP Mac Address	■ All ■ AP	MAC address of the AP.
Channel/Band	■ All ■ AP	Last connected channel and band.
Switch Name	■ All ■ Switch	Name of the switch.
Port	■ All ■ Switch ■ Gateway	Port number of the switch.
Gateway Name	■ All ■ Gateway	Name of the Aruba Gateway.
Tunneled	■ All ■ AP ■ Switch ■ Gateway	Tunnel mode applicable for the Aruba Gateway managed WLAN, UBT, or PBT client.
Segmentation	■ All ■ AP ■ Switch ■ Gateway	Type of segmentation. The type of segmentation can be: ■ None ■ UBT ■ PBT ■ Underlay ■ Overlay

Table 368: *All Client Details*

Column Names	Applicability	Description
		NOTE: To view the details about dynamic segmentation, a gateway must be licensed in Aruba Central and connected to the switch.
Client Category	▪ All ▪ AP ▪ Gateway	Displays the category of the profiled device. For example, Access Points, Computer, Smart Device, VoIP phone, and so on.
Client Family	▪ All ▪ AP ▪ Gateway	Displays the type of operating system or vendor. For example, if the client category is Computer, the client family can be Windows, Linux, or Apple Mac.
Client OS	▪ All ▪ AP ▪ Gateway	Displays the operating system that the device runs on. For example, if the client category is Computer and the client family is Windows, the client OS can be Windows or Windows 8/10.

Issues in the Application Layer

In an Aruba Central-managed network, Network Check aims to identify, diagnose, and debug issues on your network. The **Network Check** tab under **Analyze** > **Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection. You must have admin privileges or read-write privileges to perform network checks.

The following tests are available to diagnose issues pertaining to WLAN network connections:

- **HTTP Test**—The HTTP test is a performance test to identify the time taken to load a web page. It sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.
- **HTTPS Test**—The HTTPS test is a performance test to identify the time taken to load a web page. It sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device.
- **TCP Test**—The TCP test verifies network connectivity to remote hosts with the remote host-port combination approach. It sends packets to the host, for example, FTP server, and tries to establish a connection and exchange data. If the FTP server returns a response, the issue could be isolated to the client device.

HTTP Test

To perform an HTTP test, complete the following steps:

1. In the **Network Operations** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.

   The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **HTTP Test**.

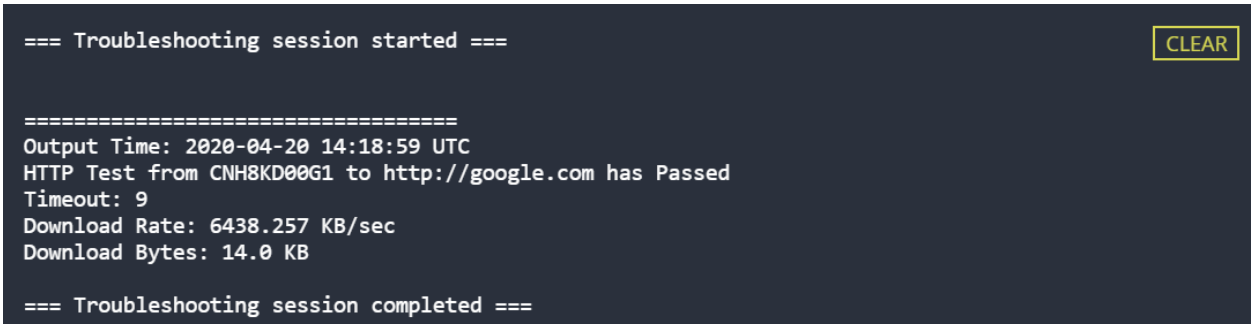
6. The value in the **Sources** drop-down list is auto-populated based on the wireless client selected.
7. In the **URL** field, enter the HTTP URL for which you want to perform the HTTP test. For example, http://*hostname* or http://*ipaddress*.
8. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds, in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

NOTE

Show Additional Test Settings is disabled when no **Test** type is selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 531 *HTTP Test—Device Output*



NOTE

The HTTP test is supported only from ArubaOS 8.3.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

HTTPS Test

To perform an HTTPS test, complete the following steps:

1. In the **Network Operations** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.

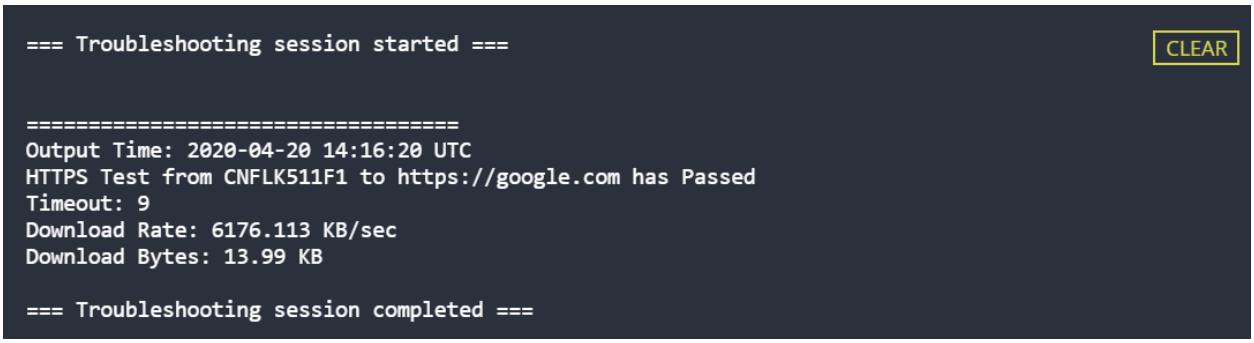
   The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **HTTPS Test**.
6. The value in the **Sources** drop-down list is auto-populated based on the wireless client selected.
7. In the **URL** field, enter the HTTPS URL for which you want to perform the HTTPS test. For example, https://*hostname* or http://*ipaddress*.
8. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds, in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

NOTE

Show Additional Test Settings is disabled when no **Test** type is selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 532 *HTTPS Test—Device Output*



NOTE

The HTTPS test is supported only from ArubaOS 8.4.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

TCP Test

To perform a TCP test, complete the following steps:

1. In the **Network Operations** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.

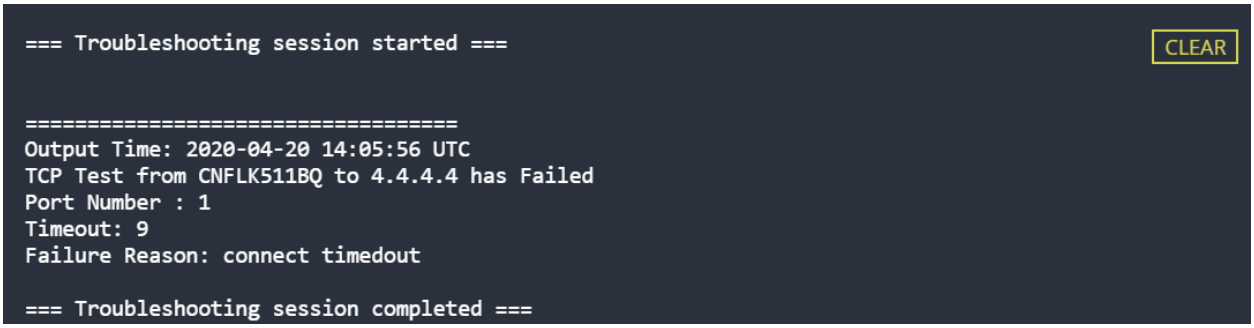
   The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **TCP Test**.
6. The value in the **Sources** drop-down list is auto populated based on the wireless client selected.
7. In the **Host** field, enter the IPv4 address. Hostname is not supported.
8. In the **Port** field, enter the port number. The port number should be in the range 1 to 65535.
9. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds, in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

NOTE

Show Additional Test Settings is disabled when no **Test** type is selected.

10. Click **Run**. The output is displayed in the **Device Output** section.

Figure 533 *TCP Test—Device Output*



NOTE

The TCP test is supported only from ArubaOS 8.3.0.0 or later versions.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and target. It also shows the status of the tests as, in progress, complete, and the buffer time. If there are multiple devices, select the device for which you want to view the output.

Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Roaming Issues in a Wireless Client

Roaming is the process of a wireless client moving from one source AP to another AP within the same Extended Service Set (ESS) without losing connection. When a wireless client roams between two APs, the association to the new AP terminates the previous AP association and the destination AP creates an event.

In Aruba Central, the **Roaming Experience** pane provides the details of the roaming events and latency parameters of a client.

Viewing the Roaming Experience Pane

To view the **Roaming Experience** pane, complete the following steps:

1. In the **Network Operations** app, search for a specific wireless client in the **Search Bar**.
2. Click any one of the wireless clients listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. In the **Client Details** page, the **Roaming Experience** pane displays the details of the roaming events and latency parameters of a client.

The **Roaming Experience** pane displays two views, the grid view and the trend view.

Grid View

The grid view is the default view and provides the following information:

Table 369: *Grid View*

Parameter	Description
Date/Time	Displays the date and time of occurrence of the client roaming/association events.
SSID	The SSID to which the client is connected.
Latency (ms)	Roaming latency in milliseconds between source and destination AP. **NOTE:** Roaming latencies above 50 ms are considered as high latency roaming events.
To BSSID	The BSSID of the destination AP.
Source AP	AP to which the client was connected.
Destination AP	AP to which the client is connected.
Roaming Type	The type of roaming. Click the icon to filter the data based on the following roaming types: ■ 11r ■ okc ■ 802.11
Band	Radio band on which the client is connected.
RSSI (dBm)	Received Signal Strength Indicator (RSSI) on the client. It is the estimated measure of power level received by client from the AP.

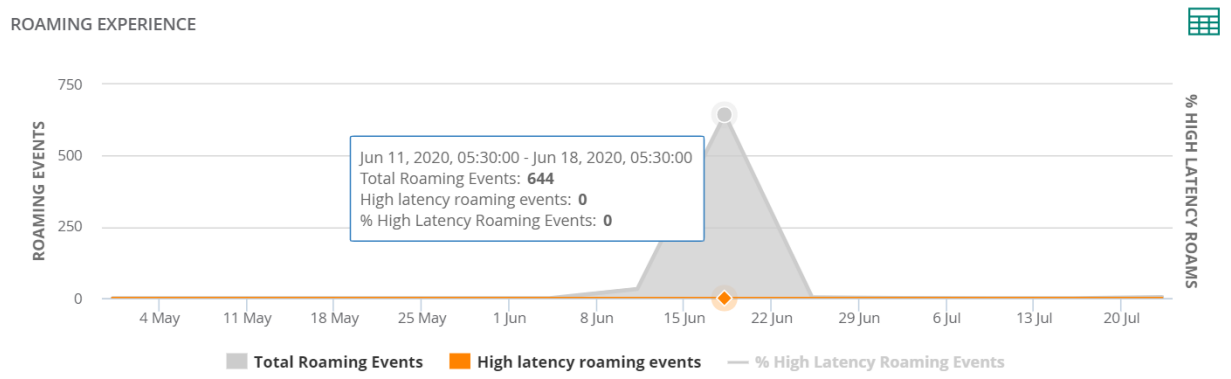
NOTE

- By default, the **Roaming Experience** table displays data for the last 3 hours. To view the table for a different time range, use the **Time Range Filter**.
- A search filter is provided only for the **Data/Time** and **Roaming Type** columns.

Trend View

The trend view displays a chart that shows the percentage of high latency roaming events, total roaming events, and the number of high latency roaming events at a particular instance based on the value selected in the **Time Range Filter**.

Figure 534 *Roaming Experience—Trend View*



Client Connection to the Network

When a client tries to connect to the AP or the network, and is unable to do so, you can navigate to the **Clients** page and check the reasons for failure.

The **Clients** page provides a list view of all the clients connected to the network. You can filter clients based on the network the clients are connected to. This page displays key client information and also allows you to view a specific client detail page.

To view the list of **Failed** clients, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The **Clients** page is displayed in **List** view.

By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
   - **All**—Displays a list of all the clients connected to the network.
   - **AP**—Displays a list of clients connected to the Instant AP.
   - **Switch**—Displays a list of clients connected to the switch.
   - **Gateway**—Displays a list of clients connected to the gateway.

The wired clients will show up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Client Summary** bar:
   - **All**—Displays a list of all the clients connected to the network.
   - **Wireless**—Displays a list of clients connected to the wireless network.
   - **Wired**—Displays a list of clients connected to the wired network.
   - **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the icon.
5. In the **Client Summary** bar, click **Failed** to view a list of all failed client connections.
6. In the **Clients** table, the **Failure Stage** column provides the following information:

Table 370: *Client Details*

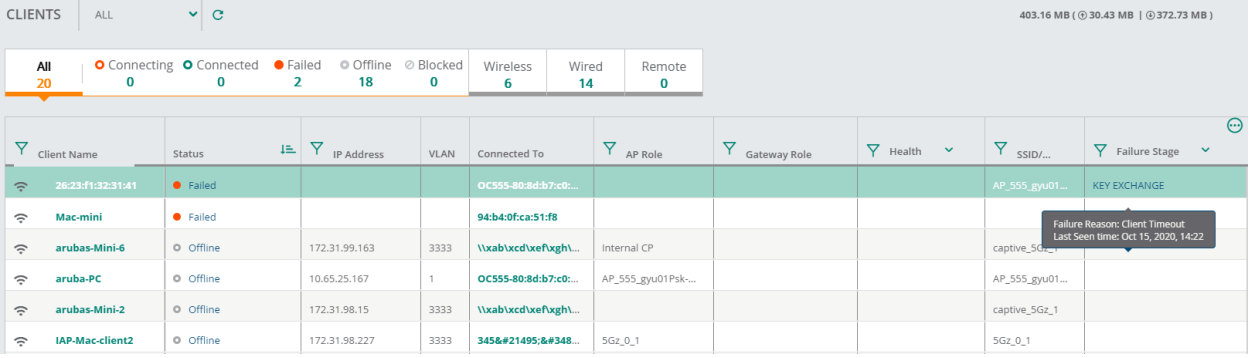
Failure Stage	▪ All ▪ AP	Failure status of the client that failed to connect. The failure reasons could be: ▪ Association error ▪ MAC authentication error ▪ 802.1X authentication error ▪ Key exchange error ▪ DHCP error ▪ Captive Portal error

Hover over the specific failure stage to display detailed information regarding the type of error. For example, if the failure stage column displays failure stage as **DHCP**, and you hover your mouse over **DHCP**, it displays the following:

- **Failure Reason**
- **Last Seen time**

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Figure 535 *Client Details*



You must also check if multiple failures have occurred and if the client is denylisted. When a client is denylisted, it is not allowed to associate with an AP in the network. If a client is connected to the network when it is denylisted, a deauthentication message is sent to force client disconnection. You can denylist a client manually or dynamically.

Denylisting Clients Manually

Manual denylisting adds the MAC address of a client to the denylist. These clients are added into a permanent denylist and are not allowed to connect to the network unless they are removed from the denylist.

To add a client to the denylist manually, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
   The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. Under **Manual Denylisting**, click **+** and enter the MAC address of the client to be denylisted.
7. Click **OK**.
8. Click **Save Settings**.

To delete a client from the manual denylist, select the MAC Address of the client under the **Manual Denylisting**, and then click the delete icon.

NOTE

You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. For the denylisting to take effect, you must enable the denylisting option when you create or edit the WLAN SSID profile. Go to **WLANs** > **Security** > **Advanced Settings** and enable the **Denylisting** option.

Denylisting Clients Dynamically

Clients can be denylisted dynamically when they exceed the authentication failure threshold or when a denylisting rule is triggered as part of the authentication process.

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically denylisted by an Instant AP.

In session firewall based denylisting, an ACL rule automates denylisting. When the ACL rule is triggered, it sends out denylist information and the client is denylisted.

To configure the denylisting duration, complete the following steps:

1. In the **Network Operations** app, set the filter to a group containing at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
   The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
   The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. Under **Dynamic Denylisting**, enter the following information:
   a. For **Auth Failure Denylist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be denylisted.
   b. For **Policy Enforcement Failure Rule Denylisted Time**, enter the duration after which the clients can be denylisted due to an ACL rule trigger.
7. Click **Save Settings**.

NOTE

You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. To enable session-firewall-based denylisting, select the **Denylist** check box in the **Access Rule** page during the WLAN SSID profile creation.

After the failure reasons are detected, select the client and navigate to the **Clients Detail** page. Click **Tools** under **Analyze** in the left navigation pane, and perform network check and advance troubleshooting check under **Network Check** and **Commands** respectively.

Client Live Troubleshooting

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. Live troubleshooting is supported only if the Instant APs are running 8.4.0.0 firmware version or a later version.

To troubleshoot a client at the site level, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites**.
2. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
3. Enter the MAC address of the client and click **Start Troubleshooting**.

To troubleshoot a wireless client, complete the following steps:

1. In the **Network Operations** app, search for the specific wireless client in the **Search Bar** for which you want to perform live troubleshooting.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.

The troubleshooting session runs for 15 minutes and the status is displayed every minute. If you want to stop live troubleshooting, click **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Device Name**—Displays the name of the device the client is connected to. Set the filter to select a specific device under **Sites**.
- **AP Name**—Displays the name of the AP the client is connected to. Use the filter option to select a specific AP.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

Packet Capture

Aruba Central allows you to interact and launch a targeted packet capture on a client connected to a specific access point or a switch. After you start packet capture from the UI, Aruba Central notifies the access point and the switch. The default packet capture duration is 15 minutes. After you start packet capture, use the toggle button to stop packet capture, or go back to the **Client Overview** page.

For packet capture, for a wired client connected to an Aruba 5400R Switch Series (V3 mode), ensure that "no-allow v2 modules" is set for the switch. Packet capture for stack switches works only if the client is connected to the commander of the stack.

Starting Packet Capture

You can start packet capture from the wireless or wired clients page. Packet capture can be done at a site level (wireless client only) or for a selected client.

To start packet capture at a site level, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Sites** that contains at least one device. The dashboard context for the selected site is displayed.
2. Under **Analyze**, click **Live Events**.The **Live Events** page is displayed.

3. Enter the MAC address of the client.

NOTE

At a site level, Aruba Central does not support packet capture for a wired client connected to a switch.

4. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
5. Click **Start Troubleshooting**.

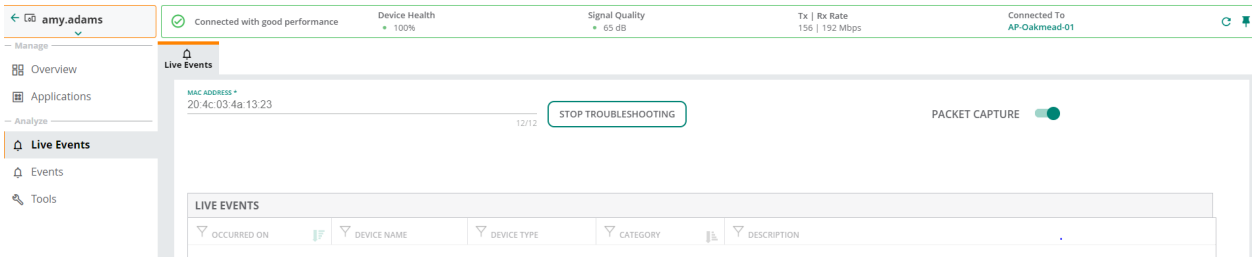
To start packet capture for a wireless or wired client, perform the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The Clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired** to filter the clients connected to the wireless or wired client respectively.
5. Enter the client name in the **Client Name** column, and click the client name.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed. The client live troubleshooting starts automatically for the selected client.
7. Click **Stop Troubleshooting** to stop live troubleshooting.
8. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
9. Click **Start Troubleshooting** to live troubleshoot the selected client. Live packet capture starts for the selected client.

   The live troubleshooting session runs for a duration of 15 minutes. After the live troubleshooting session ends, a **Download PCAP** text appears above the live events table. Click **Download PCAP** to download the generated PCAP file on your local system.

Figure 536 *Live Events*



Notifying Network and Client Anomalies to the Administrator

The **Wi-Fi Connectivity** page in Aruba Central enables you to check connection details of all the clients connected to an AP in the network. The data can be used to notify administrators of the possible anomalies in the network.

To view the **Wi-Fi Connectivity** page, complete the following steps:

1. In the **Network Operations** app, set the filter to one of the options under **Groups** or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.

2. Under **Manage** > **Overview**, click **Wi-Fi Connectivity**.
   The **Wi-Fi Connectivity** page is displayed.

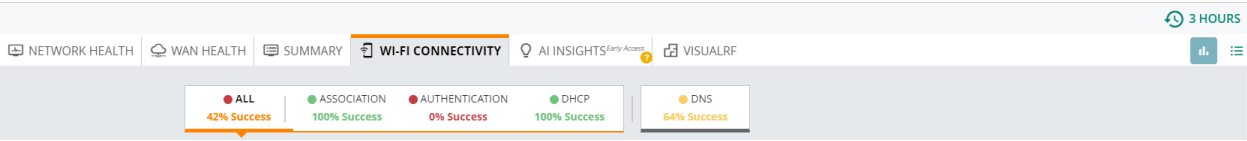
By default, the graphs on the **Wi-Fi Connectivity** page is plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** icon. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, and 1 month.

This section includes the following topics:

Connectivity Summary Bar

The connectivity summary bar displays the details of all clients in percentage. It displays the percentage success rate of each stage for the users to know the network performance.

Figure 537 *Connectivity Summary Bar*



The following table describes the information displayed in each section:

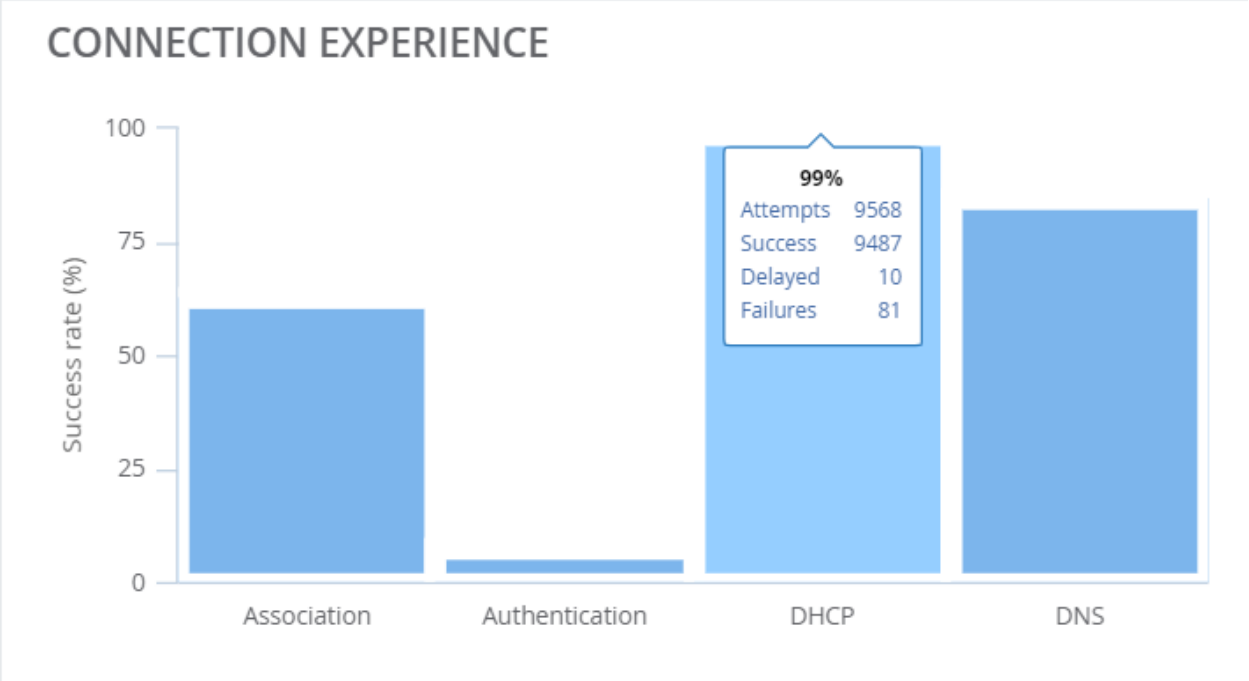
Table 371: *Connectivity Summary Bar*

Field	Description
All	Displays the aggregated success percentage of **Association**, **Authentication**, and **DHCP** for all clients connected to the network.
Association	Displays the percentage of successful attempts made by a client to connect to the network.
Authentication	Displays the percentage of successful attempts of client authentication.
DHCP	Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client.
DNS	Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network.

Connection Experience

The **Connection Experience** tile displays the overall success percentage, total number of attempts, number of successful attempts, total delays, and the total failures for each of the stages based on the selected time range filter. To view the connection experience for each individual stage, select the stage type from the **Connectivity Summary** bar.

Figure 538 *Connection Experience Tile*



AI Insights

The **AI Insights** tile provides a list of AI Insights generated for a selected time range. To view the details, click on a selected **AI Insight**. The page gets redirected to the AI Insights under the **AI Insights** page. Click each of the listed AI Insight for a detailed analysis based on the impact on the network.

NOTE

AI-Insights is not implemented for **Association** and **DNS**. AI Insights is not implemented at a Group level also. The page displays **No AI Insights observed**.

Connection Problems

The **Connection Problems** tile displays the details of **Failures** and **Delays** graphically for each of the categories from the drop-down list. Each graph displays the top five MAC addresses or SSID based on the selected category. Each category in the **Connection Problems** drop-down lists changes based on the selected stage in the **Connectivity Summary** bar. Selecting the required category from the drop-down displays the failures and delays in a pie chart with percentage, and a bar graph with the number of failures and delays. Hover the cursor over each graph to view the number of failures or delays for each stage.

Figure 539 *Connection Problems Tile*

The following table describes the information displayed in each connection category based on the selected stage:

Table 372: *Connection Problems Rolls-Ups*

Data Pane Content	Description
All	Displays the details of the failures and delays that occurred during a client connection. The chart displays the failure details of Association, Authentication, and DHCP for each client. The Connection Problems drop-down list includes the following categories: ▪ **By Stage** ▪ **By Clients** ▪ **By Access Points** ▪ **By Band** ▪ **By SSID**
Association	Charts the details of the failures and delays that occurred during a client association. The **Connection Problems** drop-down list includes the following categories: ▪ **By Clients** ▪ **By Access Points** ▪ **By Band** ▪ **By SSID** ▪ **By Reason**
Authentication	Charts the details of the failures and delays that occurred during a client authentication. The **Connection Problems** drop-down list includes the following categories: ▪ **By Type** ▪ **By Clients**

Data Pane Content	Description
	▪ **By Access Points** ▪ **By Band** ▪ **By SSID** ▪ **By Server**
DHCP	Charts the details of the failures and delays that occurred during the attempts of DHCP requests and responses by a client. The **Connection Problems** drop-down list includes the following categories: ▪ **By Clients** ▪ **By Access Points** ▪ **By Reason**
DNS	Charts the details of the failures and delays that occurred during the attempts in detected DNS resolutions when a client is connected to the network. The **Connection Problems** drop-down list includes the following categories: ▪ **By Access Points** ▪ **By Reason** ▪ **By Server**

Connection Events

The **Connection Events** table details out the list of delays and failures for each client based on the client MAC addresses. Click the **List** icon to view the connection events table. Click the **Connection Events** drop down to filter the events **By Clients** or **By Access Points**. The **Connection Events** table displays the following information:

Table 373: *Connection Events*

Data Pane Content	Description
MAC Address	Displays the MAC address of the client.
Name	Displays the name of the access point.
Delays	Displays the delays that occurred during the event.
Failures	Displays the failure details that occurred during the event.

Client Devices do not Discover Printers across the Subnet

For client devices to discover printers across the subnet, you have to turn on the AirGroup service available in Aruba Central.

AirGroup is a zero configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home.

Bonjour can be installed on computers running Microsoft Windows and is supported by the new network-capable printers. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices. The AirGroup solution supports both wired and wireless devices. Wired devices that support Bonjour services are part of AirGroup when connected to a VLAN that is terminated on the Virtual Controller.

In addition to the mDNS protocol, Instant APs also support Universal Plug and Play (UPnP) and Digital Living Network Alliance (DLNA) enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network.

DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

To enable AirGroup services, complete the following steps:

1. In the **Network Operations** app, set the filter to a group that contains at least one AP.
   The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
3. Click the **Config** icon.
   The tabs to configure access points is displayed.
4. Click **Show Advanced**, and then click the **Services** tab.
   The Services details page is displayed.
5. Click the **AirGroup** accordion.
6. Select the **AirGroup** check-box.

- The **mDNS (Bonjour)** and **SSDP (DLNA/UPNP)** check-boxes are selected by default. Select at least **mDNS (Bonjour)** or **SSDP (DLNA/UPNP)** to proceed further.
- Optionally, select the **Guest Bonjour Multicast** check-box to allow guest users to use the Bonjour services that are enabled in a guest VLAN. When **Guest Bonjour Multicast** is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup does not discover or enforce policies in guest VLAN.

7. Expand **AirGroup Settings**, and then select the **AirPrint** check-box to enable wireless printing between AirPrint capable devices and AirPrint compatible printers.
   - Optionally, when enabling an AirGroup service, define disallowed roles. The disallowed roles are not allowed to use the specific AirGroup service. To disallow roles:
     1. Click **Edit** against **Disallowed Roles**.
     2. Move the roles from the **Available** pool to the **Selected** pool.
     3. Click **Ok**.
   - Optionally, when enabling an AirGroup service, define disallowed VLANs. The disallowed VLANs are not allowed to use the specific AirGroup service. To disallow VLANs:
     1. Click **Edit** against **Disallowed VLANs**.
     2. Type the VLANs in **Enter comma-separated list of VLAN IDs**. Separate multiple VLANs with a comma.
     3. Click **Ok**.
   - Optionally, configure and enable a new AirGroup service. If defined, disallowed roles or VLANs are not allowed to use the new AirGroup service. To configure and enable a new AirGroup service:
     1. Click **Add New Service**.
     2. Type the service name in **Service Name**. Use alphanumeric characters.
     3. Type a service ID in **Service ID**. Use **+** to add additional service IDs.
        Sample service ID: **urn:schemas-upnp-org:service:RenderingControl:1** or **_sleep-proxy._udp**.

4. Click **Ok**.
5. Select the check-box against the new AirGroup service.

8. Optionally, under **ClearPass Settings** sub-accordion, configure the following parameters listed:

Table 374: *ClearPass Settings*

Mode	Description
ClearPass Policy Manager Server 1	Specify the ClearPass Policy Manager server to use. Select one from the drop-down or define a new ClearPass Policy Manager server.
Enforce ClearPass Registration	Specify is ClearPass registration should be enforced.

9. Click **Save Settings**.

Poor Voice Call Quality Issues

The growing use of Wi-Fi and the proliferation of mobile tablet and smartphone clients cause control and visibility challenges for communication and collaboration applications. To overcome these challenges, Aruba offers the Unified Communication and Collaboration (UCC) application service to manage your enterprise communication ecosystem.

The UCC application on Aruba devices provides a seamless user experience for voice calls, video calls, and application sharing when using communication and collaboration tools. The UCC application actively monitors voice, video, and application sharing sessions, provides traffic visibility, and allows you to prioritize the required sessions. The UCC application also leverages the functions of the service engine on the cloud platform and provides rich visual metrics for analytical purposes.

To access the UCC application, obtain a valid subscription. To obtain a subscription for the UCC application, contact the Aruba Central Sales team.

To analyze the VOIP call quality of a specific client, complete the following steps:

1. In the **Network Operations** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Manage**, click **Applications** > **UCC**.

   The **UCC** page is displayed in the **List** view.

Alternatively, you can also perform the following steps to navigate to the **UCC** tab to check the VOIP call quality of a specific client:

1. In the **Network Operations** app, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.

   The Clients page is displayed in the **List** view.
3. In the **Clients Summary** bar, click **Wireless** to filter the clients connected to the wireless network.
4. In the **Clients** table, click a client listed under **Client Name**.

   The Summary tab is displayed.

5. Under **Manage**, click **Applications** > **UCC**.
   The UCC page is displayed in the **List** view.

UCC Dashboard

The banner in the header pane shows the following details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended.
- **Fair**—Displays the total number of fair calls that have ended.
- **Poor**—Displays the total number of poor calls that have ended.
- **Unknown**—Displays the total number of calls whose status is unknown.

- For the ALG like Skype SDN, the end-to-end Mean Opinion Score (MOS) is used. A good call has a MOS of more than 3.5, a fair call has a MOS in the range of 2.0 to 3.5, a poor call has a MOS of less than 2.0, and an unknown call does not have a MOS.
- Wi-Fi Calling calls are not tracked. Wi-Fi Calling calls are not assigned an UCC RTPA score and are categorized as unknown.

By comparing the call quality and client health score, you can find out if the wireless network was the reason for poor quality of VOIP calls. A poor value of the client health indicates that the issue is at the wireless network side. In that case, go to **Overview** > **AI Insights** page in the wireless **Client Details** page and check if the client is dwelling on 2.4 GHz band. If the client is dwelling on 2.4 GHz band, configure the VOIP Wireless LAN to 5 GHz band.

If there are no client insights in the **AI Insights** page, you must check for the following AI Insights in the site context:

- **Access Points were impacted by high 5 GHz usage**
- **Access Points impacted by high 2.4 GHz usage**
- **Access Points had an excessive number of channel changes**

Summary View

The **Summary** view in the **Applications** > **UCC** page provides the following charts:

- **Calls**—Displays the chart of all, good, fair, poor, or unknown calls. Chart can be viewed by Health, SSID, Protocol, Operating System, Session Type, or Quality, In any chart, hover your mouse over any segment of the chart to view additional information.
- **Access Points**—Displays the chart of access points. Chart can be viewed by Poor Quality % or Most Calls. Use **Show More** to view more details of the calls.
- **Clients**—Displays the chart of clients. Chart can be viewed by Poor Quality % or Most Calls. Use **Show More** to view more details of the calls.

The **Show More** option in the **Clients** chart displays the following details of the calls:

Table 375: *Clients with Calls*

Parameter	Description
Client Name	Displays the name of the client.
Calls Total	Displays the total number of calls from the client.
Calls Good	Displays the total number of good calls from the client.
Calls Fair	Displays the total number of fair calls from the client.
Calls Poor	Displays the total number of poor calls from the client.
Calls Poor Percentage	Displays the percentage of poor calls from the client.
Calls Unknown	Displays the total number of unknown calls from the client.

Hover your mouse over any row in the list to view additional information.

List View

The **List** view in the **Applications > UCC** page provides a variety of lists that allow you to assess the quality of calls in the network. The banner in the header pane shows the following details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended.
- **Fair**—Displays the total number of fair calls that have ended.
- **Poor**—Displays the total number of poor calls that have ended.
- **Unknown**—Displays the total number of calls whose status is unknown in the last 5 minutes.

The **Calls** list displays the following details of the calls:

Table 376: *Call Details*

Parameter	Description
From	Displays the device originating the call.
To	Displays the device receiving the call.
Start Time	Displays the date and time when the call originated.
Duration	Displays the duration of the call.
State	Displays the state of the call. Possible values are: ▪ Active ▪ Success ▪ Terminated
Quality	Displays the quality of the call. Possible values are: ▪ Good ▪ Fair ▪ Poor ▪ Unknown

Table 376: *Call Details*

Parameter	Description
AP Name	Displays the name of the AP.
Client	Displays the name of the client.

The Call Detail Record (CDR) for FaceTime and Skype for Business calls may be incorrect. The CDR for a Facetime call may be empty or it may display the quality of the call as **unknown**. Duplicate CDRs may be created for a Skype for Business call.

Device Issues

The following section provides details on the typical issues you might face with devices provisioned and managed in the Aruba Central network and the steps to help troubleshoot these issues.

APs are not seen in the Aruba Central Network

Aruba Central validates device connectivity by the network Web socket connection that the device maintains with Aruba Central. If there is no communication of state information from the device for more than 5 minutes, Aruba Central marks the device as offline and the device is not configurable. You must also add device subscription licenses to enable the AP to appear in the Aruba Central network.

If the AP moves to a new network and the new connected Virtual Controller is not licensed, the AP is not shown in the network. For an AP to show up in Aruba Central, you must make sure that the MAC address and the serial number of the AP is added in the device inventory and also the AP is licensed in the inventory. Even after adding the device inventory, if the AP is not showing up in Aruba Central you must verify if the following ports and URLs are allowed by the firewall at the customer's site:

- TCP Port 443
- TCP Port 80
- UDP Port 123
- activate.arubanetworks.com
- device.arubanetworks.com
- rcs-m.central.arubanetworks.com (console)
- pool.ntp.org (time server)

If all the ports and URLs are allowed by the firewall and you are still unable to see the AP in Aruba Central, raise a ticket with the Aruba Technical Support.

Devices are Offline in the Aruba Central Network

If there is a network outage or the device looses Web socket connection to Aruba Central at the customer site, the device goes offline and is unable to communicate with Aruba Central. Apart from network issues, there are a few physical issues that could also cause the device to go offline.

- The LEDs on the AP are turned OFF.
- System LED lights are blinking in green or red—Depending on the warning and error messages the color of the LED lights change from green to red.

- Bad Ethernet port—If the Ethernet port on the AP has gone bad or the cable itself has some issue.
- Cable falling off—The AP is so heated up and has caused some physical damage. The AP shuts down automatically and reboots again because of the thermal issue.
- PoE issue— An AP is powered up either through an adapter or through the Ethernet port. There are two scenarios where an AP might not come up:
  - The Ethernet port does not provide sufficient power to the AP.
  - The Uplink port or PoE port is disabled or not configured correctly.

The **Switch Details** page will display PoE alerts and the status of the port that is connected to the AP.

In order to solve these physical issues of a device, you must issue a direct Return Merchandise Authorization (RMA).

Under Standard Warranty or Limited Lifetime Warranty (LLW) hardware RMAs are handled through best effort. Out of warranty and/or expired contract hardware requires Service Renewal prior to an RMA. TAC only handles defective RMAs under proper entitlement.

Cabling Issues in Switch

The **Cable Test** enables testing of the electrical connections in the switch cable. It checks whether the cabling is conformed to the cabling plans and is of expected quality. It is useful for production and maintenance.

Cable Test is supported only from ArubaOS Switch version 16.05.000 or later. **Cable Test** is not supported in Aruba CX switches.

Cable Test

To perform a **Cable Test** on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

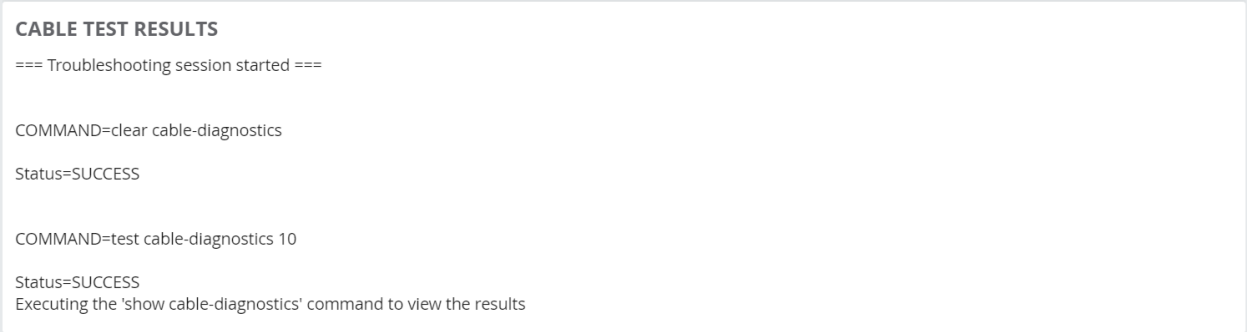
     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch listed under **Device Name** for which you want to perform the cable test.

        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, click **Device Check**.
3. From the **Device Type** drop-down list, select **Switch**.
4. From the **Sources** drop-down list, select a source.
5. From the **Test** drop-down list, select **Cable Test**.
6. From the **Port** drop-down list, enter a port number.
7. Click **Run**. The output is displayed in the **Cable Test Results** section.

- By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.
- The action will cause a loss of link on all tested ports and will take several seconds per port to complete.
- Enter port numbers and/or port ranges separated by commas. For stacking switch, enter member id/port number.

Figure 540 *Cable Test-Device Output*



Reboot an IoT Sensor

Users can reboot an IoT sensor to troubleshoot and conduct event log analysis, renegotiate LLDP power supplied, apply new role configuration, or for enhanced serviceability.

The **PoE Bounce** test reboots an IoT sensor port interface and forces a client to re-initiate a DHCP request.

PoE Bounce is supported only from ArubaOS Switch version 16.04.000 or later.

PoE Bounce

To perform a **PoE Bounce** test on a switch, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

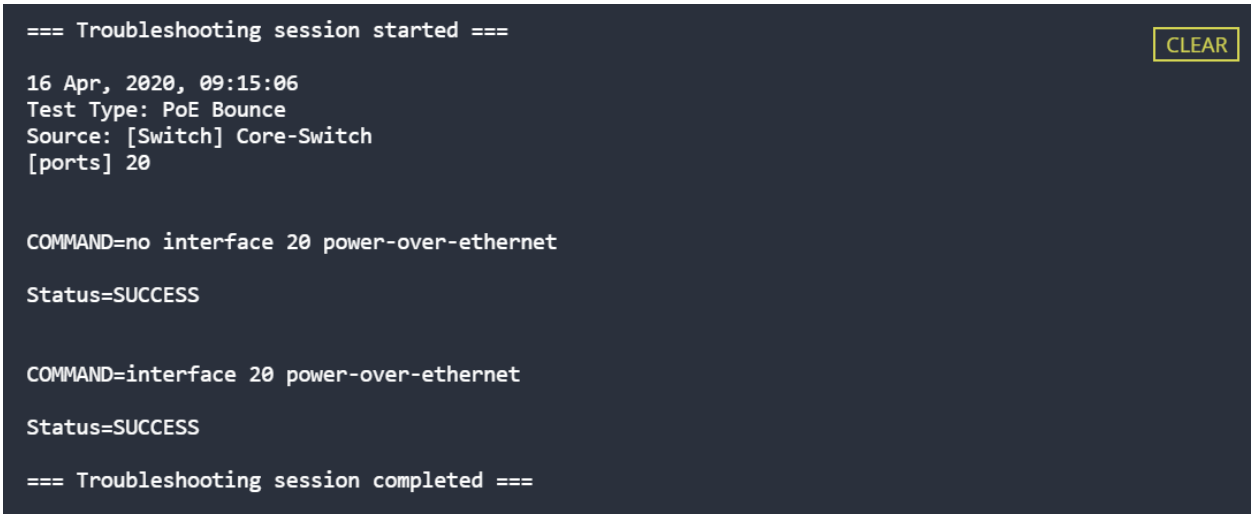
     The dashboard context for the selected filter is displayed.
   - To select a switch in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Switches**.

        A list of switches is displayed in the **List** view.
     c. Click a switch listed under **Device Name** for which you want to perform the PoE bounce test.

        The dashboard context for the switch is displayed.
2. Under **Analyze** > **Tools**, click **Device Check**.
3. From the **Sources** drop-down list, select a source.
4. From the **Test** drop-down list, select **PoE Bounce**.
5. From the **Port** drop-down list, enter a port number.
6. Click **Run**. The output is displayed in the **Device Output** section.

- By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.
- Multiple device selection is not allowed at this level.
- Devices which are already running commands shall not execute newly added commands.

Figure 541 *PoE Bounce Test-Device Output*



AI Insights

The following section describes the anomalies observed in the Aruba Central network that might affect the quality of the overall network performance and the steps to help troubleshoot these issues.

AI Insights Anomalies

The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level for the selected time range. Each insight provides specific details on the occurrences of these events for easy debugging.

In this release the insights are classified under three categories:

- Connectivity—Issues related to the wireless connectivity in the network.
- Wireless Quality—Issues related to the RF Info or RF Health in the network.
- Availability—Issues related to the health of your network infrastructure and the devices in the network such as, APs, switches, and gateways.

To launch the **AI Insights** dashboard, complete the following steps:

1. In the **Network Operations** app, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Overview** > **AI Insights**.
   The Insights table is displayed. AI Insights listed in the dashboard are sorted from high priority to low priority.

3. Click › against each insight to view the further details.

Figure 542 *Insight Details*

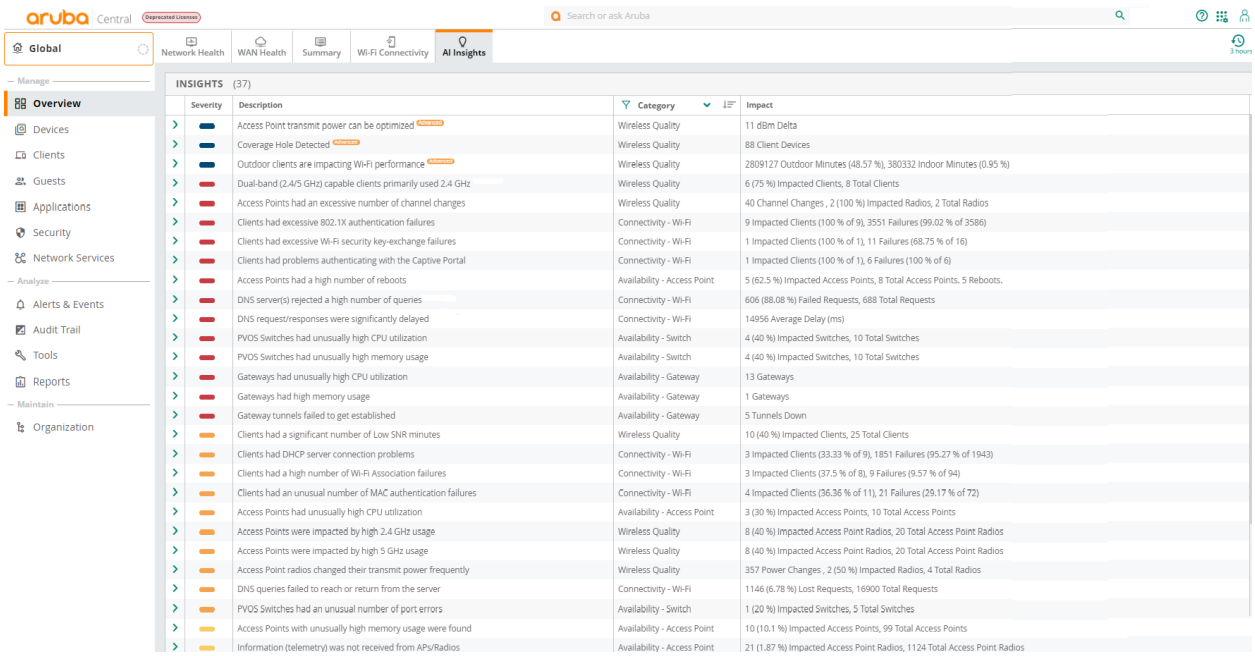
Callout Number	Description
1	Click this arrow to expand any specific insight to view further details.
2	Displays the insight severity, using the following colors: ■ Red—High priority ■ Orange—Medium priority ■ Yellow—Low priority
3	Short description of the insight.
4	Insight Summary displays the reason why the insight was generated along with recommendation. It also shows the number and percentage of failures that occurred against each failure reason. The reasons are classified into: ■ Static—These reasons rely on Aruba's domain expertise. ■ Dynamic—These reasons are generated based on error codes that is received from infrastructure devices.
5	Time Series graph is a graphical representation of the failure percentage or failure events that occurred for the selected time range. The entries in each time series bar can be customized to highlight a specific entry by clicking on it. Only one specific entry can be highlighted at a time.
6	Category of the insight.
7	Short description of the impact.
8	Cards display additional information specific to each insight. Cards might vary for each insight based on the context the insight is accessed from.

All AI Insights generated are listed in the **Global > AI Insights** dashboard. Alternatively, AI Insights for a specific site, device, or client can be viewed by selecting the respective context.

NOTE

AI Insights are displayed for a selected time period based on the time selected in the **Time Range Filter**. You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**.

Figure 543 *AI Insights Dashboard*



For more information, see AI Insights Dashboard.

Network Check

The following section provides details on the typical network issues you might face with the devices managed by Aruba Central network and the steps to help troubleshoot these issues.

Network Performance

To identify the network speed, you must perform a network check on the APs in the network. A network check aims to identify, diagnose, and debug issues detected in an Aruba Central-managed network. The **Network Check** tab on the **Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection.

The following tests are available for APs to troubleshoot issues pertaining to WLAN network connections:

- Ping Test
- Traceroute
- TCP Test
- HTTP Test
- HTTPS Test
- Speed Test (iPerf)

Ping Test

Sends ICMP echo packets to the hostname or IP addresses of the selected devices to check for latency issues.

To perform a ping test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the ping test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Ping Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. From the **Destination Type** drop-down list, select one of the following:
   - **Hostname/IP Address**—Enter the hostname or IP address.
   - **Client**—Select a client.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:

Show Additional Test Setting is not displayed when a **Test** type is not selected.

   a. In the **Packet Size** field, enter the packet size in order to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 65507 bytes.
   b. In the **Count** field, enter the count. The value should be between 1 to 2147483647.
   c. Select **Port** from the **Source Interface** drop-down list and select the port number.
8. Click **Run**. The output is displayed in the **Device Output** section.

Figure 544 *Ping Test—Device Output*

As mentioned in the steps, you can ping a client, gateway, or a WAN IP address to identify the wireless speed. When you ping the client, it sends the packets at a specified speed. If the network is slow, the time taken for the transfer will be high and some packets may get lost in the process. This behavior indicates that there is an issue between the AP and the client. Hence, when you notice that the network is slow, execute a ping test in **Tools** and check if the ping test is optimal. Similarly, you can choose your destination to be a gateway or a WAN/IP address. The tests show the same network speed from an AP to a gateway or from an AP to an outside WAN.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on APs, complete the following steps:

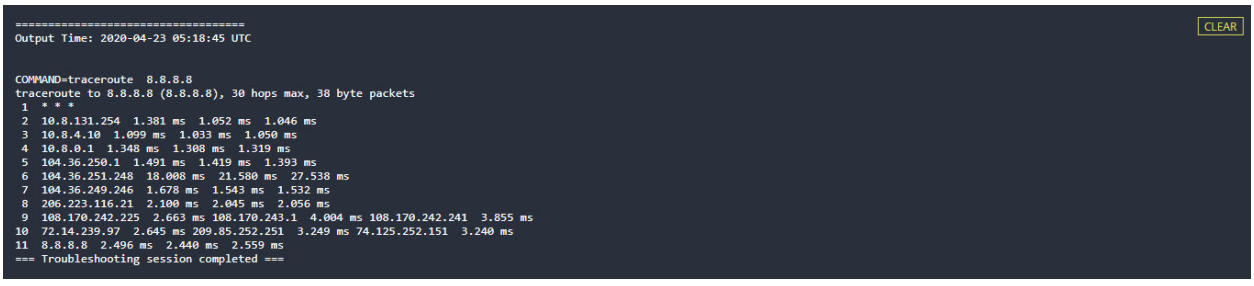
1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the traceroute test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. Click **Run**. The output is displayed in the **Device Output** section.

Figure 545 *Traceroute Test—Device Output*



TCP Test

Sends packets to the host such as an FTP server, and tries to establish a connection and exchanges data. If the FTP server returns a response, the issue could be isolated to the client device.

To perform a TCP test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

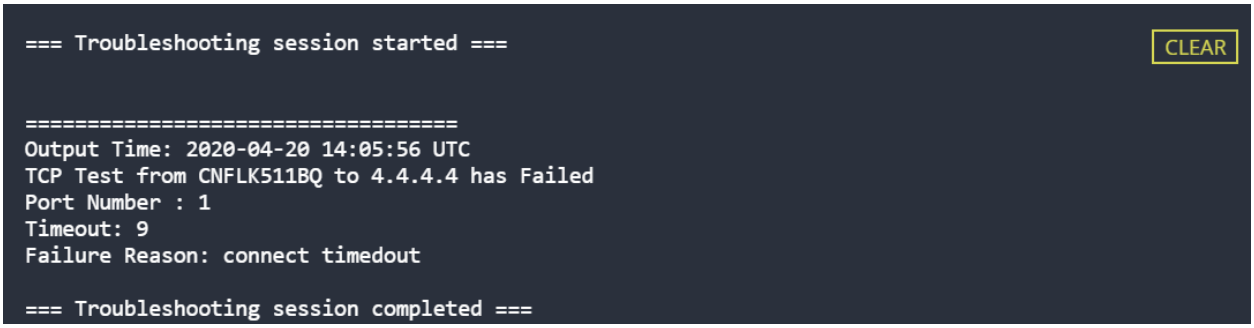
        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the TCP test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **TCP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter a valid IPv4 address in the **Host** field. Hostname is not supported.
7. Enter the port number in the **Port** field. The port number should be between 1 to 65535.
8. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, to enter the timeout value in seconds.
   The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.

Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 546 *TCP Test—Device Output*



The TCP test is supported only from ArubaOS 8.3.0.0 or later versions.

HTTP Test

Sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.

To perform an HTTP test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the HTTP test.

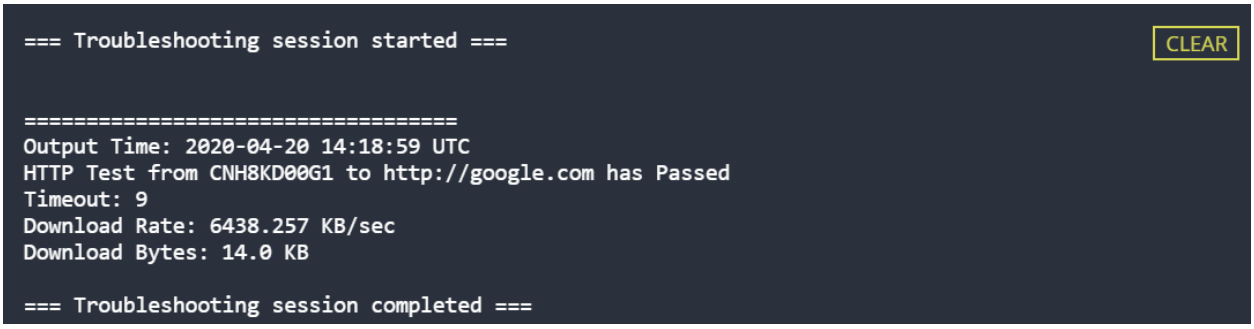
        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTP URL for which you want to perform the HTTP test, in the **URL** field, For example, http://*hostname* or http://*ipaddress*.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
   The value should be between 1 to 10 seconds. The default timeout value is 1 second.

NOTE

Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 547 *HTTP Test—Device Output*



NOTE

The HTTP test is supported only from ArubaOS 8.3.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

HTTPS Test

Sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device. HTTPS is a performance test to identify the time taken to load a web page.

To perform an HTTPS URL test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the HTTPS test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTPS URL for which you want to perform the HTTPS test, in the **URL** field, For example, https://*URL* or https://*IPv4*.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
   The value should be between 1 to 10 seconds. The default timeout value is 1 second.

NOTE

Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 548 *HTTPS Test—Device Output*

```
=== Troubleshooting session started ===                    CLEAR


==================================
Output Time: 2020-04-20 14:16:20 UTC
HTTPS Test from CNFLK511F1 to https://google.com has Passed
Timeout: 9
Download Rate: 6176.113 KB/sec
Download Bytes: 13.99 KB

=== Troubleshooting session completed ===
```

NOTE

If there is an application server running at the customer site and the application server has HTTPS and HTTP service enabled you can run these tests from the AP to the server. Once you run the test, the test status, download rate, and the download bytes indicate the network speed.

Speed Test (iPerf)

Performs a speed test to measure network speed and bandwidth. The speed test diagnostic tool is available only for Instant APs. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on APs, complete the following steps:

1. In the **Network Operations** app, select one of the following options:
   - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

     The dashboard context for the selected filter is displayed.
   - To select a device in the filter:
     a. Set the filter to **Global**.
     b. Under **Manage**, click **Devices** > **Access Points**.

        A list of access points is displayed in the **List** view.
     c. Click an access point listed under **Device Name** for which you want to perform the speed test.

        The dashboard context for the access point is displayed.
2. Under **Analyze** > **Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Speed Test (iPerf)**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. In the **Host** field, enter a valid hostname.
7. From the **Protocol** drop-down list, select the protocol. The available options are **TCP** or **UDP**.
8. To use additional parameters, click **Show Additional Test Settings** and in the **Options** field, enter the option. For example, bandwidth.

Show Additional Test Settings is not when a **Test** type is not selected.

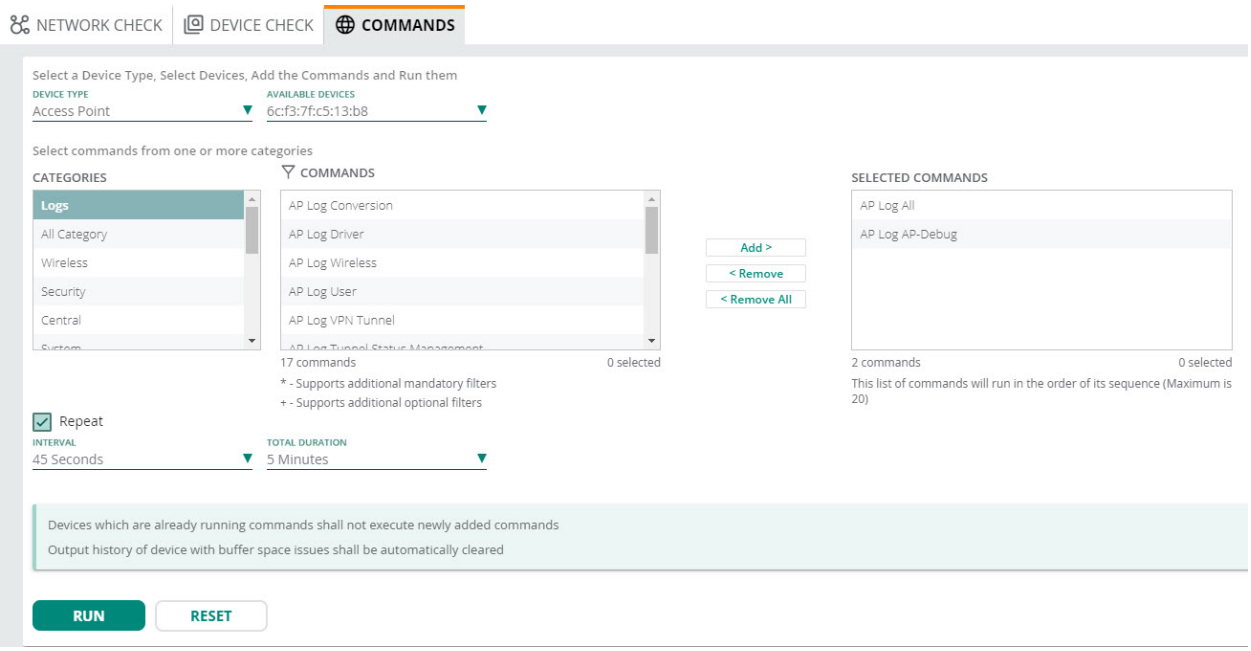
9. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 549 *Speed Test—Device Output*

While troubleshooting APs, a maximum of 20 APs are listed in the drop-down list. If there are more than 20 APs, use the **Search** option to search for an AP on which you would like to perform diagnostic checks

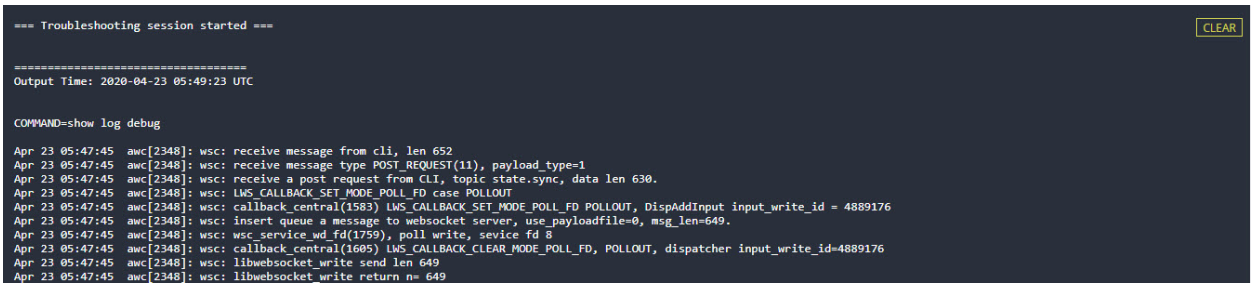
In addition to the **Network Check** tests, you can also leverage the **Commands** tab to troubleshoot your network performance using the available CLI commands. The **Commands** tab on the **Tools** page lists commands specific to a particular device to test the device entity and collect results based on your selection.

Figure 550 *Advanced Device Troubleshooting*



When a troubleshooting operation is initiated, Aruba Central establishes a session with the devices selected for the troubleshooting operation and displays the output in the **Device Output**.

Figure 551 *Command Test—Device Output*



Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output section displays information, such as list of devices on which the troubleshooting commands were executed, initial timestamp, **Test Type**, **Source**, and **Target**. It also shows the status of the tests as, in progress, complete, and buffer time. If there are multiple devices, select the device for which you want to view the output.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.