User Guide

Omada SDN Controller

© 2025 TP-Link 1910013934 V5.15.24

About this Guide

This User Guide provides information for centrally managing Omada devices via the Omada SDN Controller. Please read this guide carefully before operation.

Intended Readers

This User Guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

When using this guide, notice that:

- Features available in the Omada SDN Controller may vary due to your region, controller type and version, and device model. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.
- The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.
- This guide uses the specific formats to highlight special messages. The following table lists the notice icons that are used throughout this guide.

In this guide, the following conventions are used:

Controller	Stands for the Omada SDN Controller, including the Omada Software Controller, Omada Hardware Controller, Omada Integrated Gateway (Controller), and Omada Cloud-Based Controller.
On-premise controller	Includes the Omada Software Controller, Omada Hardware Controller, and Omada Integrated Gateway (Controller).
Gateway/Router	Stands for the Omada Gateway/Router.
Switch	Stands for the Omada Switch.
AP	Stands for the Omada AP.
Note:	The note contains the helpful information for a better use of the controller.
Configuration Guidelines:	Provide guidelines for the feature and its configurations.

More Resources

Main Site	https://www.omadanetworks.com/
Video Center	https://support.omadanetworks.com/video/
Documents	https://support.omadanetworks.com/document/
Product Support	https://support.omadanetworks.com/product/
Technical Support	https://support.omadanetworks.com/contact-support/

For technical support, the latest software, and management app, visit https://support.omadanetworks.com/.

CONTENTS

About this Guide

1.Omada SDN Controller Solution Overview

1. 1 Overview 2
1. 2 Core Components 3

2.Get Started with Omada SDN Controller

2. 1 Set Up Your Software Controller 8
2. 1. 1 Determine the Network Topology 8
2. 1. 2 Install the Software Controller 8
2. 1. 3 Start and Log In to the Software Controller 11
2. 2 Set Up Your Hardware Controller 16
2. 2. 1 Determine the Network Topology 16
2. 2. 2 Deploy the Hardware Controller 16
2. 2. 3 Start and Log in to the Controller 17
2. 3 Set Up Your Integrated Gateway (Controller) 21
2. 3. 1 Determine the Network Topology 21
2. 3. 2 Deploy the Integrated Gateway (Controller) 21
2. 3. 3 Start and Log in to the Controller 22
2. 4 Set Up Your Cloud-Based Controller 26

3.Get Started with Your Network on Omada SDN Controller

3. 1 Create Sites 28
3. 2 Configure the Site Template 32
3. 3 Adopt Devices 34
3. 3. 1 For Software Controller / Hardware Controller 34
3. 3. 2 For Integrated Gateway (Controller) 43
3. 3. 3 For Cloud-Based Controller 52
3. 4 Navigate the Controller UI 57

4.Configure the Network with the SDN Controller

4. 1 Modify the Current Site Settings 63
4. 1. 1 Site Configuration 63
4. 1. 2 General Config 64
4. 1. 3 Wireless Features 65

4. 1. 4 Device Account 68
4. 2 Configure Wired Networks 70
4. 2. 1 Set Up an Internet Connection 70
4. 2. 2 Configure LAN Networks 88
4. 2. 3 Configure LAN DNS 100
4. 3 Configure Wireless Networks 102
4. 3. 1 Set Up Basic Wireless Networks 102
4. 3. 2 Advanced Settings 108
4. 3. 3 WLAN Schedule 110
4. 3. 4 802.11 Rate Control 110
4. 3. 5 MAC Filter 111
4. 3. 6 Multicast/Broadcast Management 112
4. 3. 7 WLAN Optimization 113
4. 3. 8 Bluetooth Settings 115
4. 4 Network Security 120
4. 4. 1 ACL 120
4. 4. 2 URL Filtering 130
4. 4. 3 MAC Filtering 133
4. 4. 4 Attack Defense 134
4. 4. 5 Firewall 138
4. 4. 6 IP-MAC Binding 140
4. 4. 7 IDS/IPS 142
4. 4. 8 Application Control 147
4. 5 Transmission 151
4. 5. 1 Routing 151
4. 5. 2 Switch OSPF 154
4. 5. 3 NAT 156
4. 5. 4 Session Limit 161
4. 5. 5 Bandwidth Control 162
4. 5. 6 Gateway QoS 164
4. 5. 7 Switch QoS 168
4. 5. 8 VRRP 170
4. 6 Configure VPN 172
4. 6. 1 VPN 172
4. 6. 2 VPN User 198
4. 6. 3 IPsec Failover 199
4. 6. 4 SSL VPN 200
4. 6. 5 WireGuard VPN 207
4. 7 Create Profiles 210

4. 7. 1 Time Range 210
4. 7. 2 Groups 211
4. 7. 3 Rate Limit 213
4. 7. 4 PPSK 214
4. 7. 5 Gateway QoS Service 216
4. 7. 6 Bonjour Service 217
4. 7. 7 RADIUS Profile 218
4. 7. 8 LDAP Profiles 221
4. 7. 9 APN Profile 223
4. 8 Authentication 225
4. 8. 1 Portal 225
4. 8. 2 802.1X 234
4. 8. 3 MAC-Based Authentication 237
4. 9 Services 240
4. 9. 1 DHCP Reservation 240
4. 9. 2 Dynamic DNS 241
4. 9. 3 mDNS 244
4. 9. 4 SNMP 245
4. 9. 5 UPnP 246
4. 9. 6 SSH 247
4. 9. 7 Reboot Schedule 248
4. 9. 8 Port Schedule 249
4. 9. 9 IPTV 250
4. 9. 10 DNS Proxy 252
4. 9. 11 Auto Send Data to Email 253
4. 10 SIM 254
4. 10. 1 Statistics 254
4. 10. 2 SMS Message 256
4. 10. 3 SMS Settings 257
4. 11 CLI Configuration 260
4. 11. 1 Site CLI 262
4. 11. 2 Device CLI 263

5.Configure the SDN Controller

5. 1 System Settings 266
5. 1. 1 Controller Status 266
5. 1. 2 Controller Updates 266
5. 1. 3 HTTPS Certificate 267

5. 1. 4 System Logging 268
5. 1. 5 Access Config 269
5. 2 Controller Settings 272
5. 2. 1 General Settings 272
5. 2. 2 Services 274
5. 2. 3 MSP Mode 275
5. 2. 4 Join User Experience Improvement Programm 275
5. 3 UI Interaction 276
5. 3. 1 User Interface 276
5. 3. 2 Notifications 276
5. 4 History Data Retention 277
5. 5 Server Settings 279
5. 5. 1 Mail Server 279
5. 5. 2 Built-in RADIUS 280
5. 5. 3 Radius Proxy Server 282
5. 6 Account Security 283
5. 6. 1 Two-Factor Authentication (2FA) 283
5. 6. 2 Controller IP Access Rules 283
5. 7 Maintenance 284
5. 7. 1 Restore 284
5. 7. 2 Backup 284
5. 7. 3 Backup Schedule 286
5. 8 Migration 289
5. 8. 1 Site Migration 289
5. 8. 2 Controller Migration 294
5. 9 Export Data 299
5. 9. 1 Export Data 299
5. 9. 2 Export for Support 300
5. 9. 3 Auto Send Data to Email 301
5. 10 Cloud Access 302

6.Configure and Monitor Controller-Managed Devices

6. 1 Introduction to the Devices Page 305
6. 2 Configure and Monitor the Gateway 309
6. 2. 1 Configure the Gateway 309
6. 2. 2 Monitor the Gateway 319
6. 3 Configure and Monitor Switches 321
6. 3. 1 Configure Switches 321

6. 3. 2 Monitor Switches 343
6. 4 Configure and Monitor APs 347
6. 4. 1 Configure APs 347
6. 4. 2 Monitor APs 358
6. 5 Create and Manage Stack Groups 370
6. 5. 1 Introduction to Stack 370
6. 5. 2 Create a Stack Group 370
6. 5. 3 Configure and Monitor the Stack Group 371
6. 6 Create and Manage Bridge Groups 372
6. 6. 1 Introduction to Bridge 372
6. 6. 2 Create a Bridge Group 372
6. 6. 3 Configure and Monitor the Bridge Group 373

7.Monitor and Manage the Clients

7. 1 Manage Wired and Wireless Clients in Clients Page 375
7. 1. 1 Introduction to Clients Page 375
7. 1. 2 Using the Clients Table to Monitor and Manage the Clients 375
7. 1. 3 Using the Properties Window to Monitor and Manage the Clients 377
7. 2 Manage Client Authentication in Hotspot 380
7. 2. 1 Dashboard 380
7. 2. 2 Authorized Clients 381
7. 2. 3 Vouchers 381
7. 2. 4 Local Users 385
7. 2. 5 Form Auth Data 389
7. 2. 6 Operators 389

8.Monitor the Network

8. 1 View the Status of Network with Dashboard 392
8. 1. 1 Page Layout of Dashboard 392
8. 1. 2 Explanation of Widgets 393
8. 2 View the Statistics of the Network 404
8. 2. 1 Performance 404
8. 2. 2 Application Analytics 409
8. 3 Monitor the Network with Map 410
8. 3. 1 Topology 410
8. 3. 2 Heat Map 412
8. 3. 3 Device Map 417
8. 3. 4 Site Map 419

8. 4 Monitor the Network with Reports 423
8. 5 View Statistics During Specified Period with Insight 425
8. 5. 1 Session Limit 425
8. 5. 2 Known Clients 425
8. 5. 3 Past Connections 426
8. 5. 4 Past Portal Authorizations 427
8. 5. 5 Switch Status 428
8. 5. 6 Port Forwarding Status 432
8. 5. 7 VPN Status 433
8. 5. 8 Routing Table 436
8. 5. 9 Dynamic DNS 437
8. 5. 10 Rogue APs 437
8. 5. 11 Threat Management 439
8. 6 View and Manage Logs 441
8. 6. 1 Alerts 441
8. 6. 2 Events 443
8. 6. 3 Notifications 444
8. 7 Audit Logs 448
8. 8 Monitor the Network with Tools 449
8. 8. 1 Network Check 449
8. 8. 2 Packet Capture 450
8. 8. 3 Terminal 451

9.Manage Accounts of the SDN Controller

9. 1 Introduction to User Accounts 454
9. 2 Create and Manage Roles 455
9. 3 Create and Manage Local User Accounts 455
9. 3. 1 Edit the Owner Account 455
9. 3. 2 Create and Manage Other Local Accounts 456
9. 4 Create and Manage Cloud User Accounts 458
9. 4. 1 Set Up the Cloud Owner Account 458
9. 4. 2 Create and Manage Other Cloud Accounts 458
9. 5 Manage User Accounts Across Controllers 460

10.Manage Customer Networks in MSP Mode

10. 1 Quick Start 463
10. 1. 1 Enable the MSP Mode 463
10. 1. 2 Add and Manage Customers 464

10. 1. 3 Add Sites and Devices 466
10. 2 Add and Manage MSP Accounts 467

11.Configure Platform Integration and SAML SSO

11. 1 Open API 469
11. 2 Webhooks 471
11. 3 SAML SSO 472

12.Configure SD-WAN

13.Configure Multi-Controller Clusters

13. 1 Introduction to Multi-Controller Clusters 481
13. 2 Configure Hot-Standby Backup Mode on Omada Controllers 482
13. 3 Configure Distributed Cluster Mode on Linux Controllers 484
13. 3. 1 Configure an Existing Controller via Web 485
13. 3. 2 Configure a New Controller via Commands 486

Chapter 1

Omada SDN Controller Solution Overview

Omada SDN Controller Solution offers centralized and efficient management for configuring enterprise networks comprised of security gateways, switches, and wireless access points.

With a reliable network management platform powered by TP-Link Omada SDN Controller, you can develop comprehensive, software-defined networking across demanding, high-traffic environments with robust wired and wireless solutions.

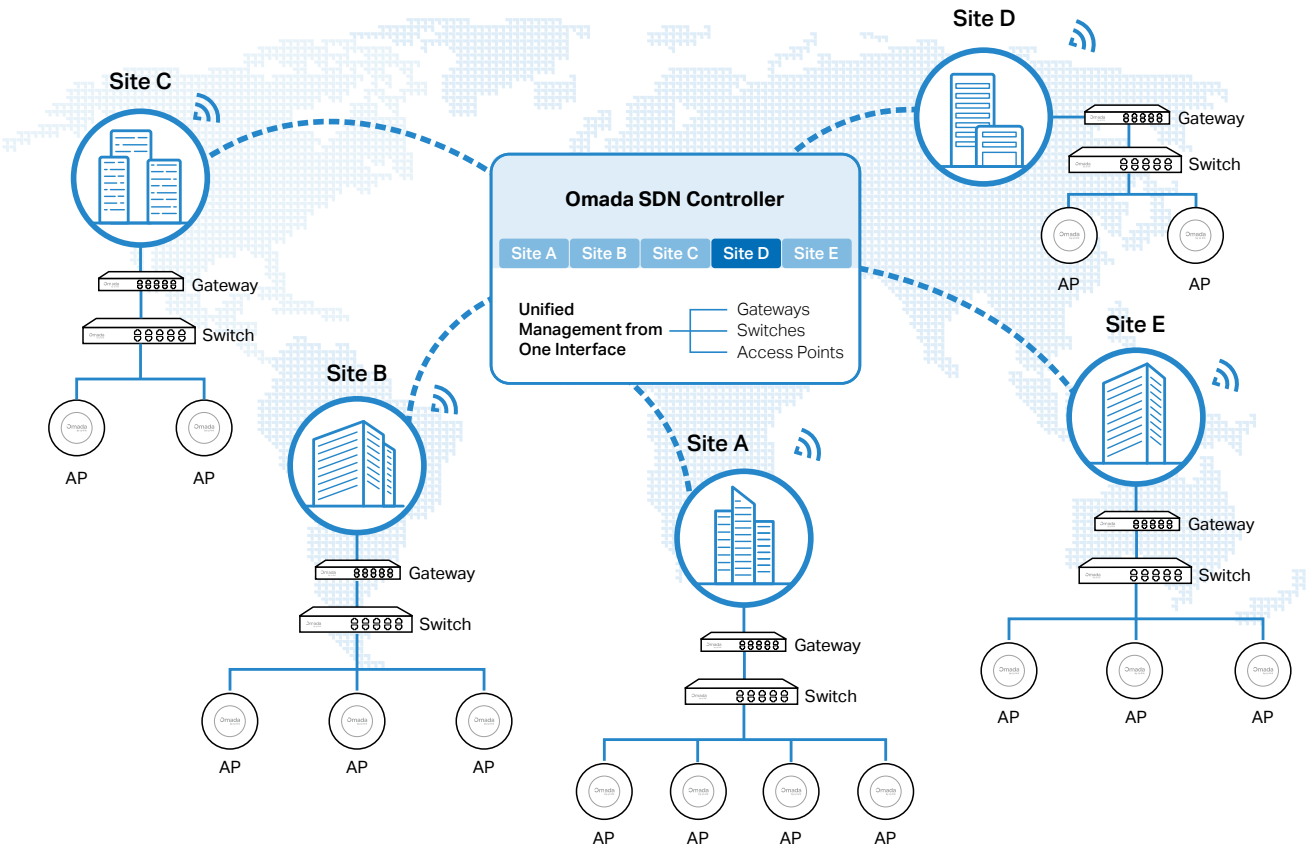
The chapter includes the following sections:

- 1. 1 Overview
- 1. 2 Core Components

1. 1 Overview

Omada SDN Controller Solution is designed to provide business-class networking solutions for demanding, high-traffic environments such as campuses, hotels, malls, and offices. It simplifies deploying and managing large-scale enterprise networks and offers easy maintenance, ongoing monitoring, and flexible scalability.

This figure shows a sample architecture of an Omada SDN enterprise network:



The interconnected elements that work together to deliver a unified enterprise network include: SDN Controller, gateways, switches, access points, and client devices. Beginning with a base of client devices, each element adds functionality and complexity as the network is developing, interconnecting with the elements above and below it to create a comprehensive, secure wired and wireless solution.

The SDN Controller is a command center and management platform at the heart of the network. With a single platform, the network administrators configure and manage enterprise networks comprised of routers, switches, and wireless access points in batches. This unleashes new levels of management to avoid complex and costly over-provisioning.

1. 2 Core Components

An Omada SDN network consists of the following core components:

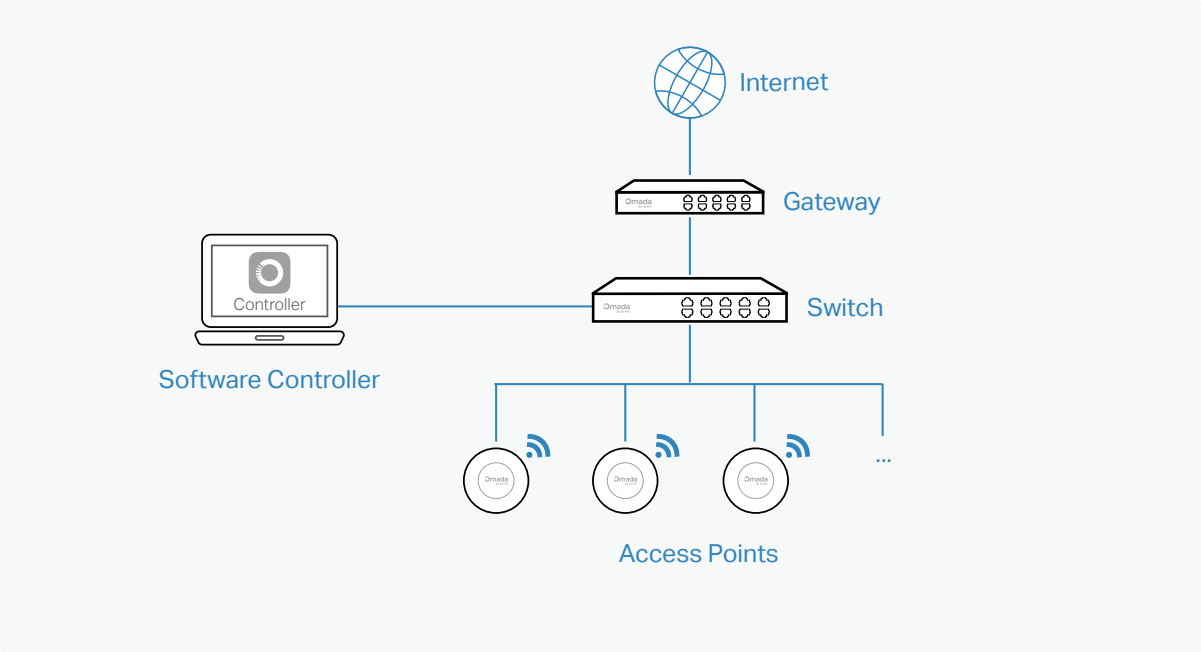
- SDN Controller — A command center and management platform at the heart of network solution for the enterprise. With a single platform, the network administrators configure and manage all Omada products which have all your needs covered in terms of routing, switching and Wi-Fi.
- Gateways — Boast excellent data processing capabilities and an array of powerful functions, including IPsec/OpenVPN/PPTP/L2TP VPN, Load Balance, and Bandwidth Control, which are ideal for the business network where a large number of users require a stable, secure connection.
- Switches — Offer flexible and cost-effective network solution with powerful Layer 2 features and PoE options. Advanced features such as Access Control, QoS, LAG and Spanning Tree will satisfy advanced business networks.
- Access Points — Satisfy the mainstream Wi-Fi Standard and address your high-density access needs with TP-Link's innovation to help you build the versatile and reliable wireless network for all business applications.

SDN Controller

Tailored to different needs and budgets, Omada SDN Controller offers diverse deployment solutions. Omada Software Controller, Hardware Controller, and Cloud-Based Controller each has their own set of advantages and applications.

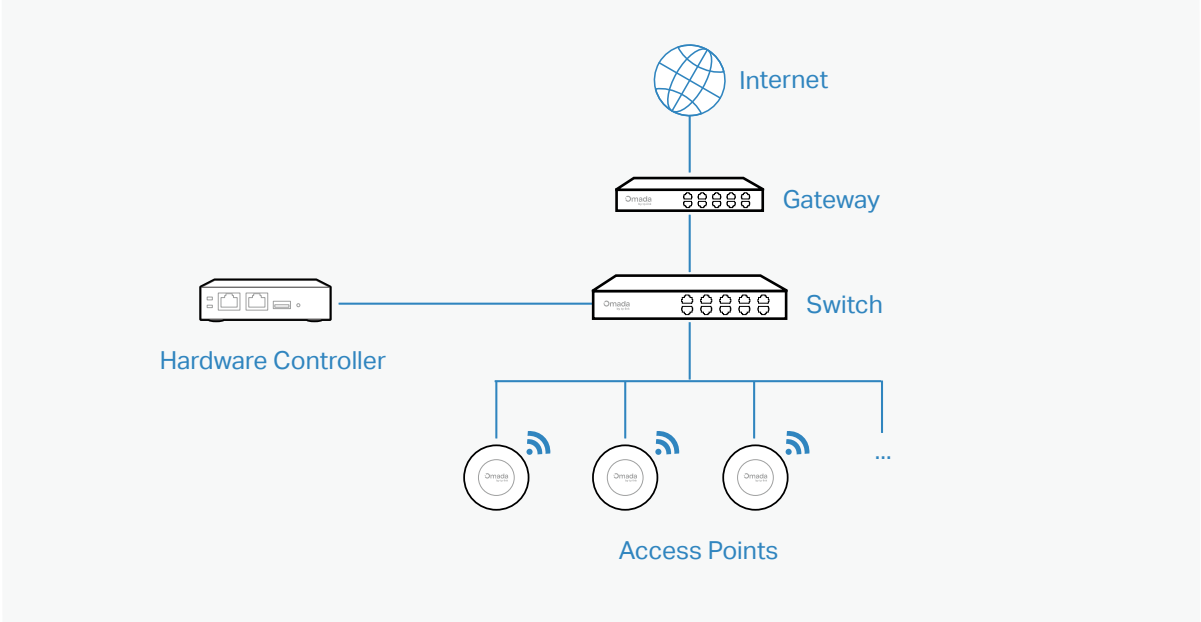
- Omada Software Controller

  Omada Software Controller can be hosted on any computers with Windows or Linux systems on your network.



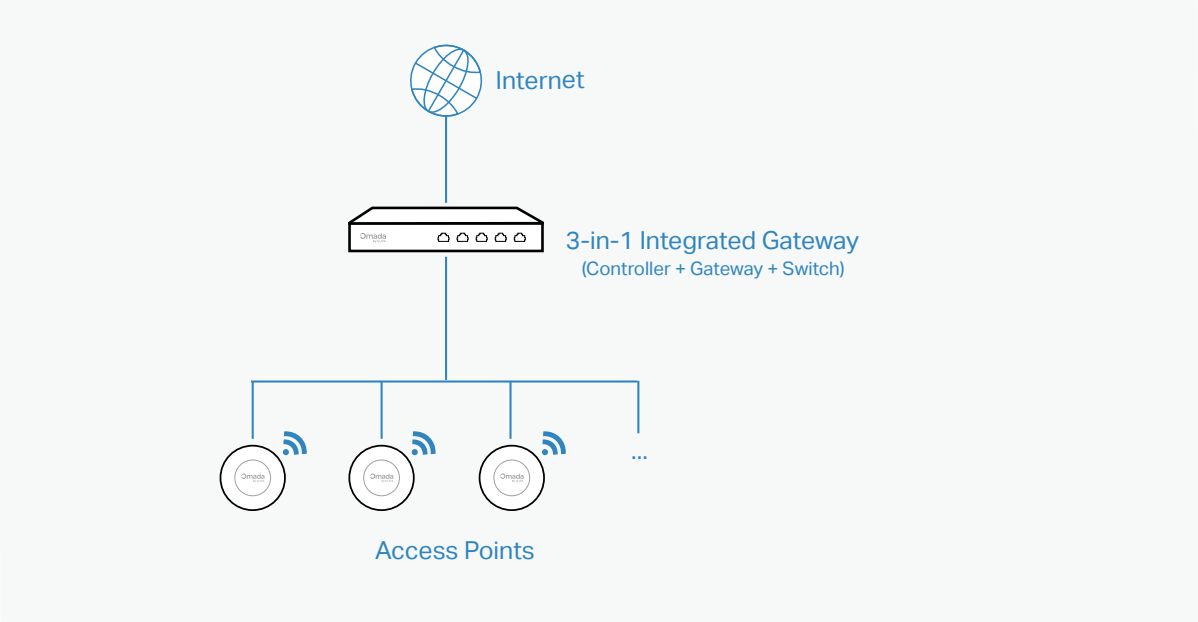
- Omada Hardware Controller

  Omada Hardware Controller is the management device which is pre-installed with Omada Software Controller. You just need to purchase the device, then the built-in software controller is ready to use. About the size of a mobile phone, the device is easy to deploy and install on your network.



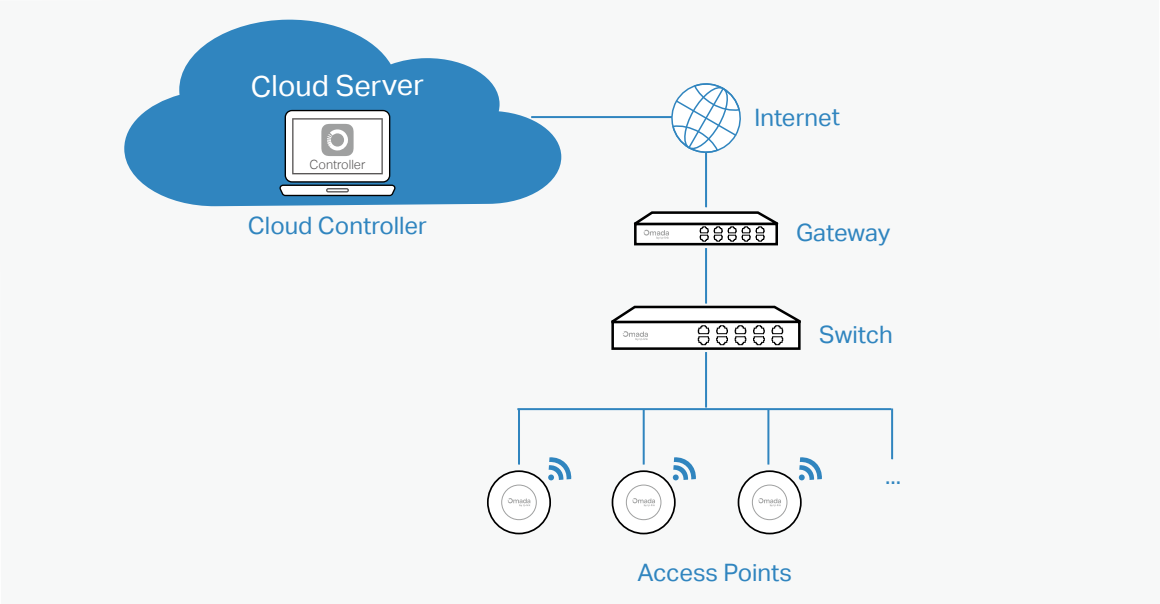
- Omada 3-in-1 Integrated Gateway (Controller)

  Omada 3-in-1 Integrated Gateway integrates PoE+ ports and Controller ability. It is the management device which is pre-installed with Omada Software Controller. You just need to purchase the device, then the built-in software controller is ready to use. It can also work as the Gateway and Switch at the same time, allowing you to connect to Omada access points and PoE-supported devices with ease.



- Omada Cloud-Based Controller

  Omada Cloud controller is deployed on the Omada Cloud server, providing paid license service with tiered pricing. With paid licenses bound to the devices on the controller, you can configure and manage the devices via the cloud Service. And you need not purchase an additional hardware device or install the software on the host.



The controllers differ in forms, but they have almost the same browser–based management interface and serve the same functions of network management.

Gateways

TP-Link's Omada Gateway supports Gigabit Ethernet connections on both WAN and LAN ports which keep the data moving at top speed. Including all the routing and network segmentation functions that a business router must have, SafeStream VPN Router will be the backbone of the SDN network. Moreover,

the router provides a secure and easy approach to deploy site-to-site VPN tunnels and access for remote clients.

Managing the gateway centrally through Omada SDN Controller is available on certain models only. For more information, refer to https://www.omadanetworks.com/omada-sdn/product-list/.

Switches

TP-Link's JetStream Switch provides high-performance and enterprise-level security strategies and lots of advanced features, which is ideal access-edge for the SDN network.

Managing the switch centrally through Omada SDN Controller is available on certain models only. For more information, refer to https://www.omadanetworks.com/omada-sdn/product-list/.

Access Points

TP-Link's Omada Access Point provides business-class Wi-Fi with superior performance and range which guarantees reliable wireless connectivity for the SDN network.

Managing the access points centrally through Omada SDN Controller is available on certain models only. For more information, refer to https://www.omadanetworks.com/omada-sdn/product-list/.

Chapter 2

Get Started with Omada SDN Controller

This chapter guides you on how to get started with Omada SDN Controller to configure the network. Omada Software Controller, Omada Hardware Controller, and Omada Cloud-Based Controller differ in forms, but they have almost the same browser–based management interface for network management. Therefore, they have almost the same initial setup steps, including building your network topology, deploying your controller, and logging in to the controller. The chapter includes the following sections:

- 2. 1 Set Up Your Software Controller
- 2. 2 Set Up Your Hardware Controller
- 2. 3 Set Up Your Integrated Gateway (Controller)
- 2. 4 Set Up Your Cloud-Based Controller

2. 1 Set Up Your Software Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up the Software Controller:

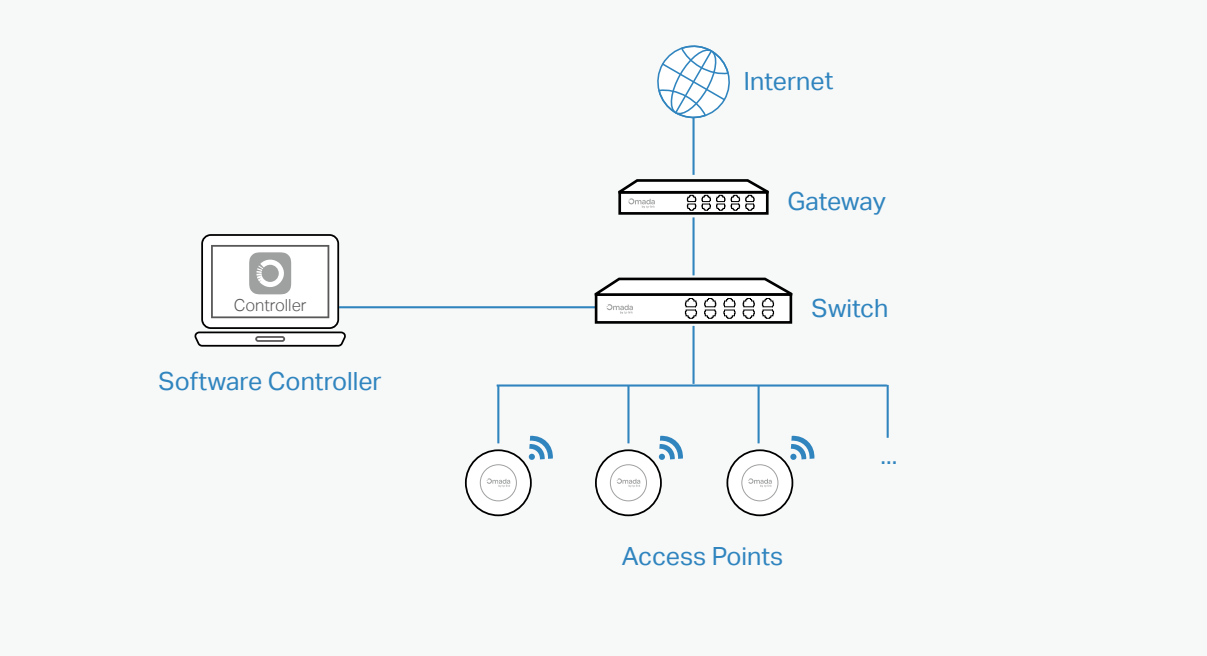
1) Determine the network topology.

2) Install the Software Controller.

3) Start and log in to the controller.

2. 1. 1 Determine the Network Topology

The network topology that you create for the SDN Controller varies depending on your business requirements. The following figure shows a typical topology for a high-availability use case.



Note:

When using the Omada SDN Controller, we recommend that you deploy the full topology with Omada-supported TP-Link devices. If you use third-party devices, Omada SDN Controller cannot discover and manage them.

2. 1. 2 Install the Software Controller

Omada Software Controller is provided for both Windows and Linux operating systems. Determine your operating system and follow the introductions below to install the Software Controller.

Installation on Windows Host

Omada Software Controller can be hosted on any computers with Windows systems on your network. Make sure your PC's hardware and system meet the following requirements, then properly install the Software Controller.

- **Hardware Requirements**

  To guarantee operational stability, we recommend that you use the hardware which meets or exceeds the following specifications:

  CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.

  Memory: 16 GB RAM or more.

- **System Requirements**

  Operating System: Microsoft Windows 7/8/10/Server. (We recommend that you deploy the controller on a 64-bit operating system to guarantee the software stability.)

  Web Browser: Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 11 (or above).

- **Install the Software Controller**

  Download the installation file of Software Controller from https://support.omadanetworks.com/download/software/omada-controller/. Then follow the instructions to install the controller. After a successful installation, the controller shortcut icon will be created on your desktop.

Installation on Linux Host

Two versions of installation package are provided: **.tar.gz** file and **.deb** file. Both of them can be used in multiple versions of Linux operating system, including Ubuntu, CentOS, Fedora, and Debian.

Make sure your PC's hardware and system meet the following requirements, then choose the proper installation files to install the Software Controller.

- **Hardware Requirements**

  To guarantee operational stability, we recommend that you use the hardware which meets or exceeds the following specifications:

  CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.

  Memory: 16 GB RAM or more.

- **System Requirements**

  Operating System: 64-bit Linux operating system, including Ubuntu 14.04/16.04/17.04/18.04, CentOS 6.x/7.x, Fedora 20 (or above), and Debian 9.8.

  Web Browser: Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 11 (or above).

- **Install the Software Controller**

  Download the installation file of Software Controller from https://support.omadanetworks.com/download/software/omada-controller/. Check the prerequisites and follow the steps based on your file version to install the controller.

  - Prerequisites for installing

    To successfully install the Software Controller, ensure that you have performed the following tasks before your installation:

a. Ensure that the Java Runtime Environment (JRE) has been installed in your system. The controller requires that the system has Java 8 installed. Download the file according to your operating system from https://www.java.com/download/linux_manual.jsp and follow the instructions to install the JRE.

   For Ubuntu16.04 or above, you can use the command: **apt-get install openjdk-8-jre-headless** to get the Java 8 installed.

b. Ensure that MongoDB has been installed in your system. The controller works when the system runs MongoDB 3.0.15–3.6.18. Download the file according to your operating system from the https://www.mongodb.com/try/download and follow the instructions to install the MongoDB.

c. Ensure that you have **jsvc** and **curl** installed in your system before installation, which is vital to the smooth running of the system. If your system does not have **jsvc** or **curl** installed, you can install it manually with the command: **apt-get install** or **yum install**. For example, you can use the command: **apt-get install jsvc** or **yum install jsvc** to get **jsvc** installed. And if dependencies are missing, you can use the command: **apt-get -f install** to fix the problem.

  - Install the .tar.gz file

a. Make sure your PC is running in the root mode. You can use this command to enter root mode:
   sudo

b. Extract the tar.gz file using the command:
   tar zxvf Omada_Controller_v*x.x.x*_**linux_x64_targz.tar.gz**

c. Install the Controller using the command:
   sudo bash ./install.sh

  - Install the .deb file

a. Make sure your PC is running in the root mode. You can use this command to enter root mode:
   sudo

b. Install the .deb file using the command:
   dpkg -i Omada_Controller_v*x.x.x*_**linux_x64.deb**

   If dependencies are missing during the installation, you can use the command: **apt-fix-broken install** to fix the problem.

After installing the controller, use the following commands to check and change the status of the controller.

a. **tpeap start** — Start the controller, use the command.

b. **tpeap stop** — Stop running the Controller.

c. **tpeap status** — Show the status of Controller.

For more detailed information about the installation on Linux hosts, refer to the Installation Instructions.

Note:

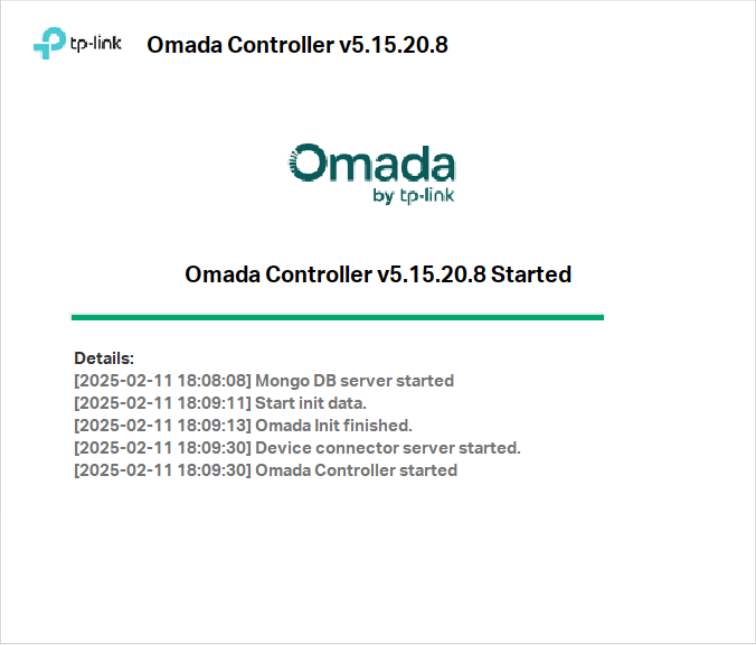
- For installing the .tar.gz, if you want the Controller to run as a user (it runs as root by default) you should modify OMADA_USER value in bin/control.sh.
- To uninstall the Controller, go to the installation path: /opt/tplink/EAPController, and run the command: sudo bash ./uninstall.sh.
- During uninstallation, you can choose whether to back up the database. The backup folder is /opt/tplink/eap_db_backup.
- During installation, you will be asked whether to restore the database if there is any backup database in the folder /opt/tplink/eap_db_backup.

2. 1. 3 Start and Log In to the Software Controller

Launch the Software Controller and follow the instructions to complete basic configurations, and then you can log in to the management interface.

Launch the Software Controller

Double-click the controller shortcut icon and the following window will pop up. After a while, your web browser will automatically open.



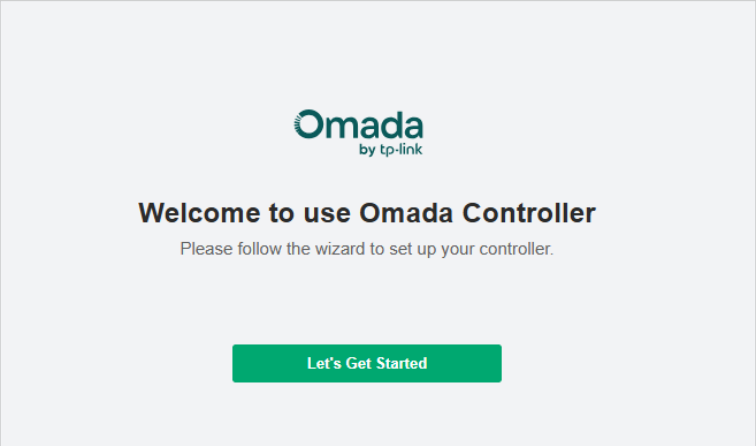
Note:

- If your browser does not open automatically, click Launch. You can also launch a web browser and enter http://127.0.0.1:8088 in the address bar.
- If your web browser opens but prompts a problem with the website's security certificate, click Continue.

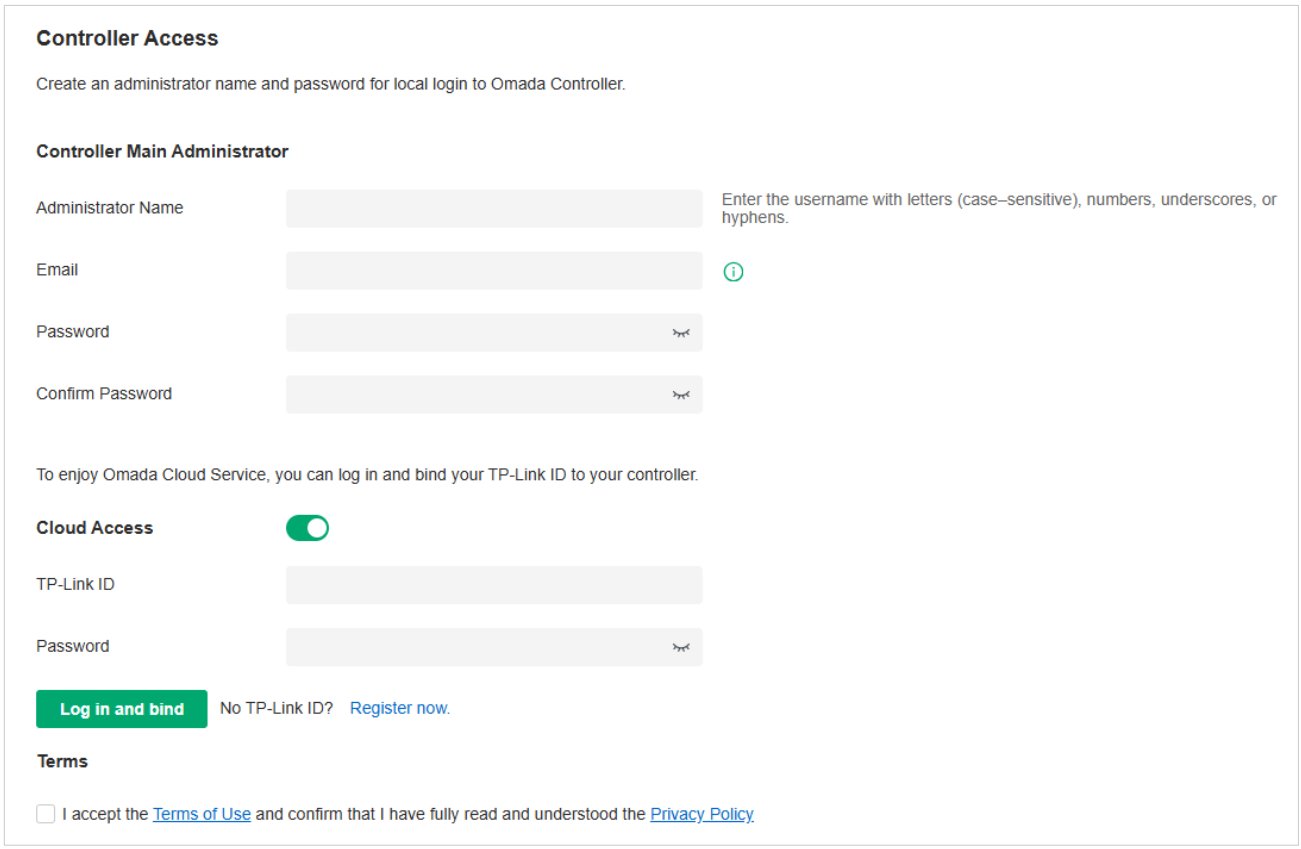
Complete Basic Configurations

In the web browser, you can see the configuration page. Follow the setup wizard to complete the basic settings for the Controller.

1. Click Let's Get Started.



2. Set up controller access settings.



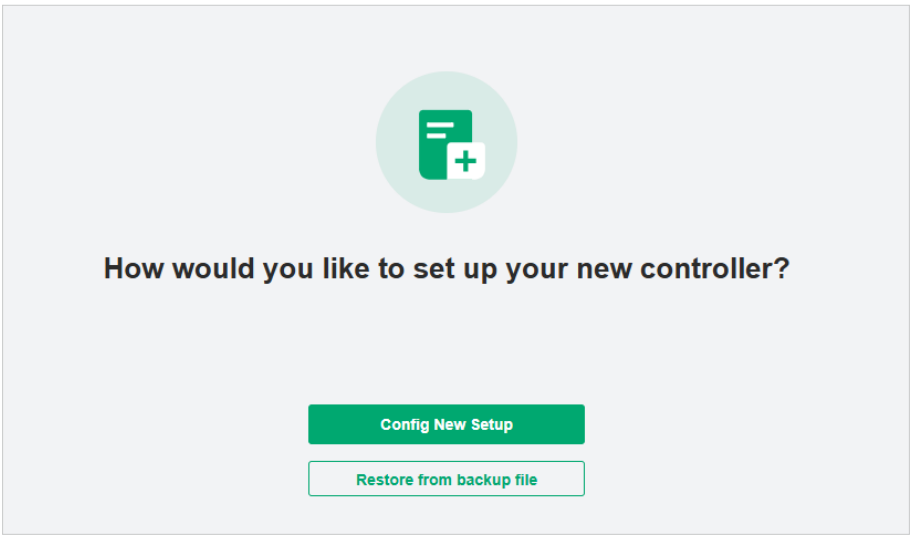
a. Create an Administrator username and password for login to the controller. Specify the email address for resetting your password in case that you forget the password. After logging into the Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to 8. 6. 3 Notifications.

b. If you want to access the controller to manage networks remotely, enable Cloud Access, and bind your TP-Link ID to your Controller. For more details about cloud access, please refer to 5. 9 Export Data.

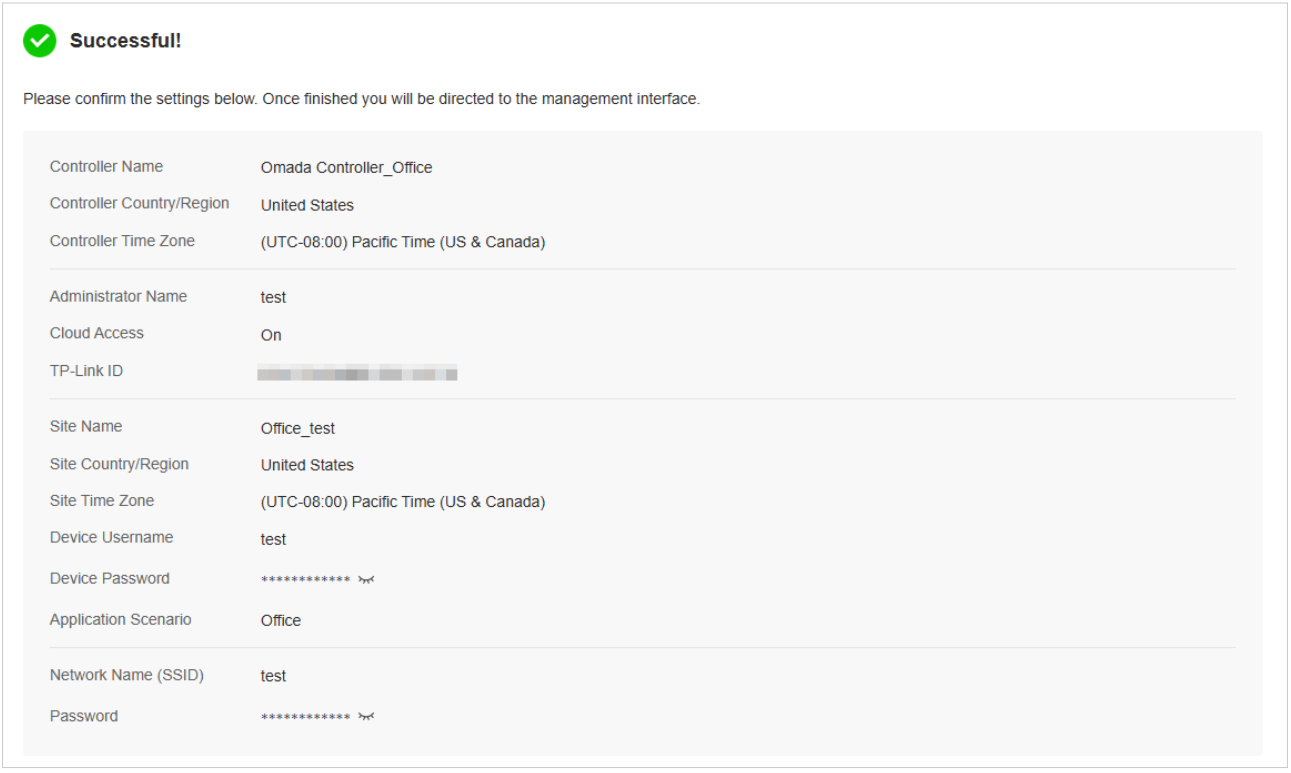
c. Read and agree to TP-Link's Terms of Use.

d. Click Next.

3. Choose how would you like to set up your new controller. You can configure a new setup or restore from backup file.

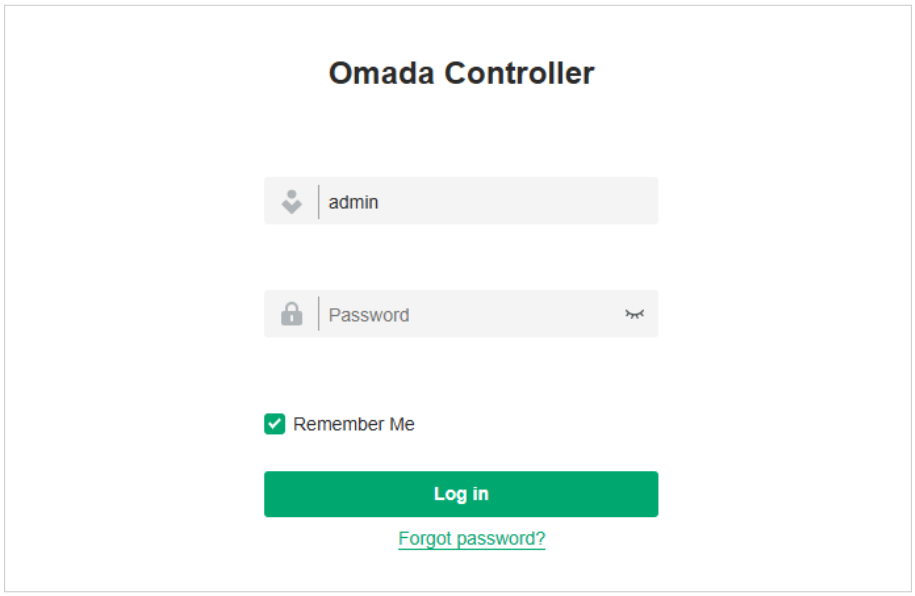


4. Follow the setup wizard to set up the controller.



Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.



Note:

In addition to the Controller Host, other hosts in the same LAN can also manage EAPs via remote access to the Controller Host. For example, if the IP address of the Controller Host is 192.168.0.100 and the Controller is running normally on this host, you can enter https://192.168.0.100:8043, or http://192.168.0.100:8088 in the web browser of other hosts in the same LAN to log in to the the Controller and manage EAPs. Or you can log in to the Controller using other management devices through Cloud service.

2. 2 Set Up Your Hardware Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up the Hardware Controller:

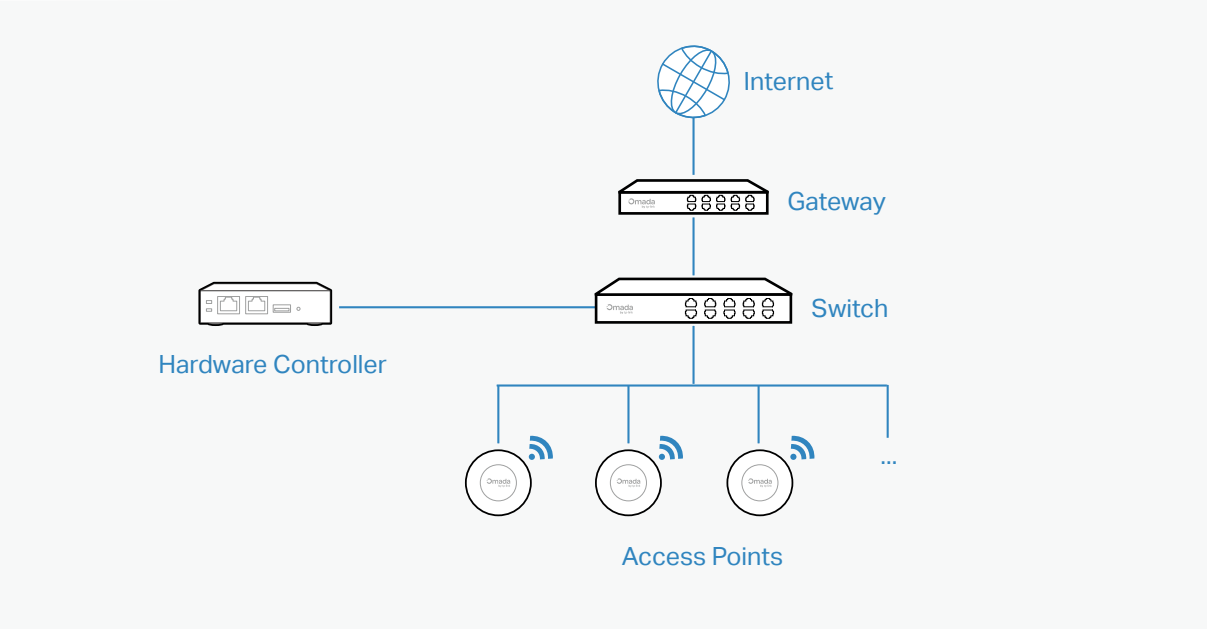
1) Determine the network topology.

2) Deploy the Hardware Controller.

3) Start and log in to the controller.

2. 2. 1 Determine the Network Topology

The network topology that you create for the SDN Controller varies depending on your business requirements. The following figure shows a typical topology for a high-availability use case.



Note:

When using the Omada SDN Controller, we recommend that you deploy the full topology with Omada-supported TP-Link devices. If you use third-party devices, Omada SDN Controller cannot discover and manage them.

2. 2. 2 Deploy the Hardware Controller

Omada Hardware Controller comes with the pre-installed controller software, so installation is not necessary. After deploying the Hardware Controller on your network infrastructure, proceed to configure the controller.

2. 2. 3 Start and Log in to the Controller

Log In to the Management Interface

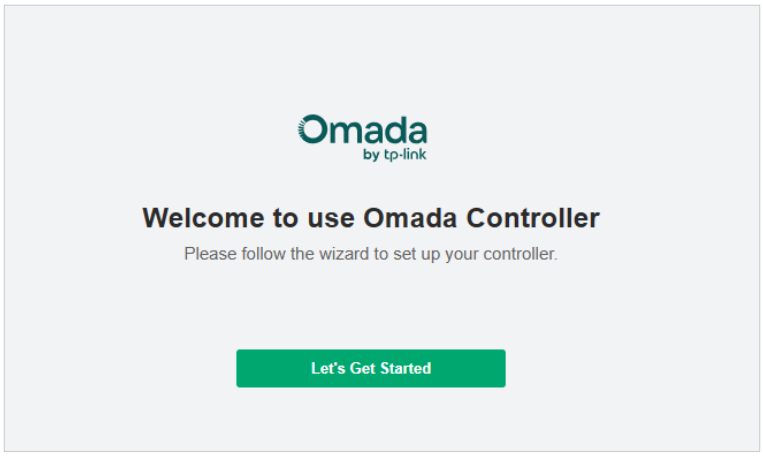
Follow the steps below to enter the management interface of the Hardware Controller:

1. Make sure that your management device has the route to access the controller.
2. Check the DHCP server (typically a router) for the IP Address of the controller. If the controller fails to get a dynamic IP address from the DHCP server, the default fallback IP address 192.168.0.253, is used.
3. Launch a web browser and type the IP address of the controller in the address bar, then press **Enter** (Windows) or **Return** (Mac).

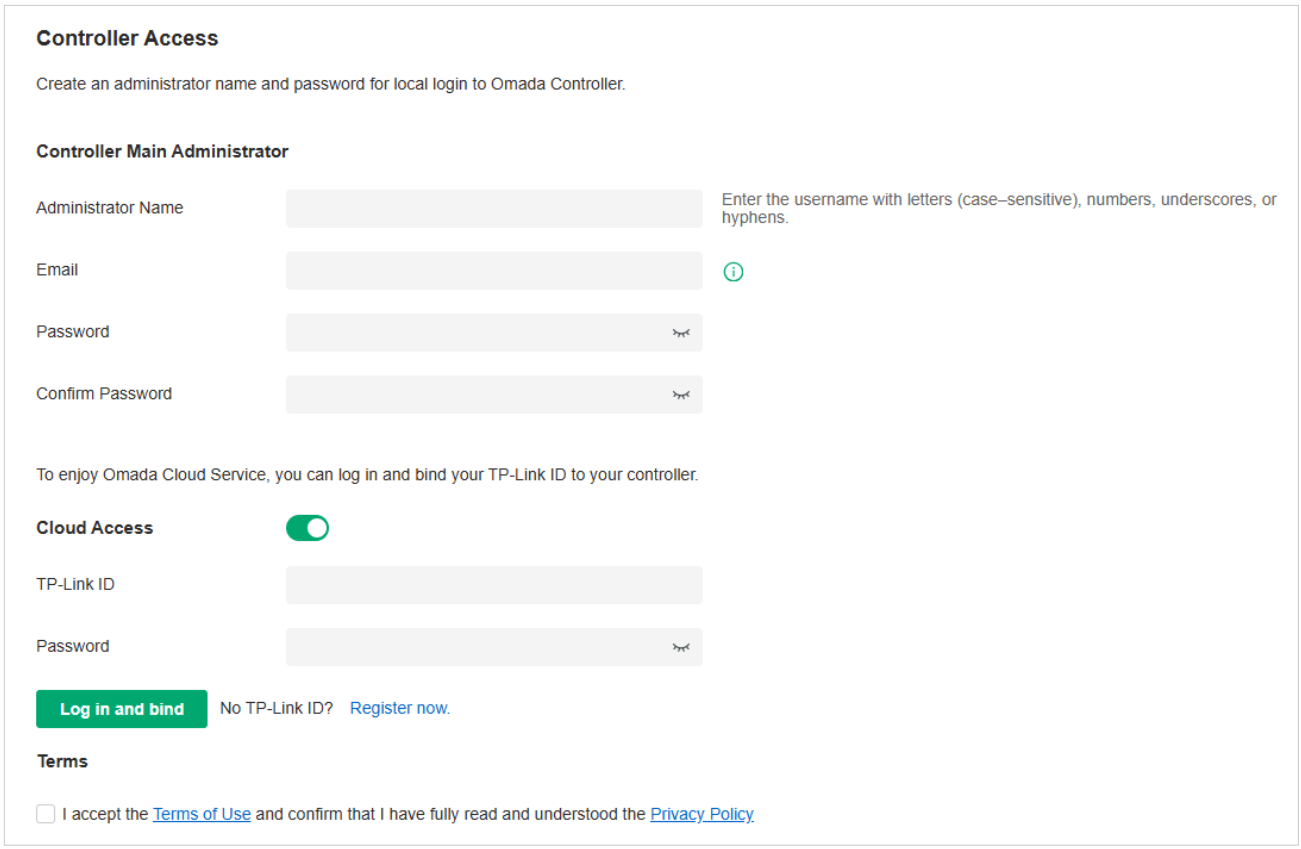
Complete Basic Configurations

In the web browser, you can see the configuration page. Follow the setup wizard to complete the basic settings for the Controller.

1. Click Let's Get Started.



2. Set up controller access settings.



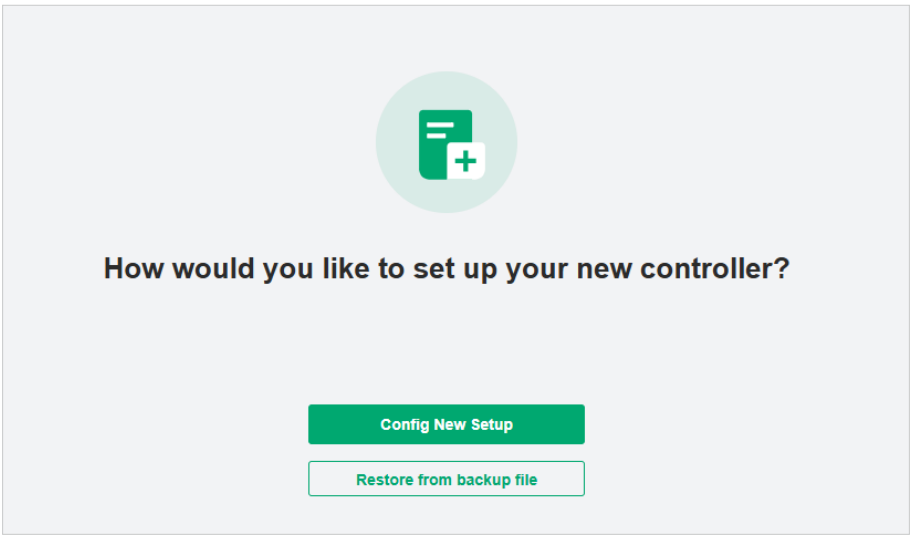
a. Create an Administrator username and password for login to the controller. Specify the email address for resetting your password in case that you forget the password. After logging into the Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to 8. 6. 3 Notifications.

b. If you want to access the controller to manage networks remotely, enable Cloud Access, and bind your TP-Link ID to your Controller. For more details about cloud access, please refer to 5. 10 Cloud Access.

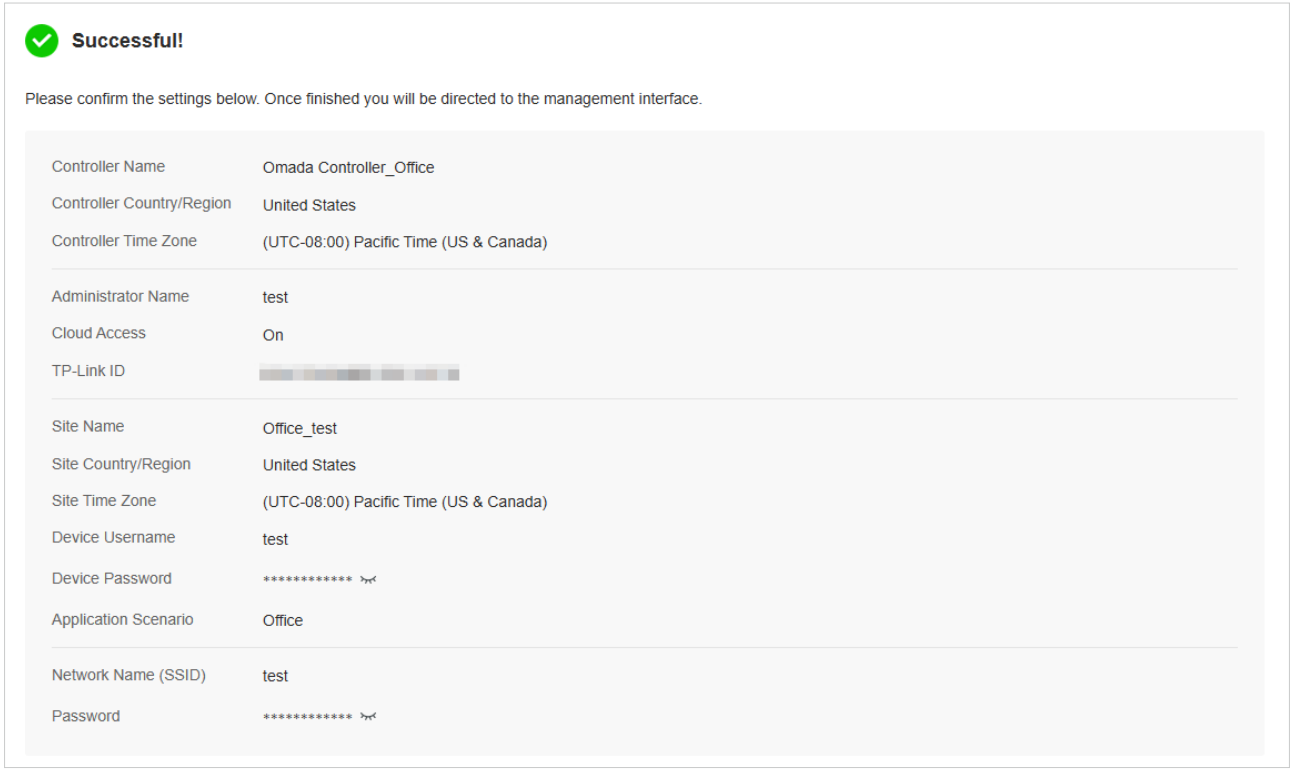
c. Read and agree to TP-Link's Terms of Use.

d. Click Next.

3. Choose how would you like to set up your new controller. You can configure a new setup or restore from backup file.

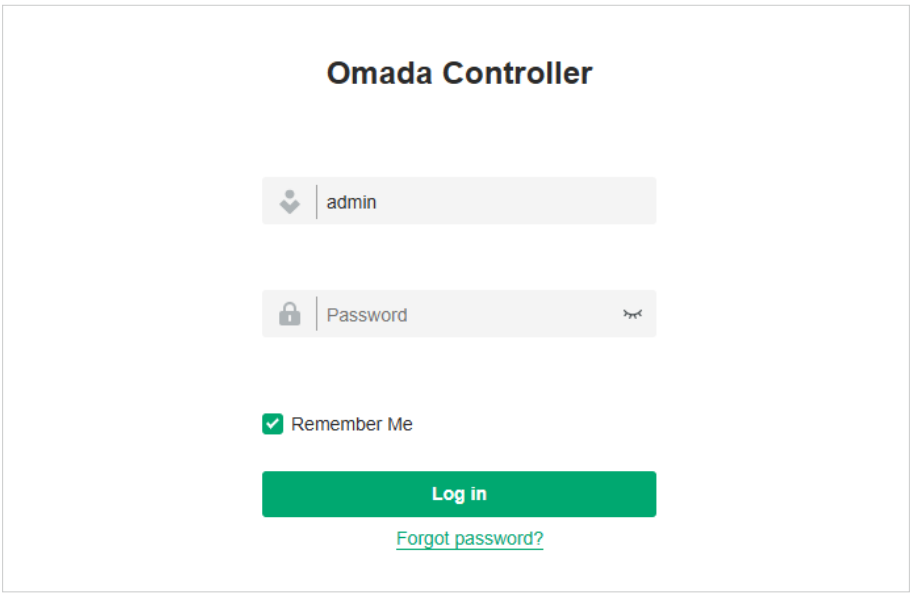


4. Follow the setup wizard to set up the controller.



Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.



Note:

In addition to the Controller Host, other hosts in the same LAN can also manage EAPs via remote access to the Controller Host. For example, if the IP address of the Controller Host is 192.168.0.100 and the Controller is running normally on this host, you can enter https://192.168.0.100:8043, or http://192.168.0.100:8088 in the web browser of other hosts in the same LAN to log in to the Controller and manage EAPs. Or you can log in to the Controller using other management devices through Cloud service.

2. 3 Set Up Your Integrated Gateway (Controller)

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up the Integrated Gateway (Controller):

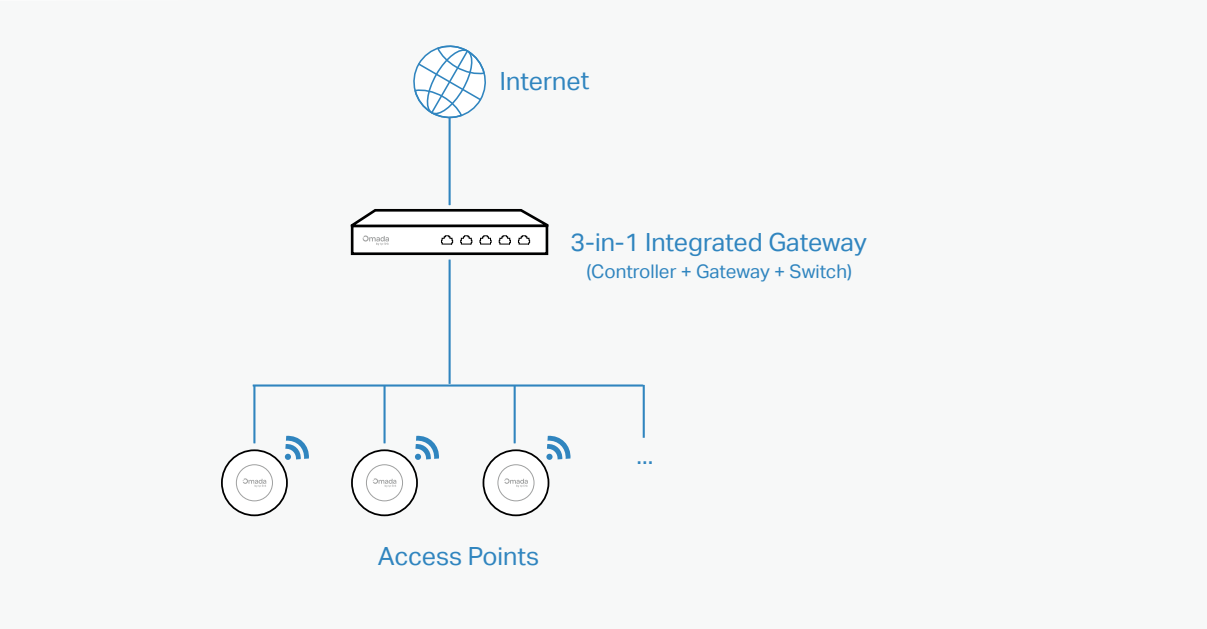
1) Determine the network topology.

2) Deploy the Integrated Gateway (Controller).

3) Start and log in to the controller.

2. 3. 1 Determine the Network Topology

The network topology that you create for the SDN Controller varies depending on your business requirements. The following figure shows a typical topology for a high-availability use case.



Note:

When using the Omada SDN Controller, we recommend that you deploy the full topology with Omada-supported TP-Link devices. If you use third-party devices, Omada SDN Controller cannot discover and manage them.

2. 3. 2 Deploy the Integrated Gateway (Controller)

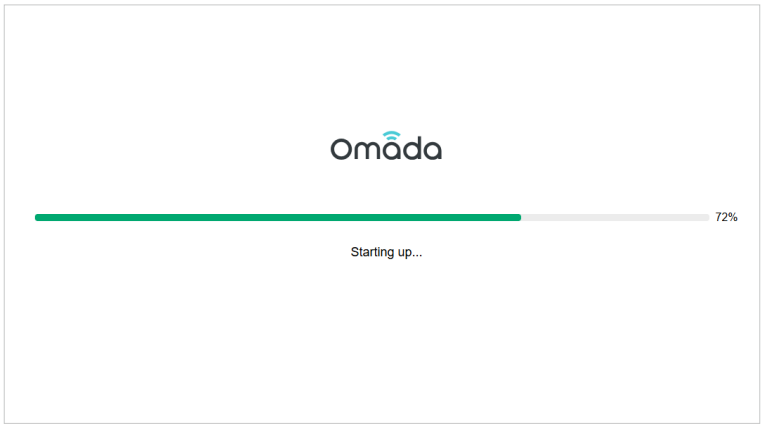
Omada Integrated Gateway (Controller) comes with the pre-installed controller software, so installation is not necessary. After deploying the Integrated Gateway (Controller) on your network infrastructure, proceed to configure the controller.

2. 3. 3 Start and Log in to the Controller

Log In to the Management Interface

Follow the steps below to enter the management interface of the Integrated Gateway (Controller):

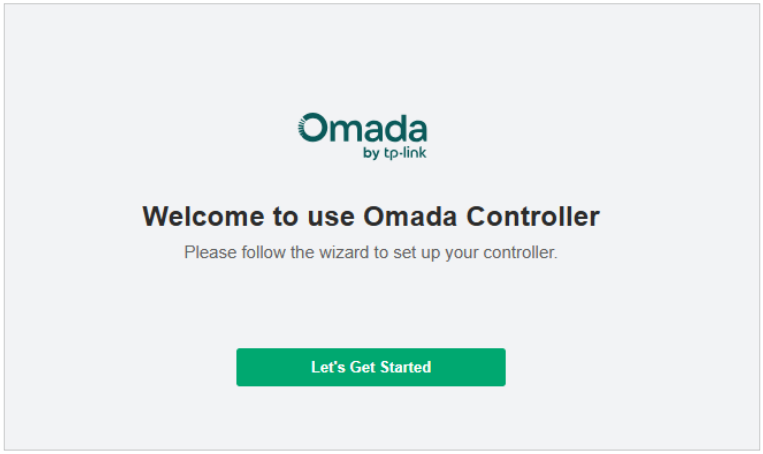
1. Connect a computer to a LAN port of the Integrated Gateway (Controller) with an RJ45 port properly. If your computer is configured with a fixed IP address, change it to obtain an IP address automatically.
2. Launch a web browser and type the default management address 192.168.0.1 in the address bar, then press **Enter** (Windows) or **Return** (Mac). The management interface will start up.



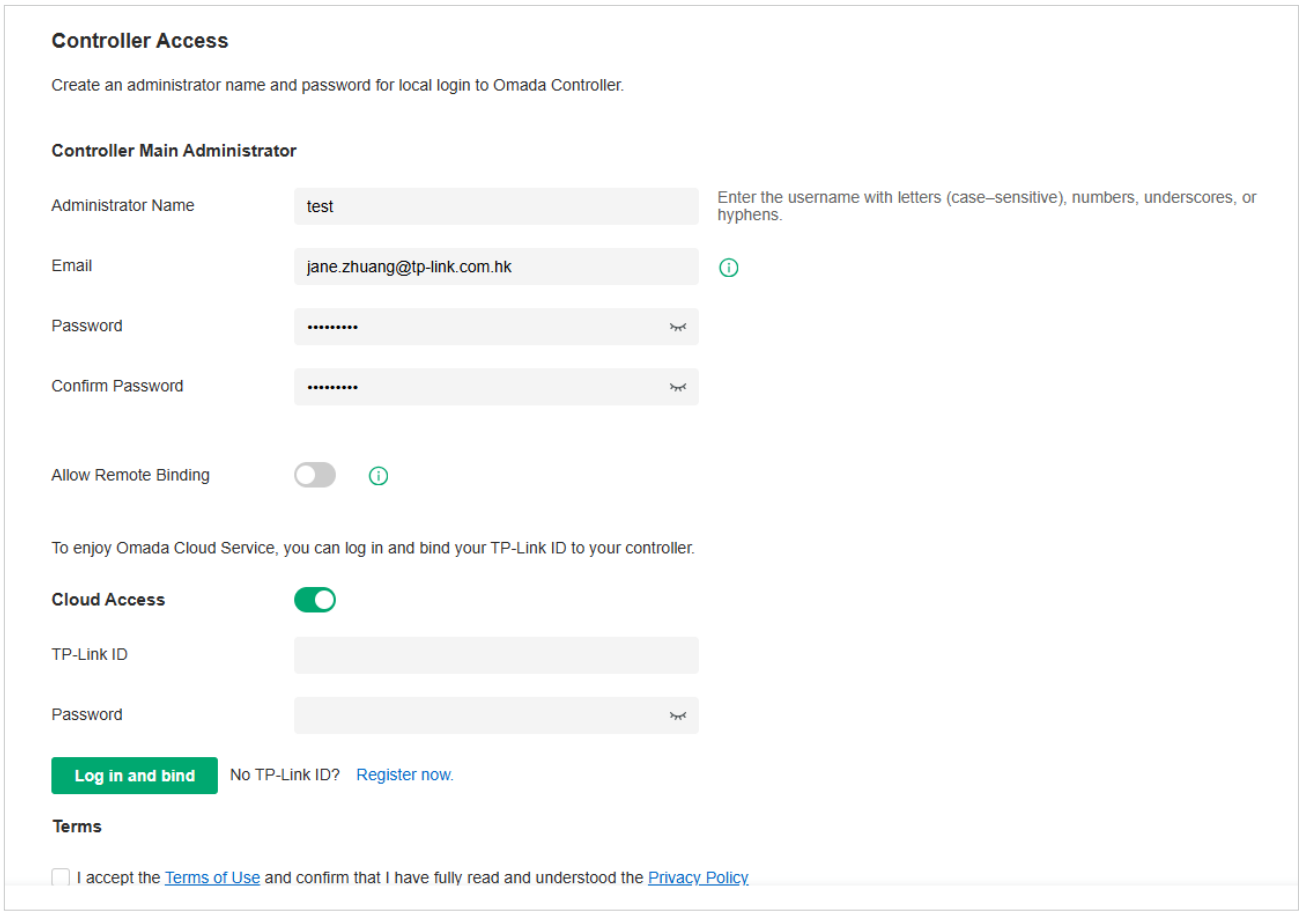
Complete Basic Configurations

In the web browser, you can see the configuration page. Follow the setup wizard to complete the basic settings for the Controller.

1. Click Let's Get Started.



2. Set up controller access settings.



a. Create an Administrator username and password for login to the controller. Specify the email address for resetting your password in case that you forget the password. After logging into the Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to 8. 6. 3 Notifications.

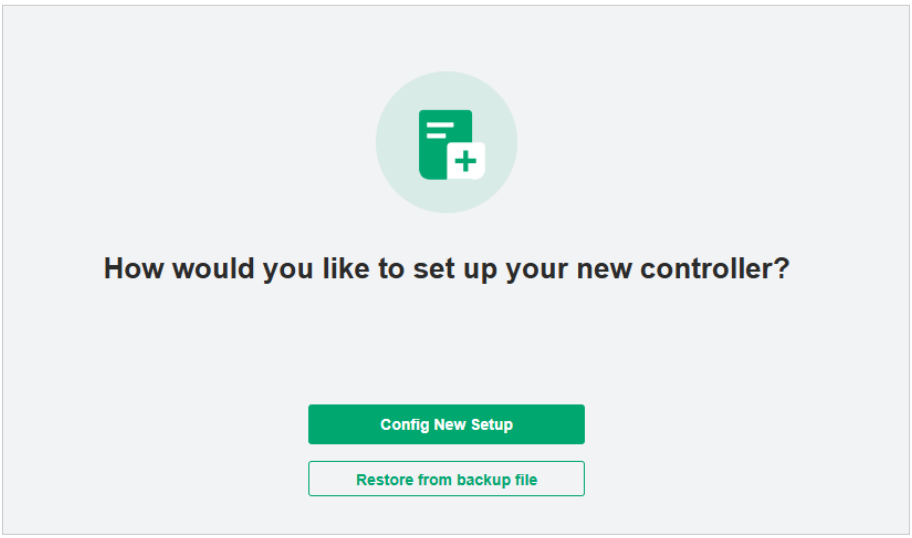
b. If you want to allow the device to connect to the cloud portal remotely, enable Allow Remote Binding.

c. If you want to access the controller to manage networks remotely, enable Cloud Access, and bind your TP-Link ID to your Controller. For more details about cloud access, please refer to 5. 10 Cloud Access.

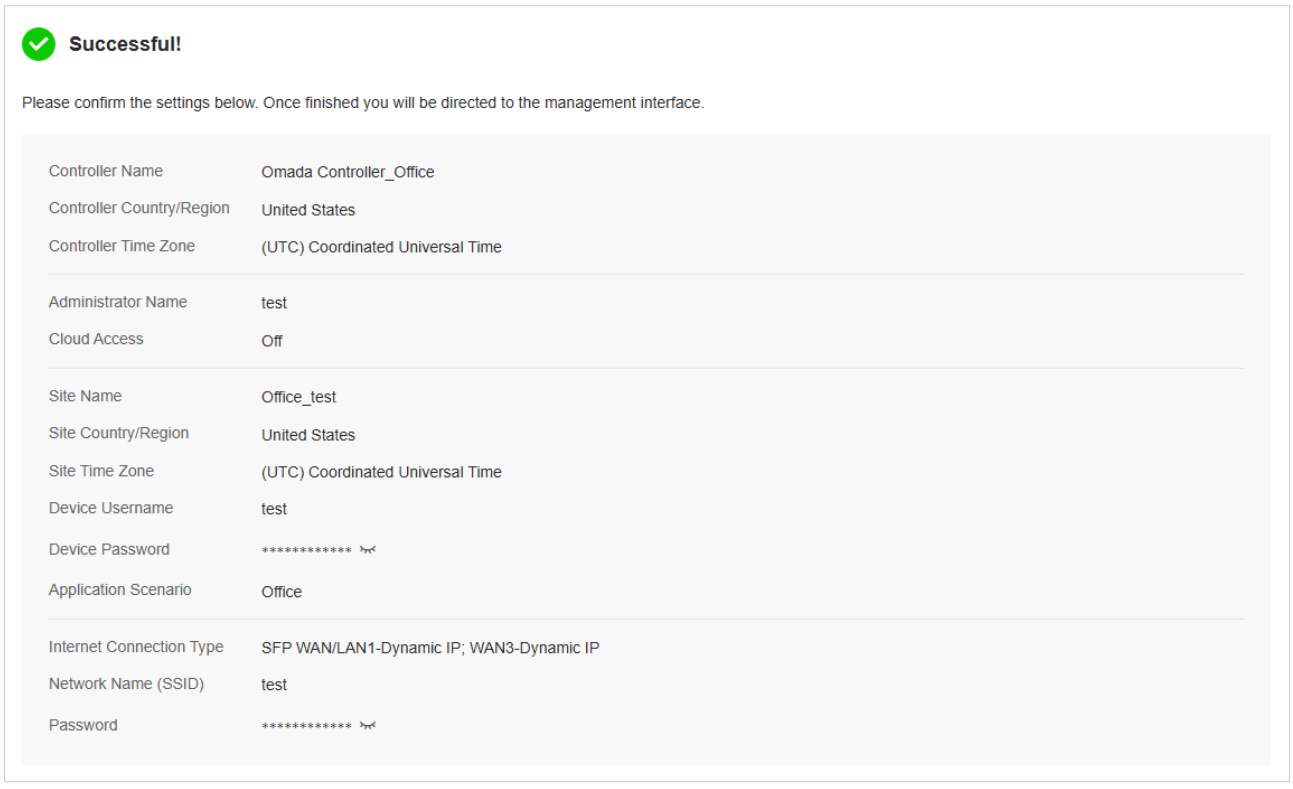
d. Read and agree to TP-Link's Terms of Use.

e. Click Next.

3. Choose how would you like to set up your new controller. You can configure a new setup or restore from backup file.

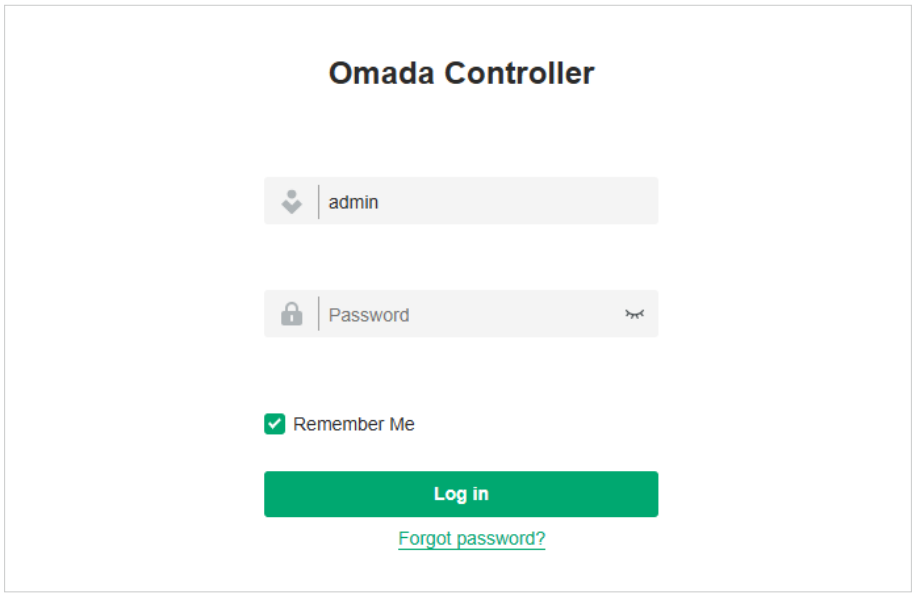


4. Follow the setup wizard to set up the controller. The integrated gateway will be adopted by the build-in controller by default.



Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.


Omada Controller
admin
Password
Remember Me
Log in
Forgot password?

2. 4 Set Up Your Cloud-Based Controller

The CBC solution offers the Essentials version for easy and free management of essential features, and the Standard version for basic and advanced features through subscription-based licensing.

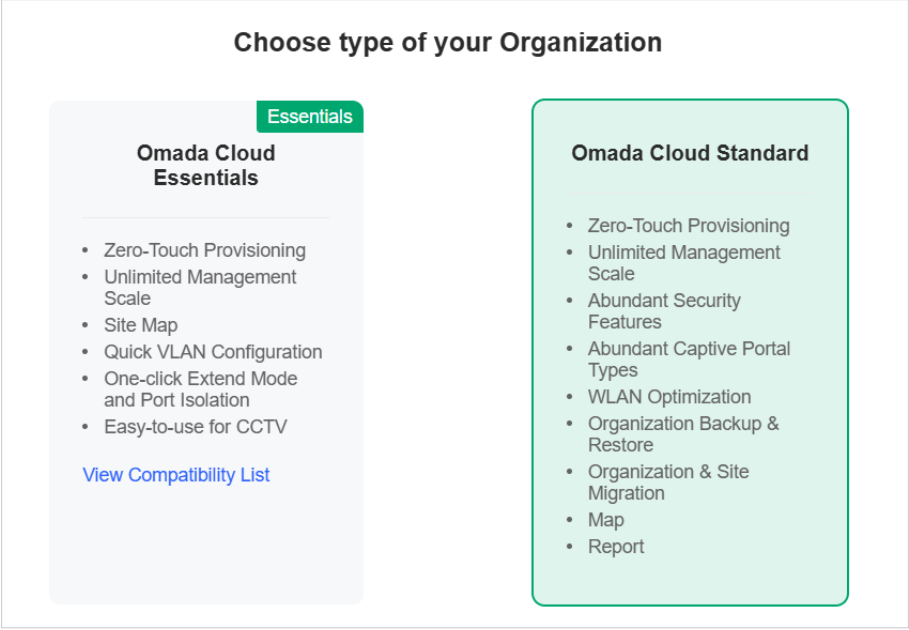
View the compatible device list below to see if your devices can be centrally managed by the Omada Cloud-Based Controller:

Essentials version: https://www.omadanetworks.com/omada-cloud-essentials/product-list/

Standard version: https://www.omadanetworks.com/omada-cloud-based-controller/product-list/

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up the Cloud-Based Controller:

1. Launch a web browser and enter https://omada.tplinkcloud.com in the address bar. Enter your TP-Link ID and password to log in. If you do not have a TP-Link ID, create a TP-Link ID first.
2. On the Cloud-Based Systems page, click Add Organization and choose the type of your organization.
   - Omada Cloud Essentials: for easy and free management of essential features.
   - Omada Cloud Standard: for basic and advanced features through subscription-based licensing.



3. Follow the instructions to complete the setup process.
4. Add devices with the serial number, make sure the devices are online and in factory default.
5. If you use the Omada Cloud Standard, assign appropriate licenses to manage and configure the devices on the cloud-based controller.

   For detailed information about device-based licensing, refer to https://www.omadanetworks.com/sg/omada-sdn/license/.

Chapter 3

Get Started with Your Network on Omada SDN Controller

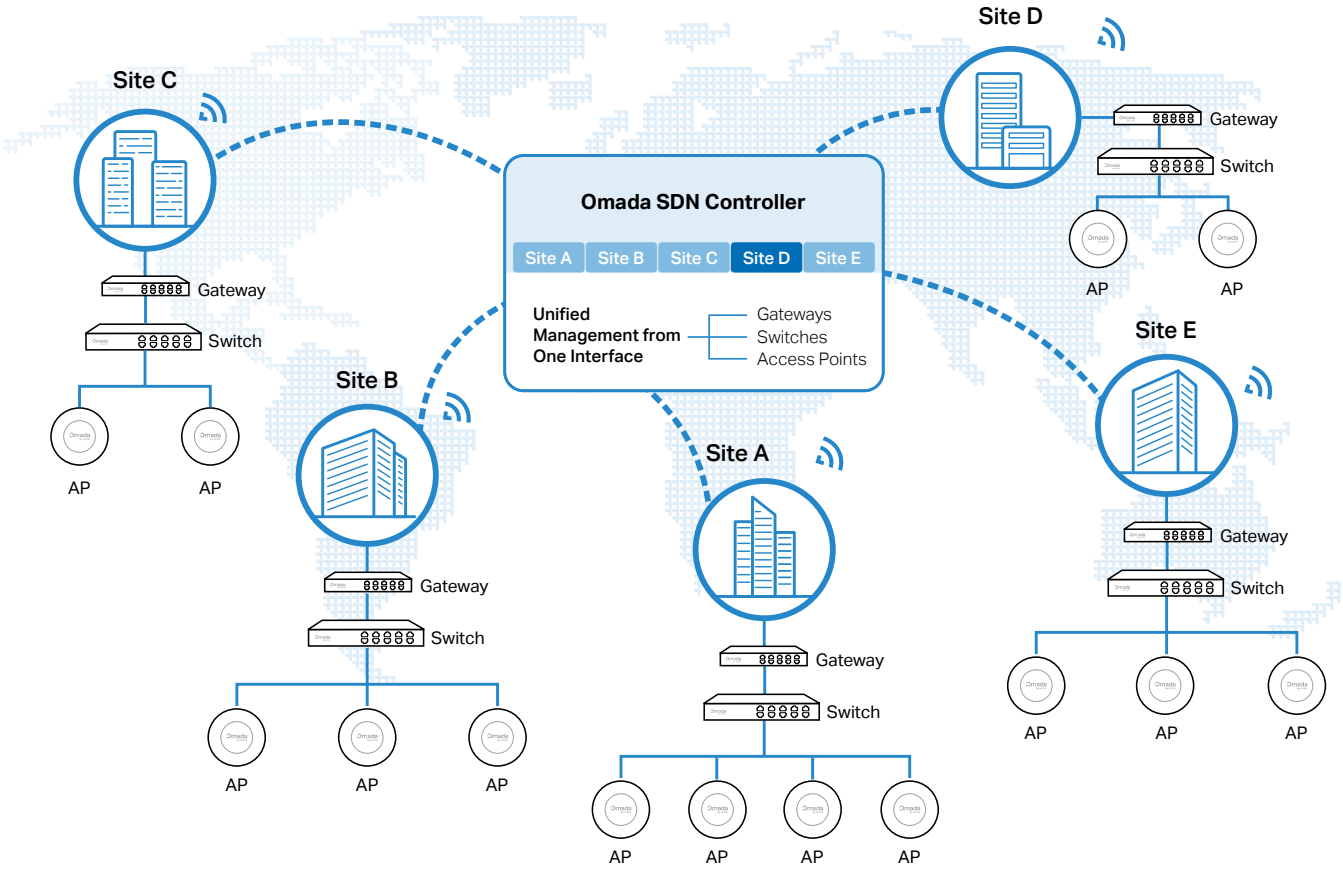
Get started with your network on Omada SDN Controller by creating sites and adopting devices so that you can configure and monitor your devices centrally while keeping things organized. Familiarize yourself with the Controller UI before configuring and monitoring your network and devices. The chapter includes the following sections:

- 3. 1 Create Sites
- 3. 2 Configure the Site Template
- 3. 3 Adopt Devices
- 3. 4 Navigate the Controller UI

3. 1 Create Sites

Overview

Different sites are logically separated network locations, like different subsidiary companies or departments. It's best practice to create one site for each LAN (Local Area Network) and add all the devices within the network to the site, including the router, switches and APs.



Devices at one site need unified configurations, whereas those at different sites are not relative. To make the best of a site, configure features simultaneously for multiple devices at the site, such as VLAN and PoE Schedule for switches, and SSID and WLAN Schedule for APs, rather than set them up one by one.

Configuration

To create and manage a site, follow these steps:

1) Create a site.

2) View and edit the site.

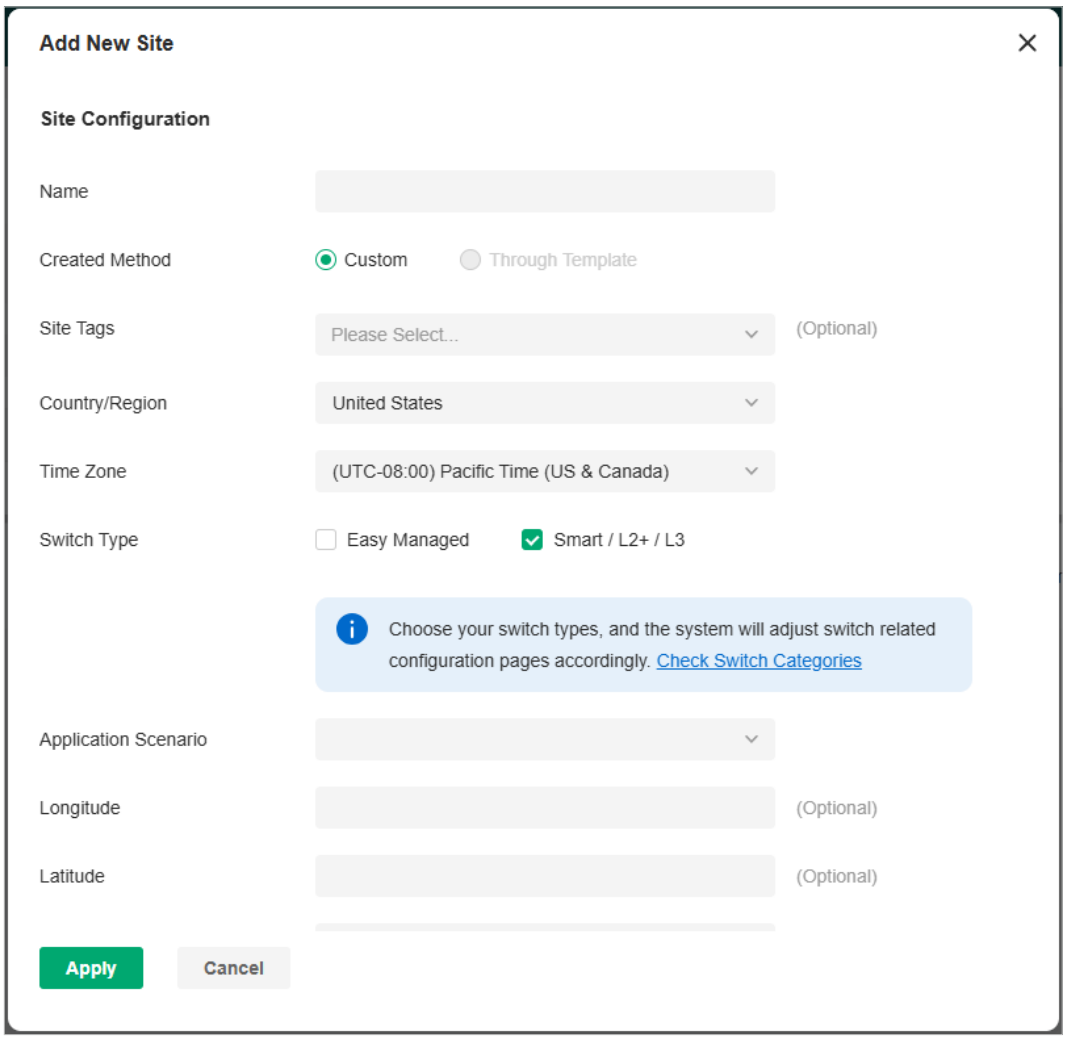
3) Access the site.

Step 1: Create a Site

To create a site, choose one from the following methods according to your needs.

- **Create a site from scratch**

  1. Launch the controller and access the Global View.
  2. Go to Dashboard > Site List and click Add New Site.



  3. Enter a Site Name to identify the site, and configure other parameters according to actual site needs and location.
  4. Create a device username and password for login to newly adopted devices.
  5. Click Apply. The new site will be added to the Site List.

- **Copy an existing site**

  You can quickly create a site based on an existing one by copying its site configuration, wired configuration, and wireless configuration among others. After that, you can flexibly modify the new site configuration to make it different from the old.

1. In the Site List, click the Copy icon in the ACTION column of the site which you want to copy.

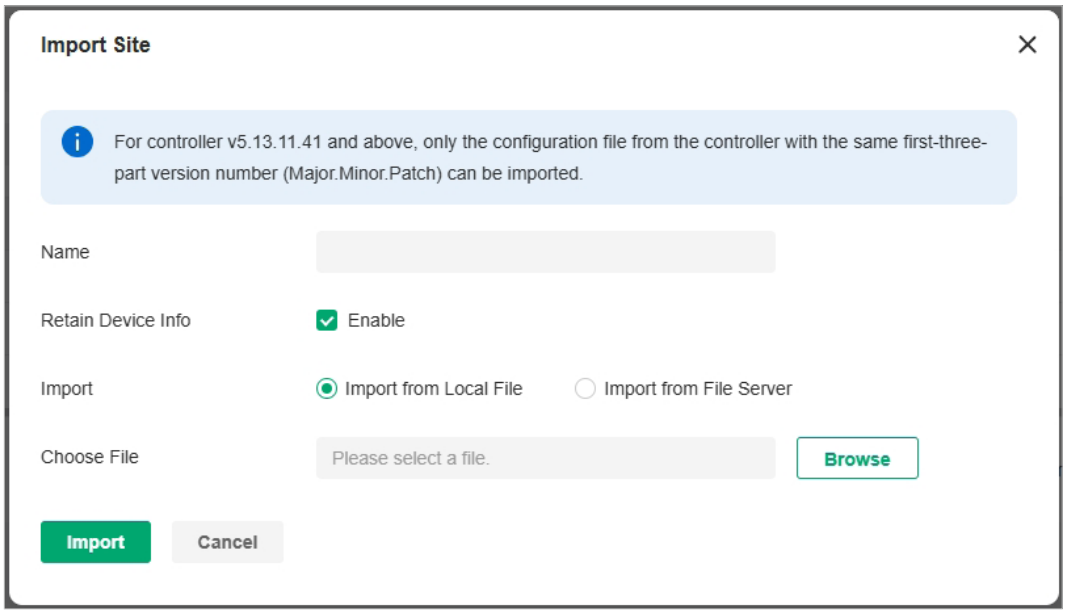


2. Enter a Site Name to identify the new site.
3. Click Apply. The new site will be added to the Site List.

- **Import a site from another controller**

  If you want to migrate seamlessly from an old controller to a new one, import the site configuration file of the old controller into the new. Before that, you need to export the site configuration file from the old controller, which is covered in 5. 8. 1 Site Migration.

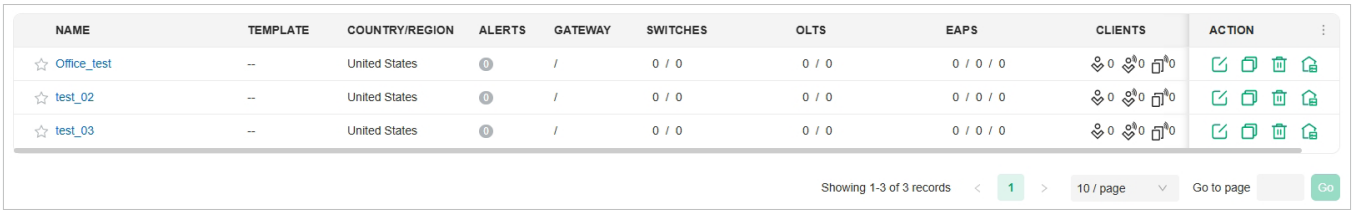
1. In the Site List, click the Import Site icon.



2. Enter a Site Name to identify the site, and configure other parameters according to actual site needs.
3. Browse your file explorer and choose a site configuration file.
4. Click Import Site. The new site will be added to the Site List.

Step 2: View and Edit the Site

After you create the site, you can view the site status in the Site List. You can click the icons in the ACTION column to edit, copy, delete and launch the site.



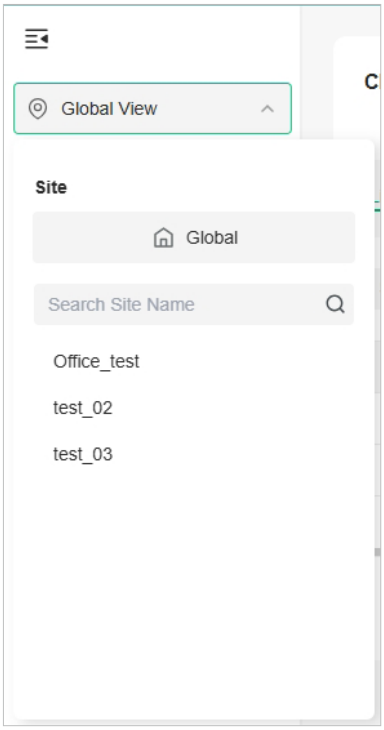
Step 3: Access the Site

To monitor and configure a site, you need first access the site.

Click the Launch icon in the ACTION column of the site to access the site.



Alternatively, select the site from the Global/Site View drop-down list in the left of the page.



Note:

Configuration items in Global View will be applied to the whole system while configuration items in Site View will be applied to the site which you are currently in.

3. 2 Configure the Site Template

Overview

The Site Template feature is implemented at the Controller's Global View to facilitate users to configure and manage sites in bulk. Most of the site's functions are supported to be set up in the Site Templates, such as Internet/LAN/WLAN/ACL/URL Filtering/Portal/MAC Authentication, etc. By binding each site to a different template, you can quickly and easily realize the batch configuration of a large number of sites. For example, if a Controller manages several different sites and needs to make bulk configuration changes for them for business changes or other reasons, you can create Site Templates ahead of time and then apply the target Site Templates directly to the sites to be changed without having to go into each site individually to make adjustments to them. The greater the number of sites, the more the feature will work.

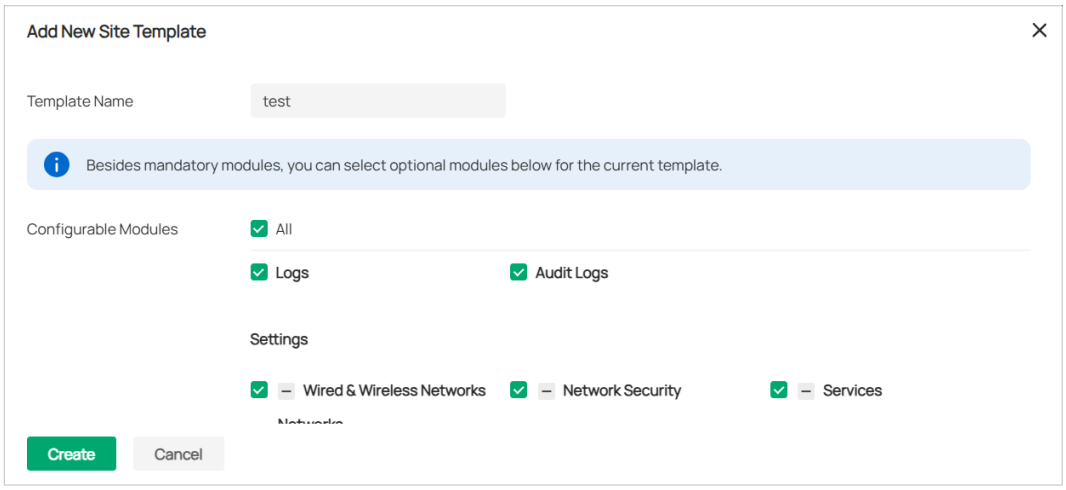
In addition, you can also create Device Template in Site template, then choose to bind the devices with the same model to the related Device template after binding them to Site template, which greatly improves the efficiency of managing and configuring devices. For instance, a large number of SG3452XP v2.20 are deployed on the same site, but the configurations are not exactly the same, in this case, it's possible to create a Device Template for each configuration, i.e. to set up different Ports/VLAN interface/Static Route/Service settings, and then apply each Device Template to the required devices.

Configuration

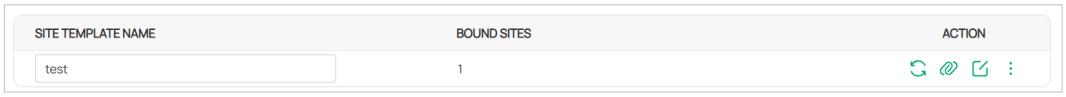
1. Launch the controller and access the Global View.
2. Go to the Site Template page. Click Add New Site Template. Name the template and select the configurable modules according to your needs.

Note:

- Most of the site's Configurable Modules are supported to be set up in the Site Template, some of them are mandatory and some are optional (you can set them up only if they are selected here). Please refer to https://www.omadanetworks.com/support/faq/4341 to know all modules supported in Site Template feature in detail.
- After the Site Template is created, its configurable modules cannot be changed.

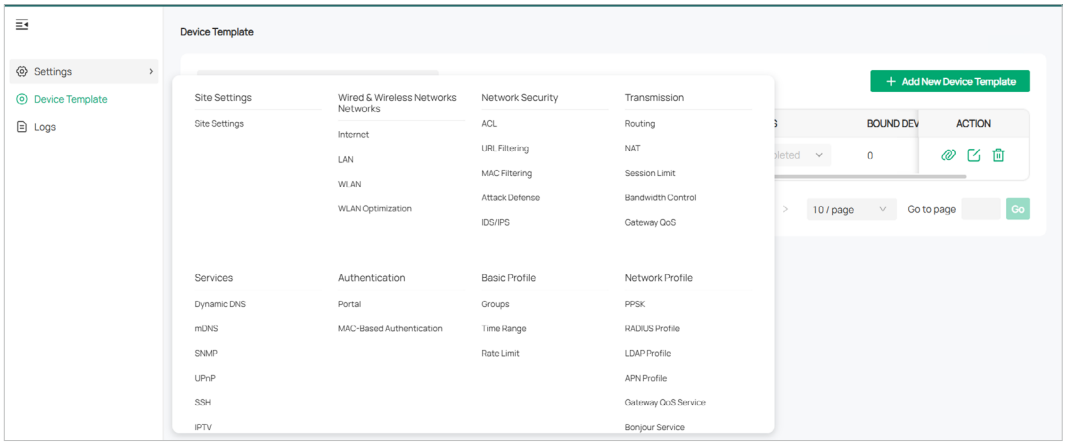


3. Click Create. The created site template will be displayed.

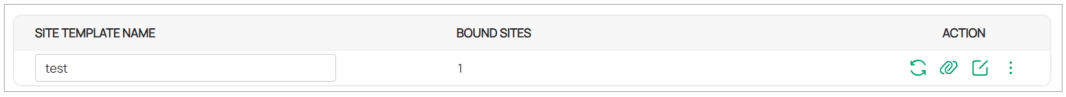


4. Click the edit icon in the Action column of the created site template, set up the site setting, device template, and log settings according to site needs.

Note: For configuration of the function modules, refer to the related chapters in this guide.

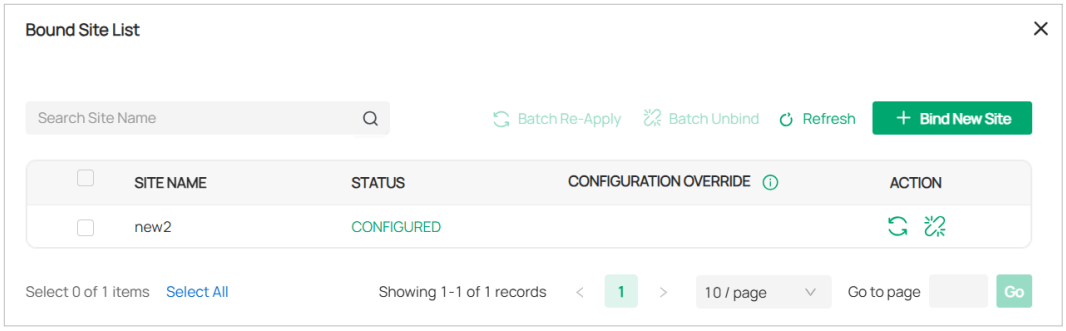


Save the settings to go back to the template list.



5. Click the Bound Site List icon in the Action column of the template, and click Bind New Site to bind the template to your desired sites. The template's configuration will be synchronized to the bound sites.

You can also click the Re-Apply icon to re-apply template settings to a site or click the Unbind icon to unbind the template from the site.

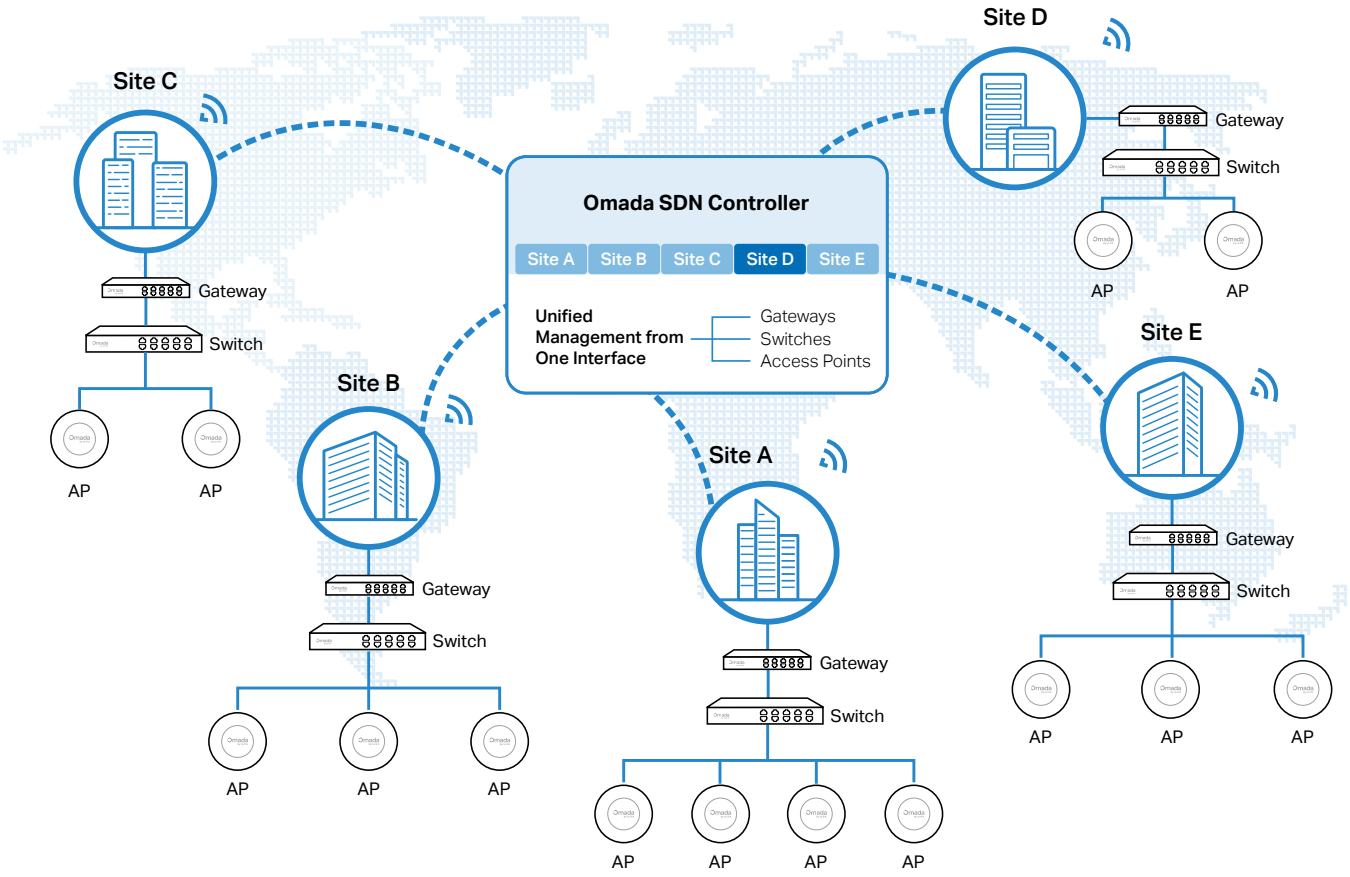


For more configuration instructions about the site template and device template, refer to https://www.omadanetworks.com/support/faq/4341.

3. 3 Adopt Devices

Overview

After you create a site, add your devices to the site by making the controller adopt them. Make sure that your devices in each LAN are added to the corresponding site so that they can be managed centrally.



Configuration

Choose a procedure according to the type of your controller:

- 3. 3. 1 For Software Controller / Hardware Controller
- 3. 3. 2 For Integrated Gateway (Controller)
- 3. 3. 3 For Cloud-Based Controller

3. 3. 1 For Software Controller / Hardware Controller

To adopt the devices on the controller, follow these steps:

1) Prepare for communication between the controller and devices.

2) Prepare for device discovery.

3) Adopt the devices.

Step 1: Prepare for Communication

Note:

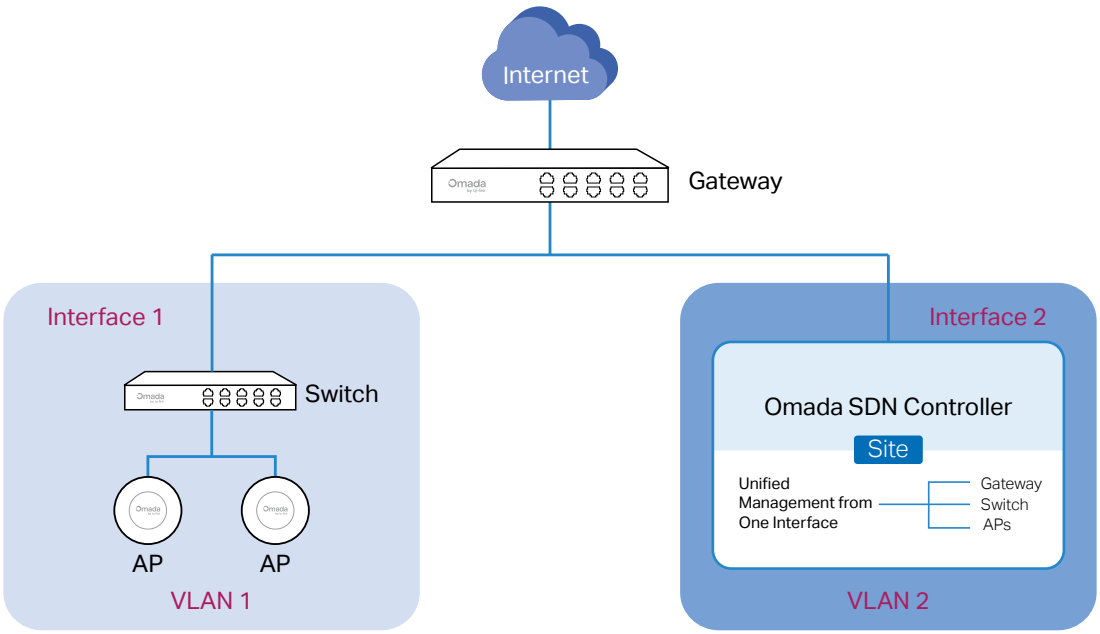
If the controller and devices are in the same LAN, subnet and VLAN, skip this step.

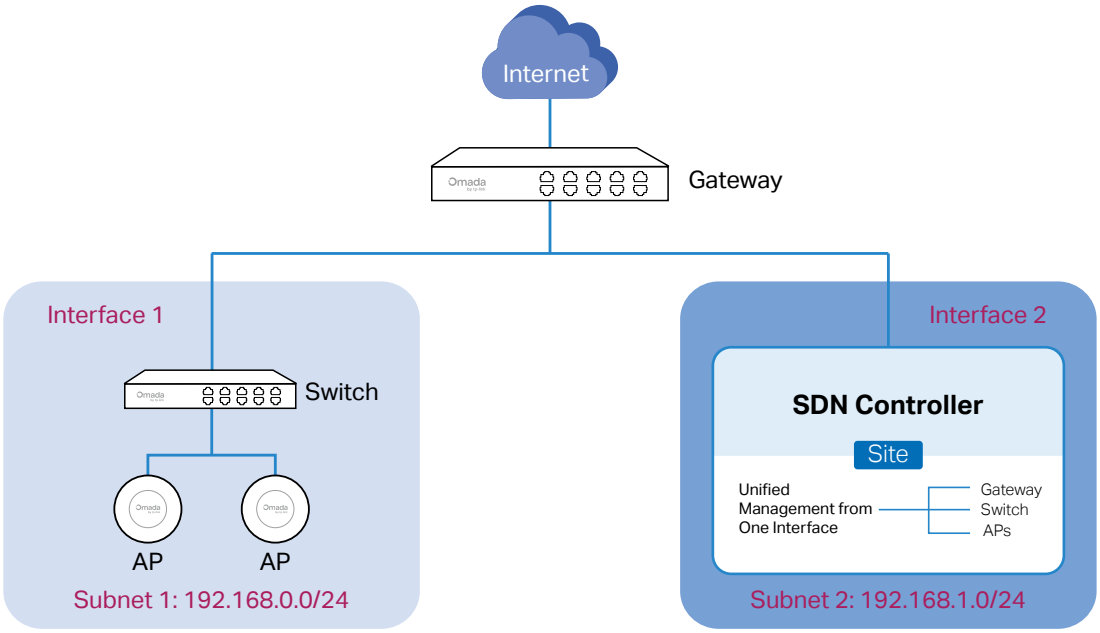
Make sure that the controller can communicate with the devices. Otherwise, the controller cannot discover or adopt the devices by any means. If the controller and devices are in different LANs, subnets or VLANs, use the following techniques to build up the connection according to your scenario.

1. Set up the Network

■ **Scenario 1: Across VLANs or Subnets**

If the controller and devices are in different VLANs or subnets, you need to set up a layer 3 interface for each VLAN or subnet, and make sure the interfaces can communicate with each other.





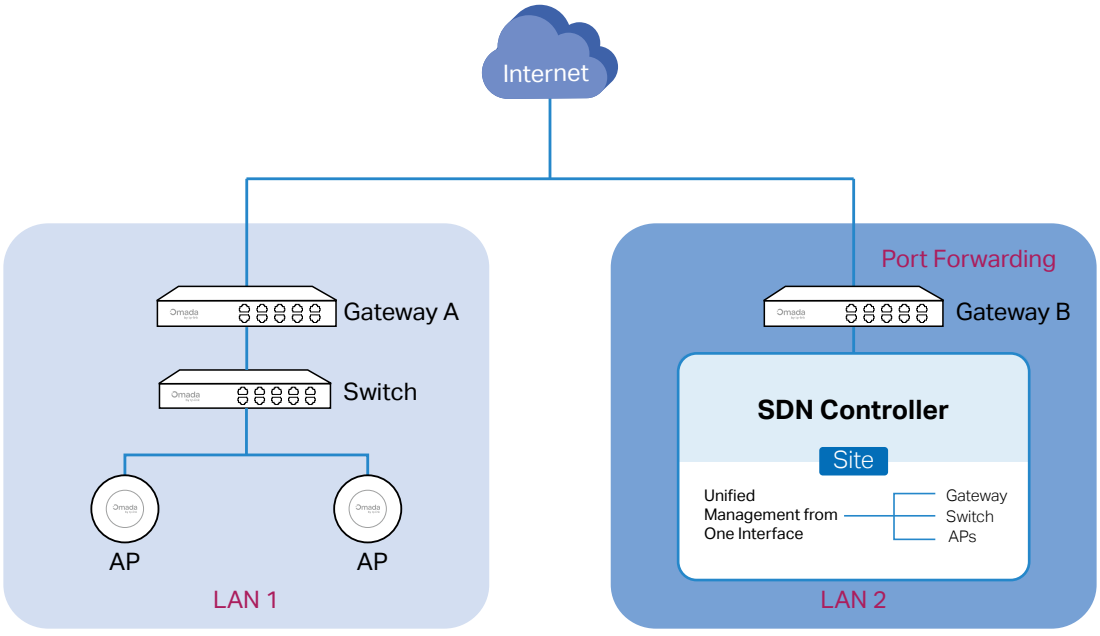
- **Scenario 2: Across LANs**

  If the controller and devices are in different LANs, you need to establish communication across the internet and the gateways.

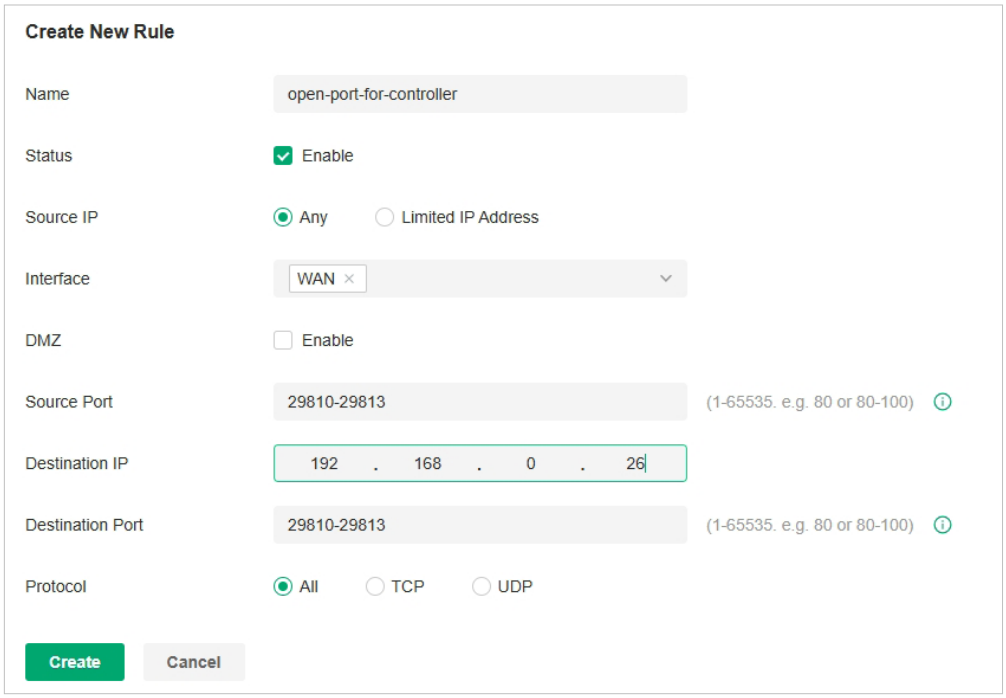
  By default, devices in LAN 1 cannot communicate with the controller in LAN 2, because Gateway B is in front of the controller and block access to it. To make the controller accessible to the devices, you can use Port Forwarding or VPN.

  - Use Port Forwarding

  Configure Port Forwarding on Gateway B and open port 29810-29813 for the controller, which are essential for discovering and adopting devices. If you are using firewalls in the networks, make sure that the firewalls don't block those ports.

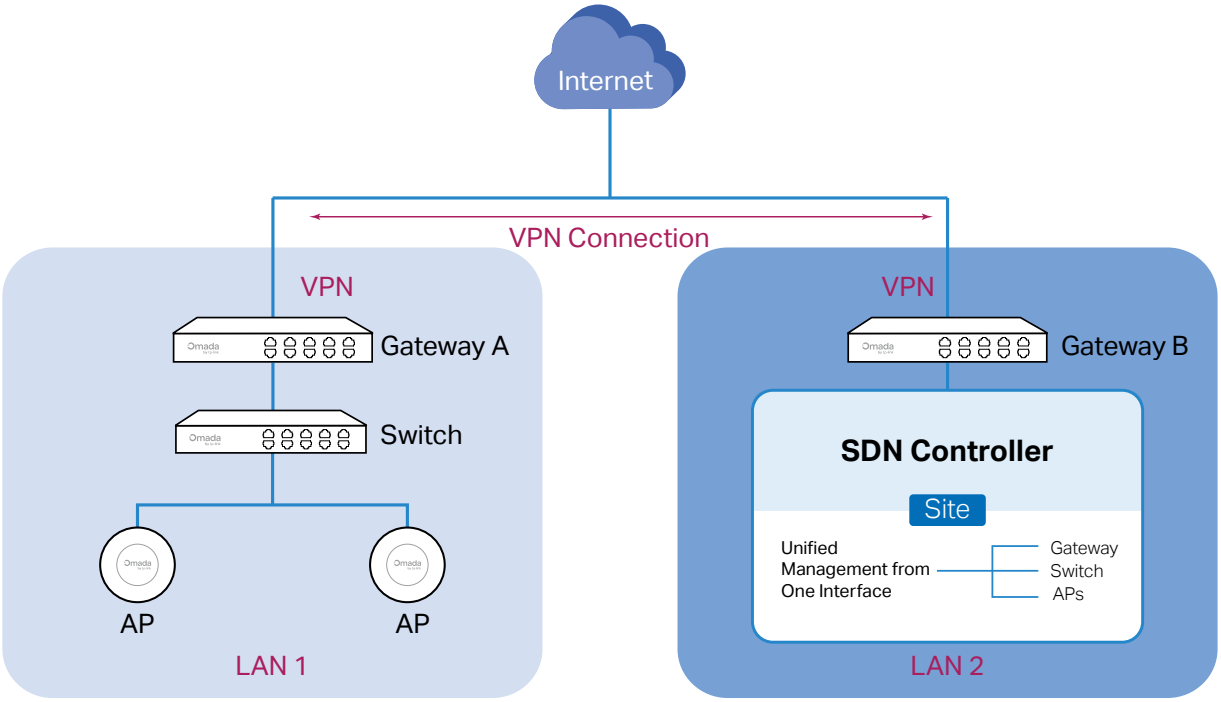


To configure Port Forwarding on Gateway B, you need first adopt Gateway B on the controller. Then go to Settings > Transmission > NAT > Port Forwarding. Click Create New Rule to load the following page. Specify a name to identify the Port Forwarding rule, check Enable for Status, select Any as Source IP, select the desired WAN port as Interface, disable DMZ, specify 29810-29813 as Source Port and Destination Port, specify the controller's IP address as Destination IP, and select All as Protocol. Then click Create.



- Use VPN

Set up a VPN connection between Gateway A and Gateway B in Standalone Mode. For details about VPN configuration, refer to the User Guide of the gateways.



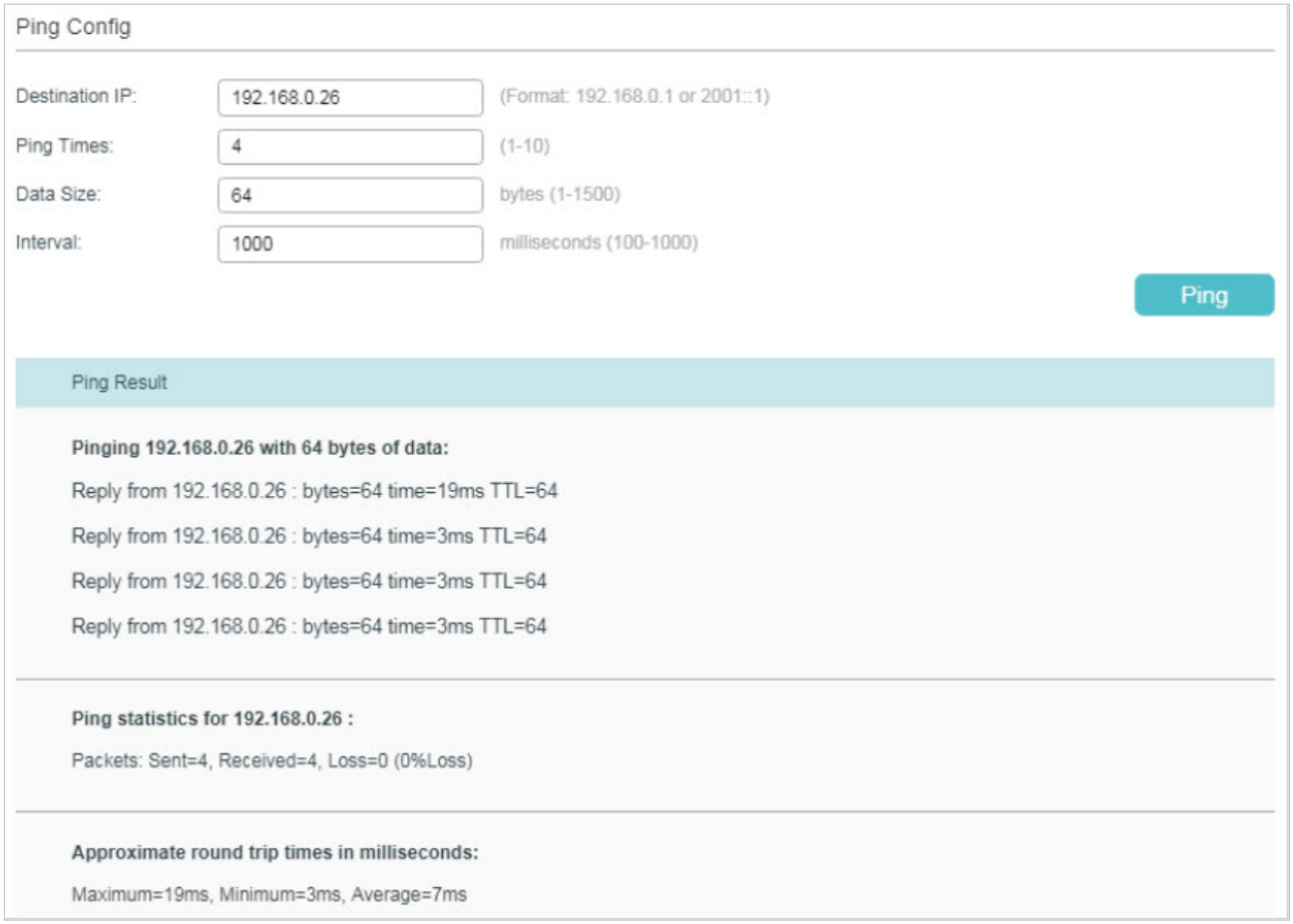
2. (Optional) Test the network

   If you are not sure whether the controller and devices can establish communication, it's recommended to do the ping test from the devices to the controller.

   Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Then Go to MAINTENANCE > Network Diagnostics > Ping to load the following page, and specify Destination IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click Ping.

Note:

To ping the router, please turn off Block WAN Ping on the **Settings > Network Security > Attack Defense** page.



   If the ping result shows the packets are received, it implies that the controller can communicate with the devices. Otherwise, the controller cannot communicate with the devices, then you need to check your network.

Step 2: Prepare for Device Discovery

Note:

If the controller and devices are in the same LAN, subnet and VLAN, skip this step. In this scenario, the controller can discover the devices directly, and no additional settings are required.

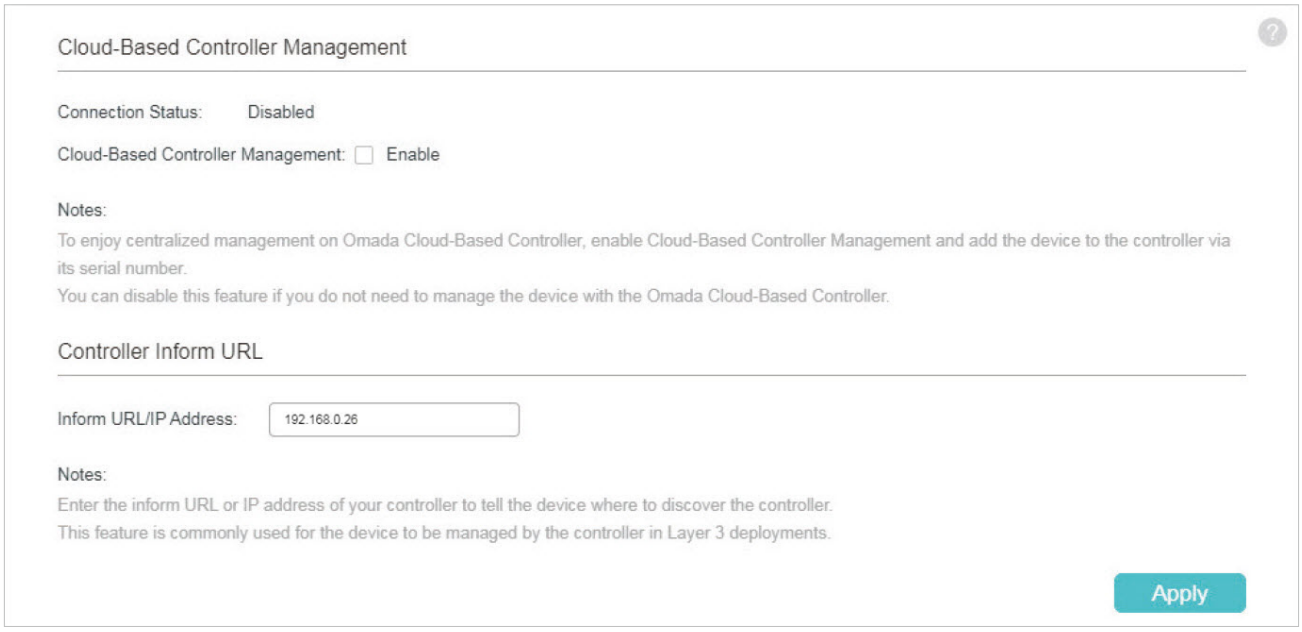
Make sure that the controller can discover the devices.

When the controller and devices are in different LANs, subnets or VLANs, the controller cannot discover the devices directly. You need to choose Controller Inform URL, Discovery Utility, or DHCP Option 138 as the method to help the controller discover the devices.

- **Controller Inform URL**

  Controller Inform URL informs the devices of the controller's URL or IP address. Then the devices make contact with the controller so that the controller can discover the devices.

  You can configure Controller Inform URL for devices in Standalone Mode. Let's take a switch for example. Log into the management page of the switch in Standalone Mode and go to SYSTEM > Controller Settings to load the following page. In Controller Inform URL, specify Inform URL/IP Address as the controller's URL or IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click Apply.

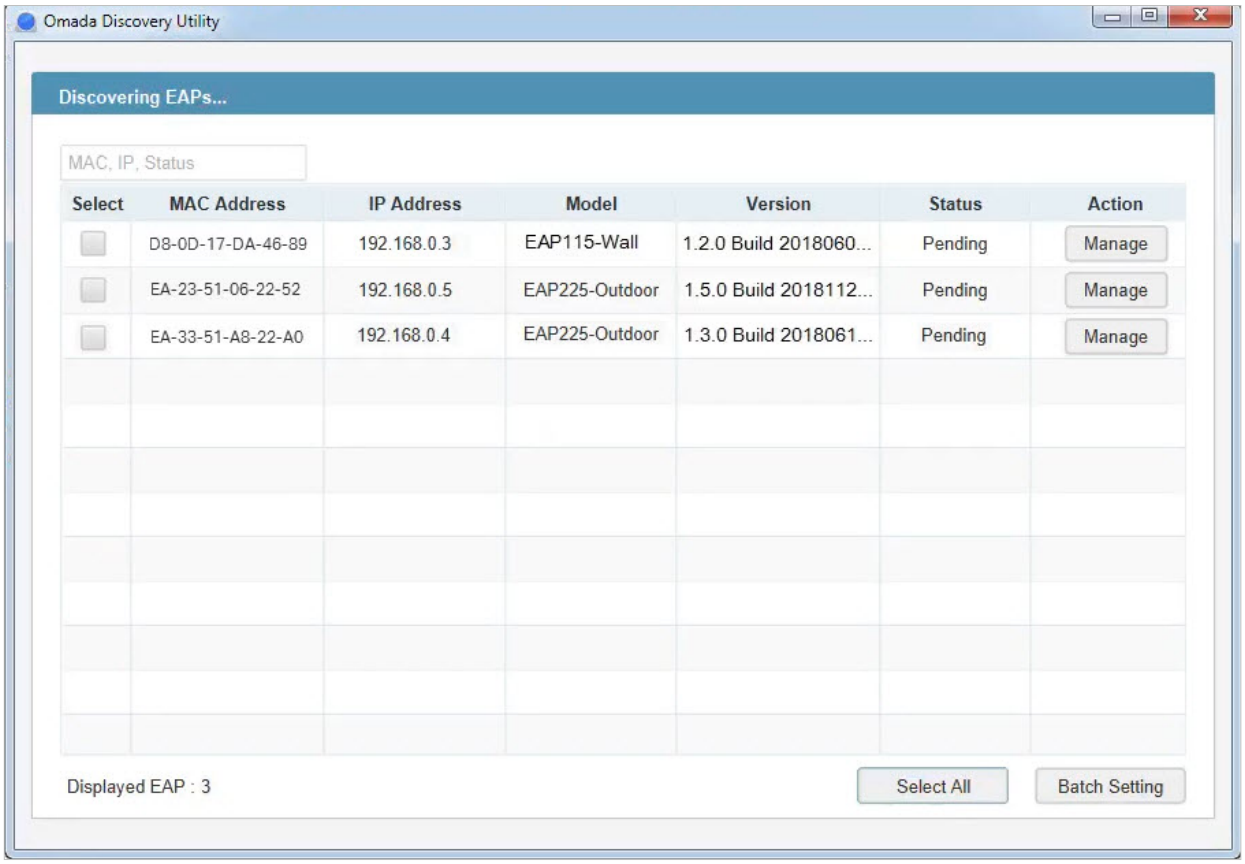


- **Discovery Utility**

  Discovery Utility can discover the devices in the same LAN, subnet and VLAN, and inform the devices of the controller's IP address. Then the devices make contact with the controller so that the controller can discover the devices.

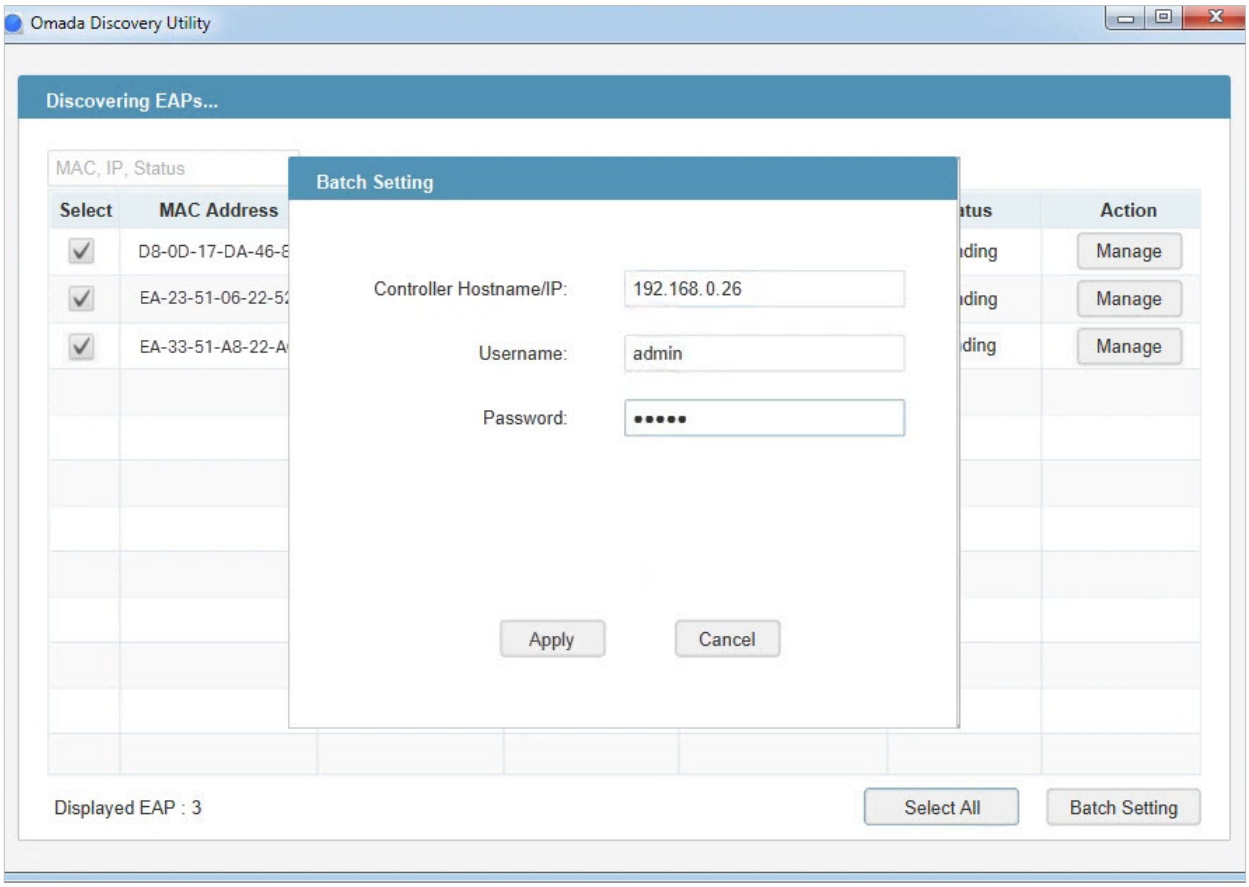
  1. Download Discovery Utility from https://support.omadanetworks.com/product/omada-software-controller/?resourceType=download and then install it on your PC which should be located in the same LAN, subnet and VLAN as your devices.

2. Open Discovery Utility and you can see a list of devices. Select the devices to be adopted and click Batch Setting.



3. Specify Controller Hostname/IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead), and

enter the username and password of the devices. By default, the username and password are both admin. Then click Apply. Wait until the setting succeeds.

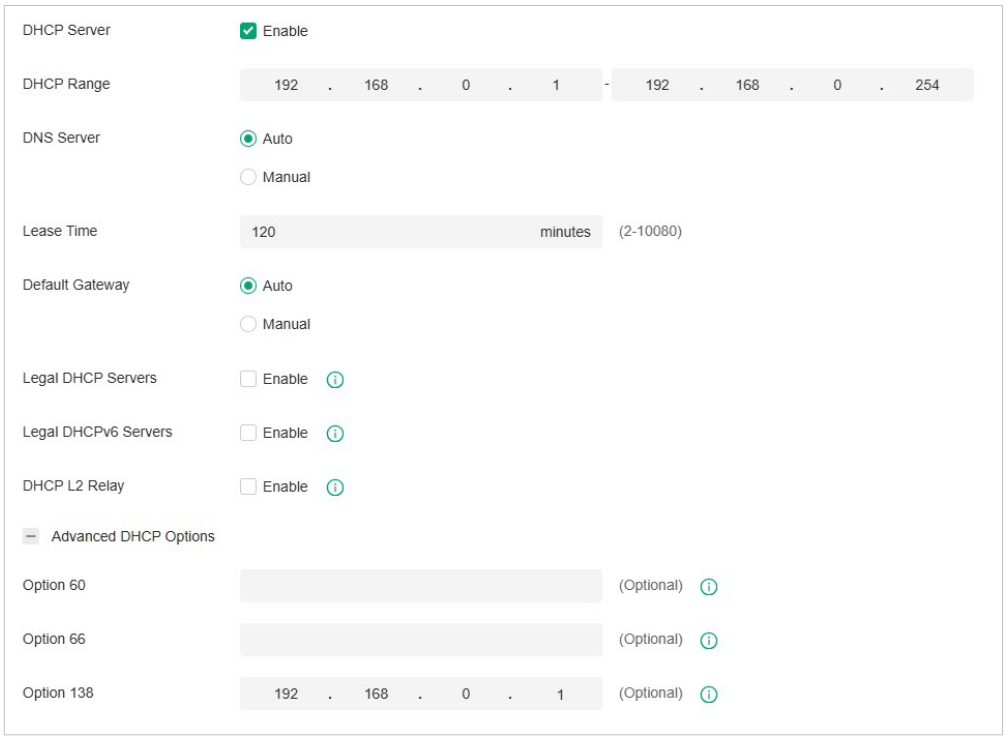


- **DHCP Option 138**

  DHCP Option 138 informs a DHCP client, such as a switch or an EAP, of the controller's IP address when the DHCP client sends DHCP requests to the DHCP server, which is typically a gateway.

  1. To use DHCP Option 138, you need to adopt the gateway on the controller first, which may require other techniques like Controller Inform URL or Discovery Utility if necessary.
  2. After the gateway is adopted, go to Settings > Wired&Wireless Networks > LAN > Networks, and click the Edit icon in the ACTION column of the LAN where the DHCP clients are located. Enable DHCP Server and configure common DHCP parameters. Then click Advanced DHCP Options

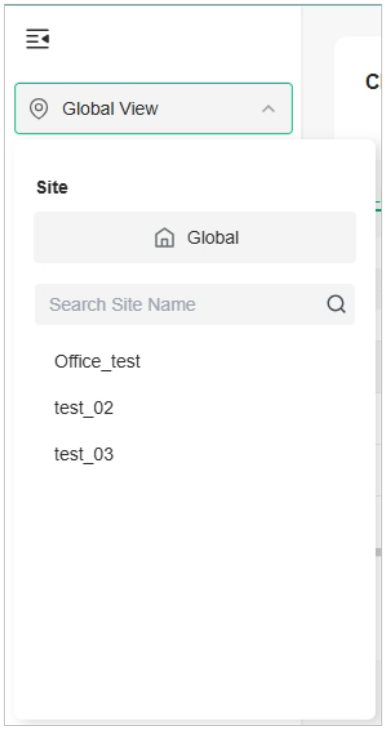
and specify Option 138 as the controller's IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Click Save.



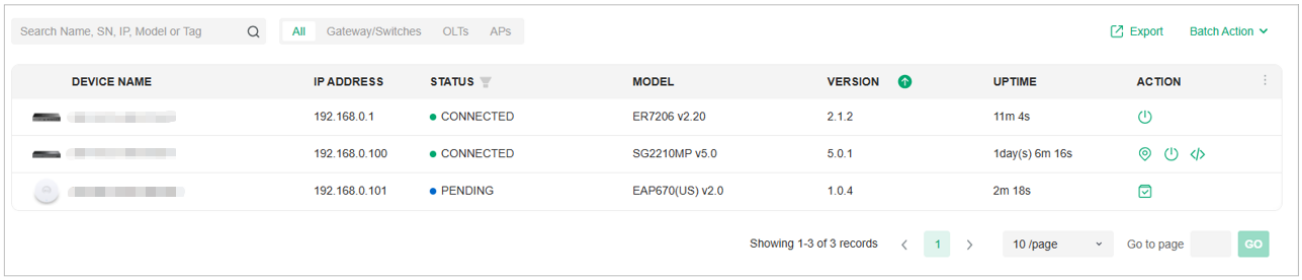
3. To make DHCP Option 138 take effect, you need to renew DHCP parameters for the DHCP clients. One possible way is to disconnect the DHCP clients and then reconnect them.

Step 3: Adopt the Devices

1. Launch the controller and access a site.

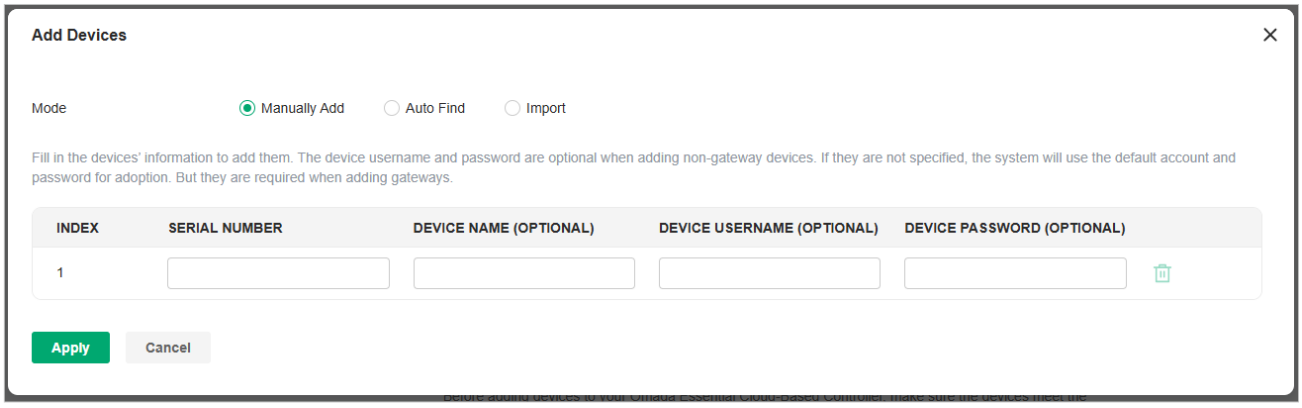


2. Go to Devices, and the devices which have been discovered by the controller are displayed.



Click the Adopt icon in the ACTION column of each pending device that you want to add to the site. Wait until the device status turns into CONNECTED. Then the devices are adopted by the controller and added to the current site. Once the devices are adopted, they are subject to central management in the site.

3. You can also add devices offline. Click Add Devices and choose a method to add your devices.



- **Manually Add**

Fill in the devices' information to add them. The device username and password are optional when adding non-gateway devices. If they are not specified, the system will use the default account and password for adoption. But they are required when adding gateways.

- **Auto Find**

Automatically find the Omada devices with Inform URL configured to add them.

- **Import**

Download the template and fill in your devices' information. Then import the file. Up to 1500 devices can be imported at a time.

3. 3. 2 For Integrated Gateway (Controller)

The integrated gateway has been adopted by the build-in Controller by default during the initial setup.

To adopt other devices on the build-in cntroller of the Integrated Gateway, follow these steps:

1) Prepare for communication between the controller and devices.

2) Prepare for device discovery.

3) Adopt the devices.

Step 1: Prepare for Communication

Note:

If the controller and devices are in the same LAN, subnet and VLAN, skip this step.

Make sure that the controller can communicate with the devices. Otherwise, the controller cannot discover or adopt the devices by any means. If the controller and devices are in different LANs, subnets or VLANs, use the following techniques to build up the connection according to your scenario.

1. Set up the Network

■ **Scenario 1: Across VLANs or Subnets**

If the controller and devices are in different VLANs or subnets. You need to set up a layer 3 interface for each VLAN or subnet, and make sure the interfaces can communicate with each other.

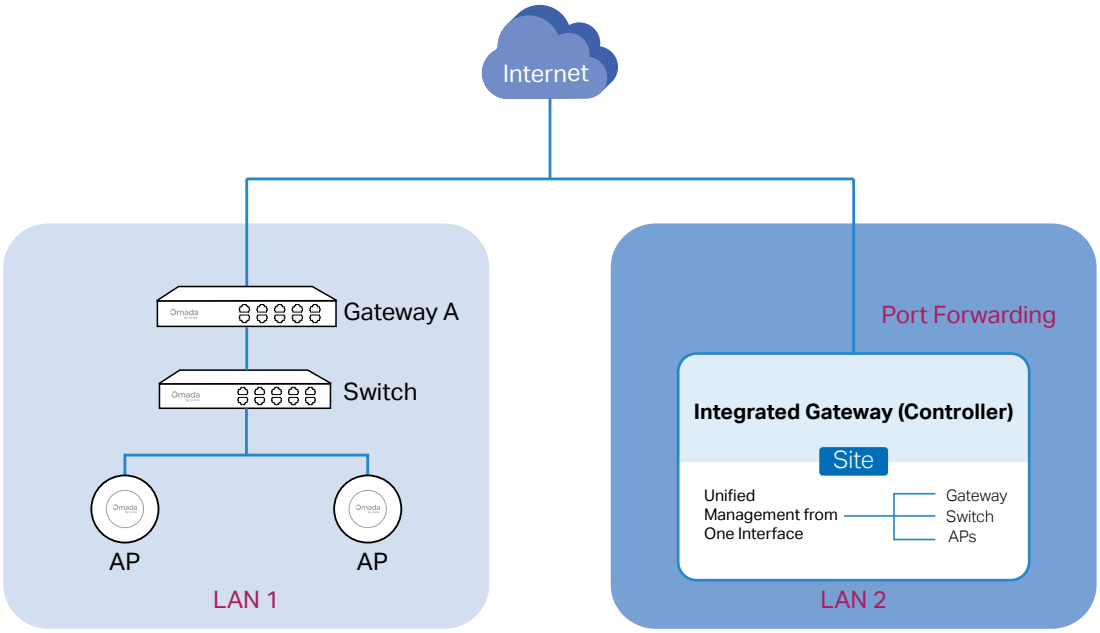
■ **Scenario 2: Across LANs**

As shown in the following figure, the controller and devices are in different LANs. You need to establish communication across the internet and the gateways.

By default, devices in LAN 1 cannot communicate with the controller in LAN 2, because Gateway A blocks their access to the controller. To make the controller accessible to the devices, you can use Port Forwarding or VPN.

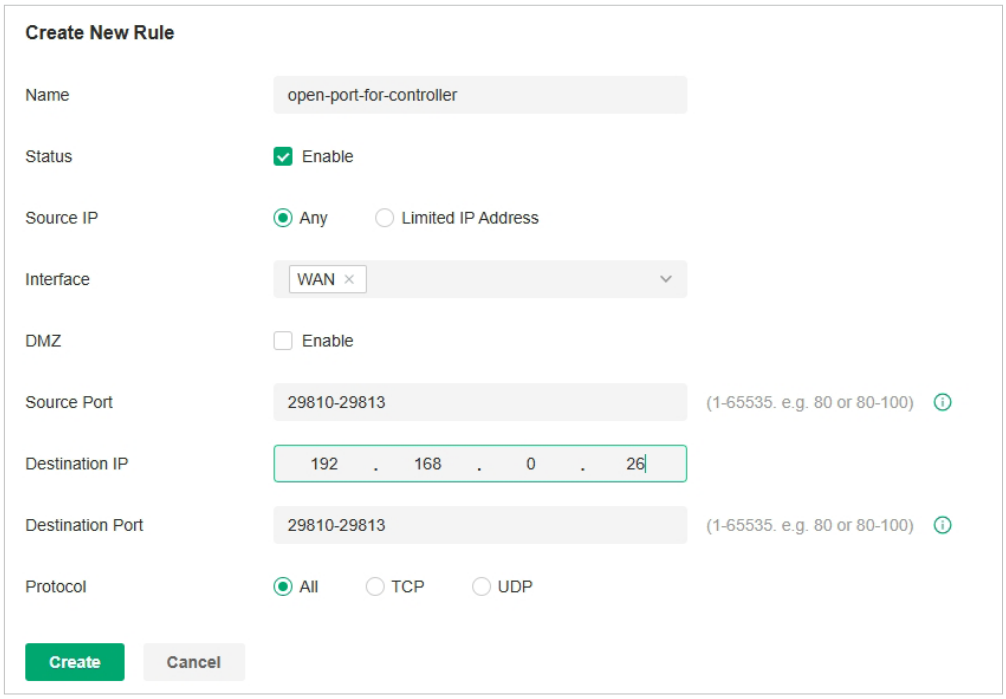
- Use Port Forwarding

Configure Port Forwarding on Gateway B and open port 29810-29814 for the controller, which are essential for discovering and adopting devices. If you are using firewalls in the networks, make sure that the firewalls don't block those ports.



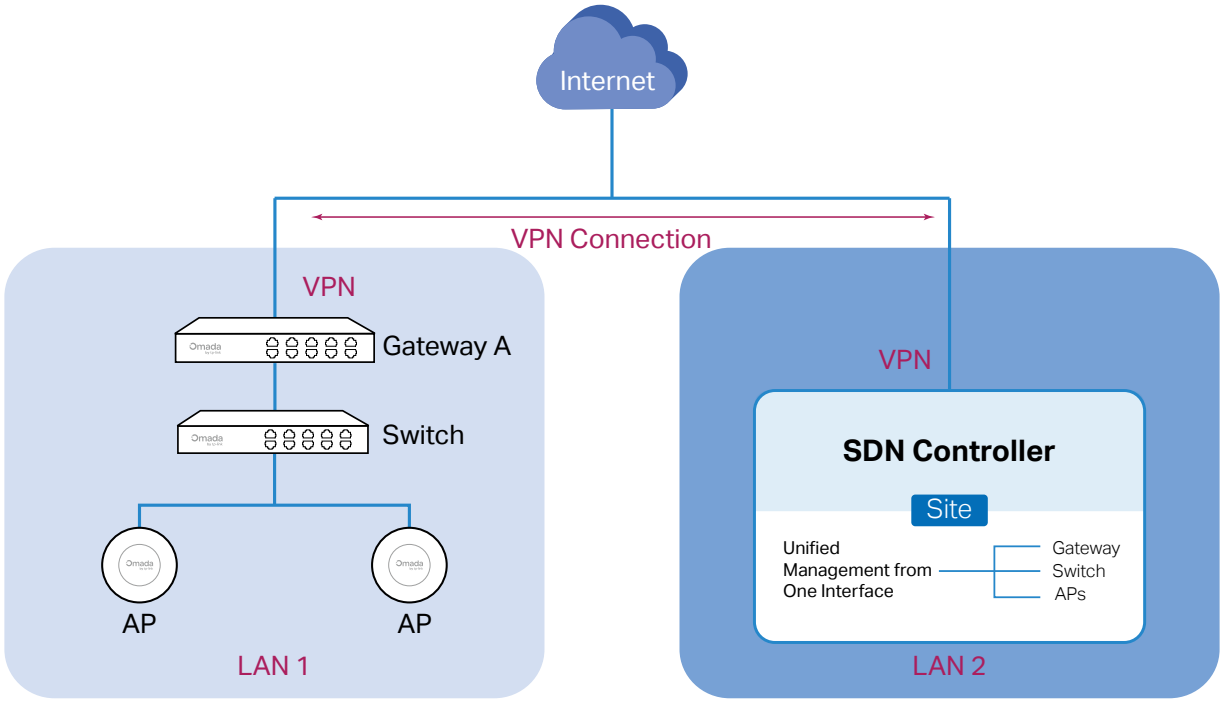
To configure Port Forwarding on the controller, go to Settings > Transmission > NAT > Port Forwarding. Click Create New Rule to load the following page. Specify a name to identify the Port Forwarding rule, check Enable for Status, select Any as Source IP, select the desired WAN port

as Interface, disable DMZ, specify 29810-29814 as Source Port and Destination Port, specify the controller's IP address as Destination IP, and select All as Protocol. Then click Create.



- Use VPN

Set up a VPN connection between Gateway A and the controller. For details about VPN configuration, refer to the User Guide of the gateways, and 4. 6 Configure VPN of this guide.



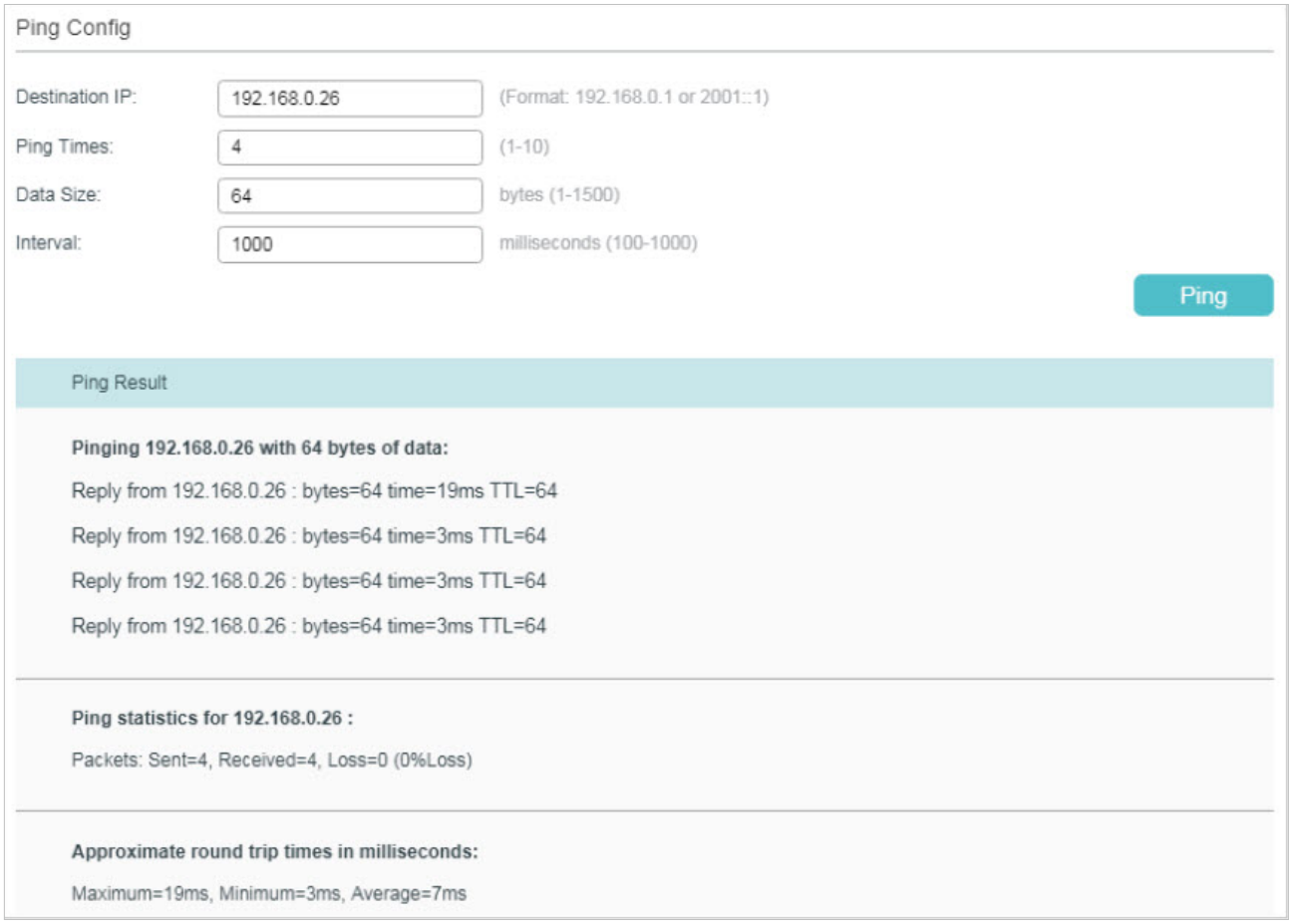
2. (Optional) Test the network

If you are not sure whether the controller and devices can establish communication, it's recommended to do the ping test from the devices to the controller.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Then Go to MAINTENANCE > Network Diagnostics > Ping to load the following page, and specify Destination IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click Ping.

Note:

To ping a router, please turn off Block WAN Ping on the **Settings** > **Network Security** > Attack Defense page.



If the ping result shows the packets are received, it implies that the controller can communicate with the devices. Otherwise, the controller cannot communicate with the devices, then you need to check your network.

Step 2: Prepare for Device Discovery

Note:

If the controller and devices are in the same LAN, subnet and VLAN, skip this step. In this scenario, the controller can discover the devices directly, and no additional settings are required.

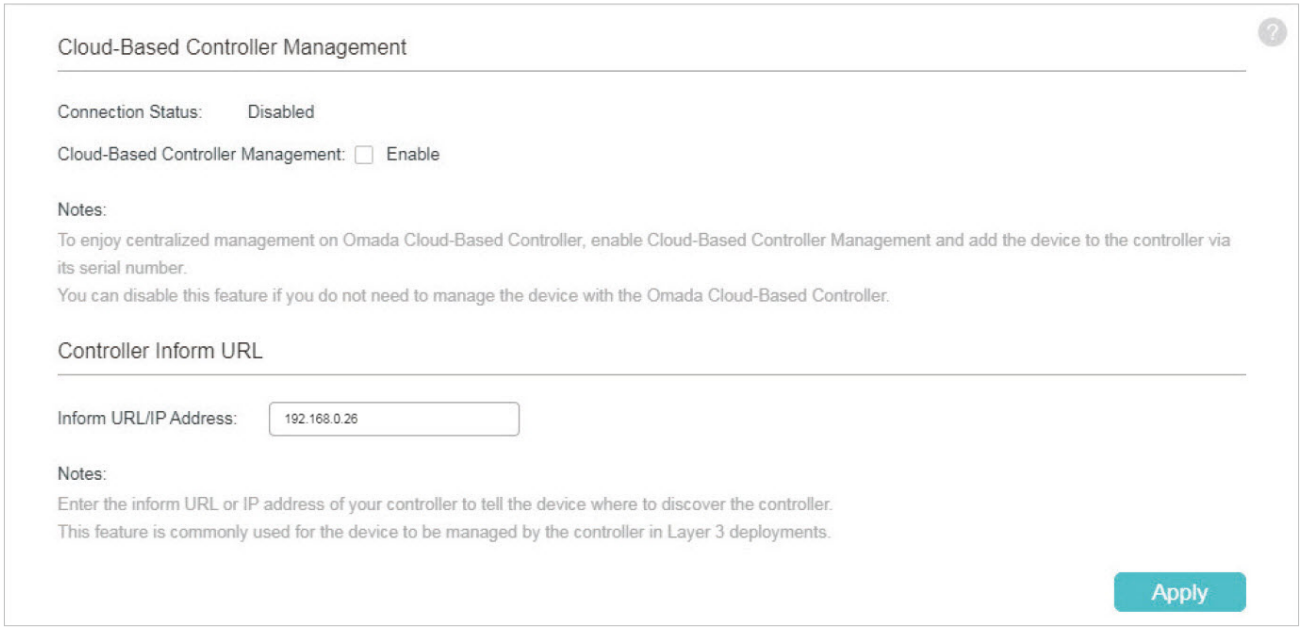
Make sure that the controller can discover the devices.

When the controller and devices are in different LANs, subnets or VLANs, the controller cannot discover the devices directly. You need to choose Controller Inform URL, Discovery Utility, or DHCP Option 138 as the method to help the controller discover the devices.

- **Controller Inform URL**

  Controller Inform URL informs the devices of the controller's URL or IP address. Then the devices make contact with the controller so that the controller can discover the devices.

  You can configure Controller Inform URL for devices in Standalone Mode. Let's take a switch for example. Log into the management page of the switch in Standalone Mode and go to SYSTEM > Controller Settings to load the following page. In Controller Inform URL, specify Inform URL/IP Address as the controller's URL or IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click Apply.

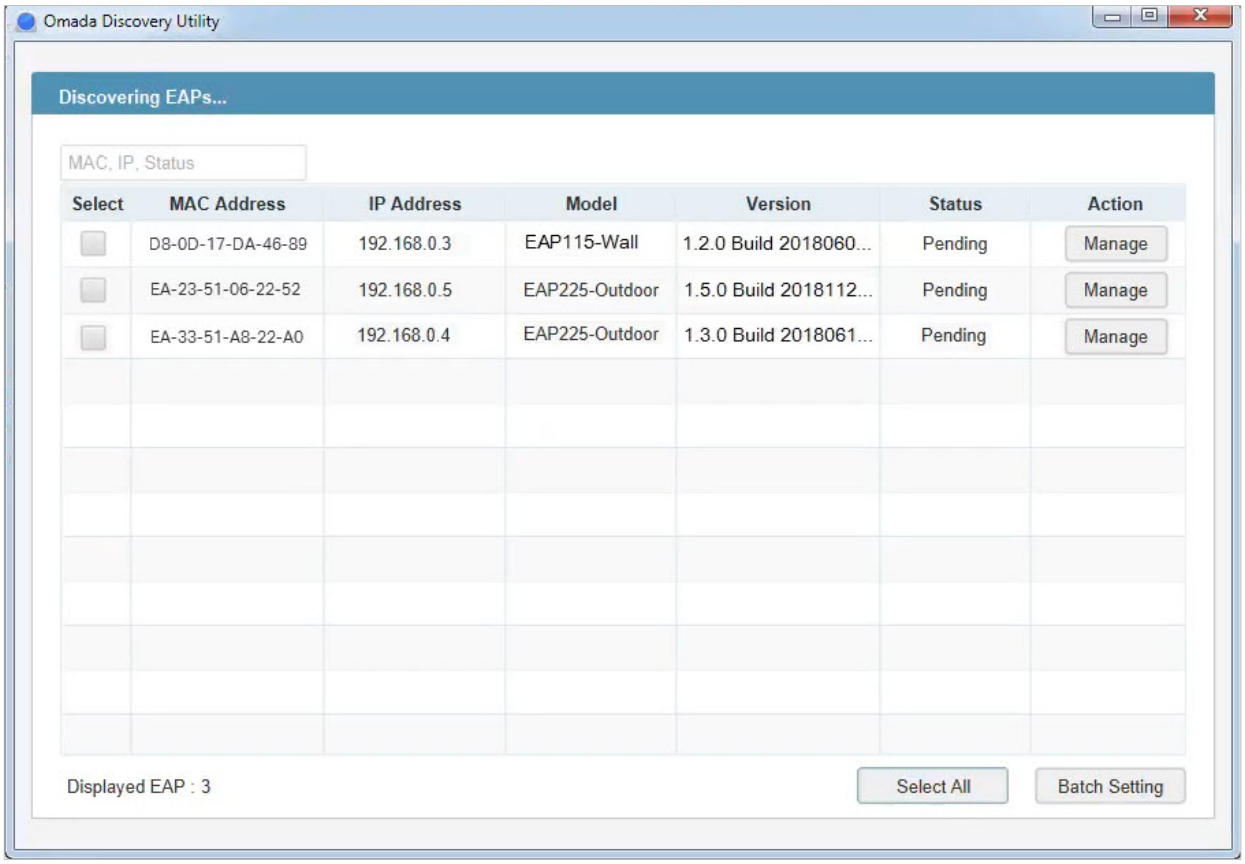


- **Discovery Utility**

  Discovery Utility can discover the devices in the same LAN, subnet and VLAN, and inform the devices of the controller's IP address. Then the devices make contact with the controller so that the controller can discover the devices.

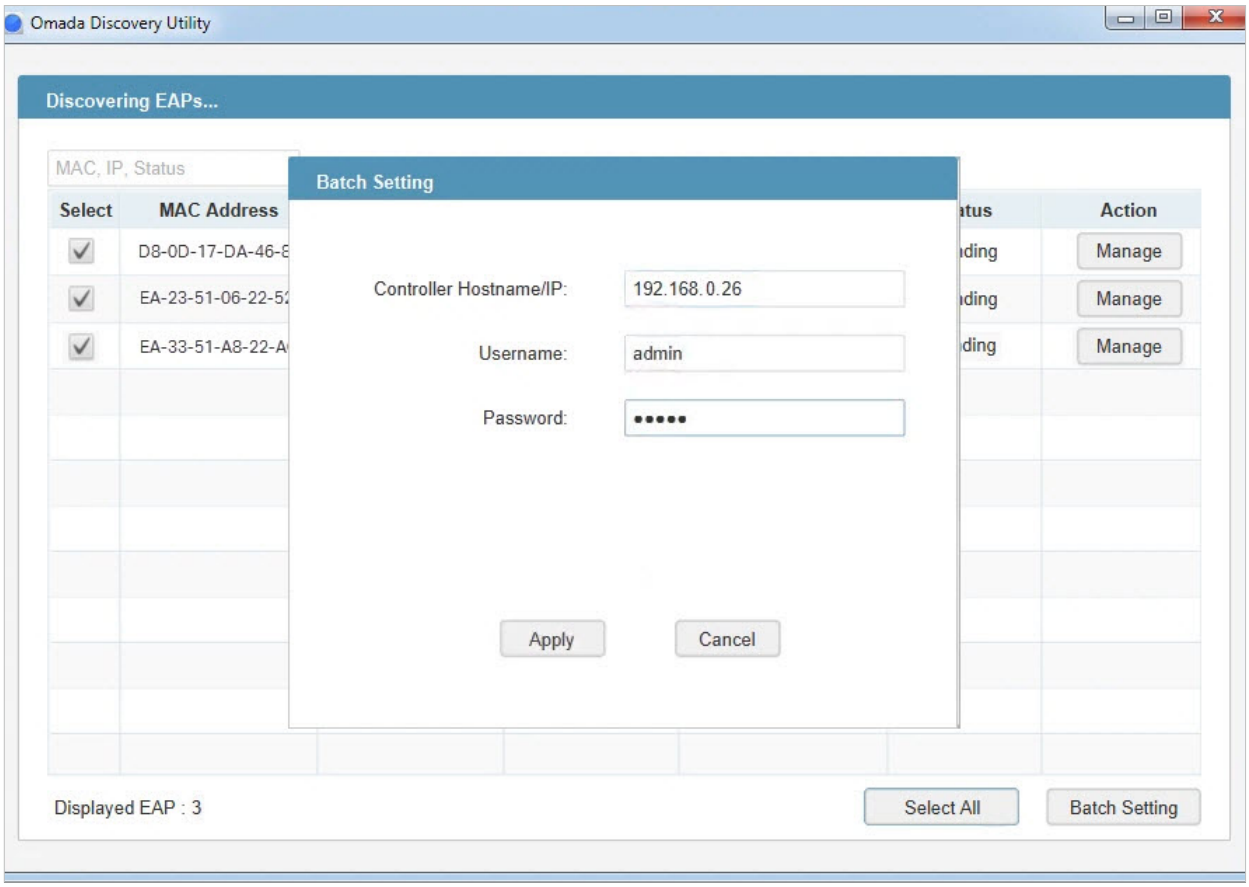
  1. Download Discovery Utility from https://support.omadanetworks.com/product/omada-software-controller/?resourceType=download and then install it on your PC which should be located in the same LAN, subnet and VLAN as your devices.

2. Open Discovery Utility and you can see a list of devices. Select the devices to be adopted and click Batch Setting.



3. Specify Controller Hostname/IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead), and

enter the username and password of the devices. By default, the username and password are both admin. Then click Apply. Wait until the setting succeeds.

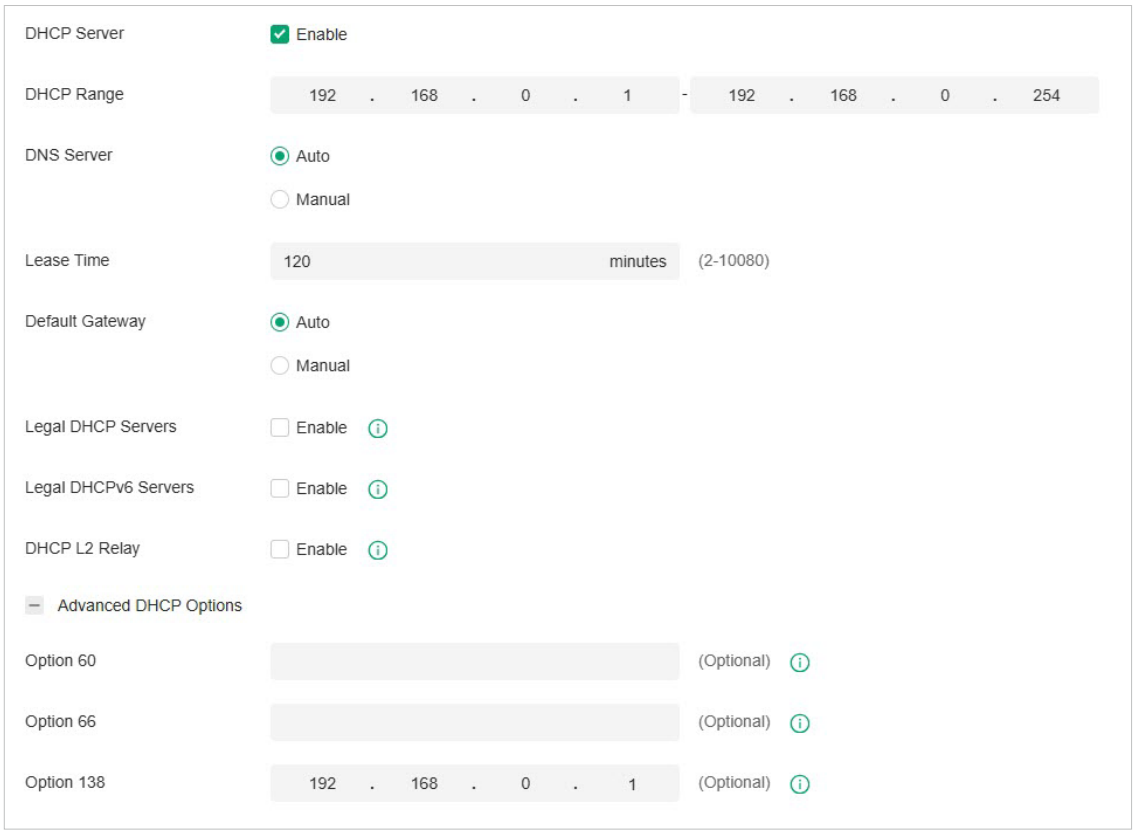


- **DHCP Option 138**

  DHCP Option 138 informs a DHCP client, such as a switch or an EAP, of the controller's IP address when the DHCP client sends DHCP requests to the DHCP server, which is typically a gateway.

  1. To use DHCP Option 138, you need to adopt the gateway on the controller first, which may require other techniques like Controller Inform URL or Discovery Utility if necessary.
  2. After the gateway is adopted, go to Settings > Wired Networks > LAN > Networks, and click the Edit icon in the ACTION column of the LAN where the DHCP clients are located. Enable DHCP Server and configure common DHCP parameters. Then click Advanced DHCP Options

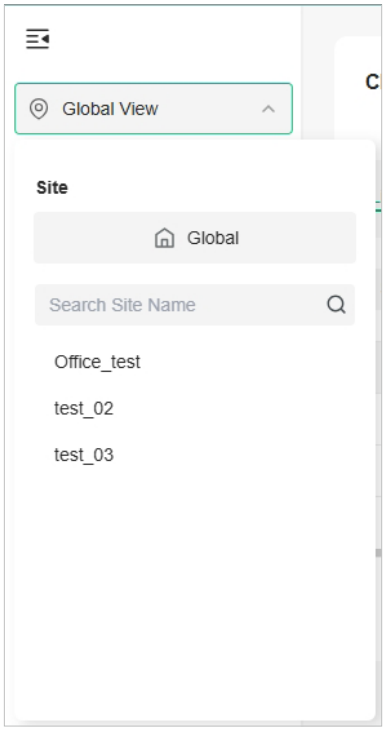
and specify Option 138 as the controller's IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Click Save.



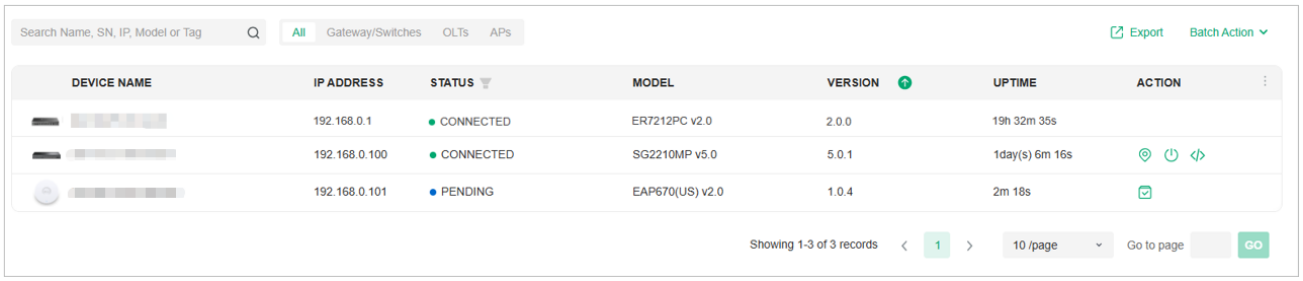
3. To make DHCP Option 138 take effect, you need to renew DHCP parameters for the DHCP clients. One possible way is to disconnect the DHCP clients and then reconnect them.

Step 3: Adopt the Devices

1. Launch the controller and access a site.

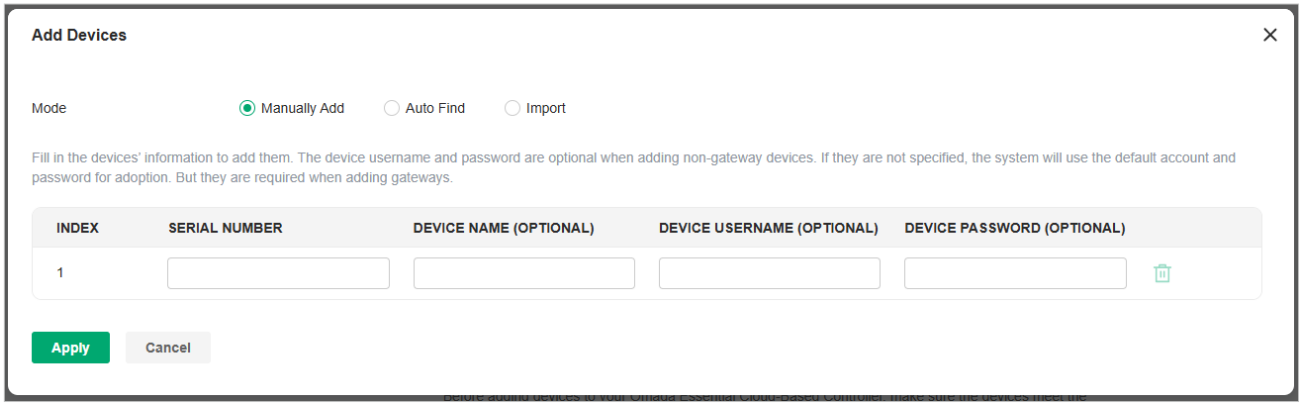


2. Go to Devices, and the devices which have been discovered by the controller are displayed.



Click the Adopt icon in the ACTION column of each pending device that you want to add to the site. Wait until the device status turns into CONNECTED. Then the devices are adopted by the controller and added to the current site. Once the devices are adopted, they are subject to central management in the site.

3. You can also add devices offline. Click Add Devices and choose a method to add your devices.



- **Manually Add**

  Fill in the devices' information to add them. The device username and password are optional when adding non-gateway devices. If they are not specified, the system will use the default account and password for adoption. But they are required when adding gateways.

- **Auto Find**

  Automatically find the Omada devices with Inform URL configured to add them.

- **Import**

  Download the template and fill in your devices' information. Then import the file. Up to 1500 devices can be imported at a time.

3. 3. 3 For Cloud-Based Controller

To adopt the devices on the controller, follow these steps:

1) Connect to the internet.

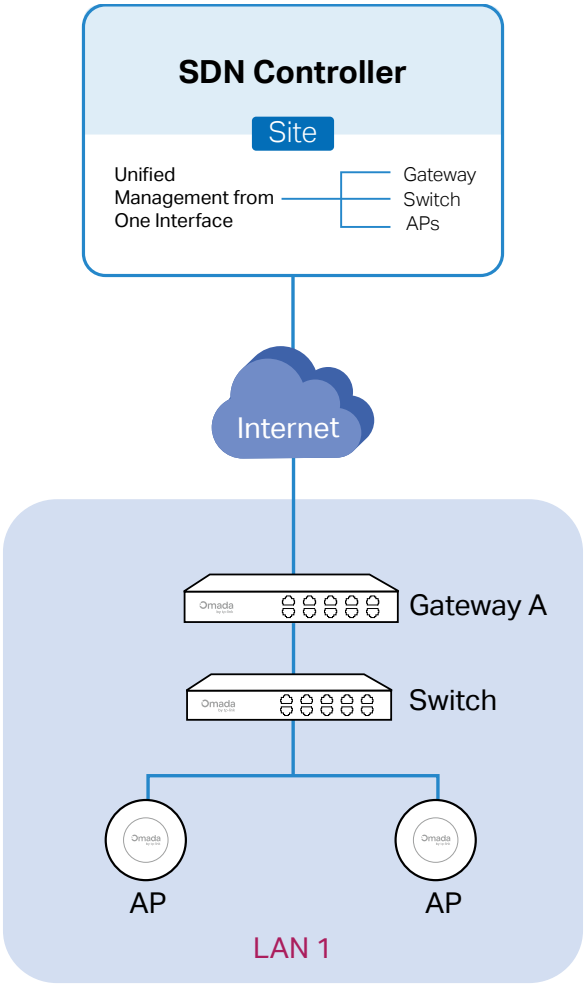
2) Prepare for controller management.

3) Adopt the devices.

Step 1: Connect to the Internet

1. Set up the network.

   Make sure that your devices are connected to the internet.

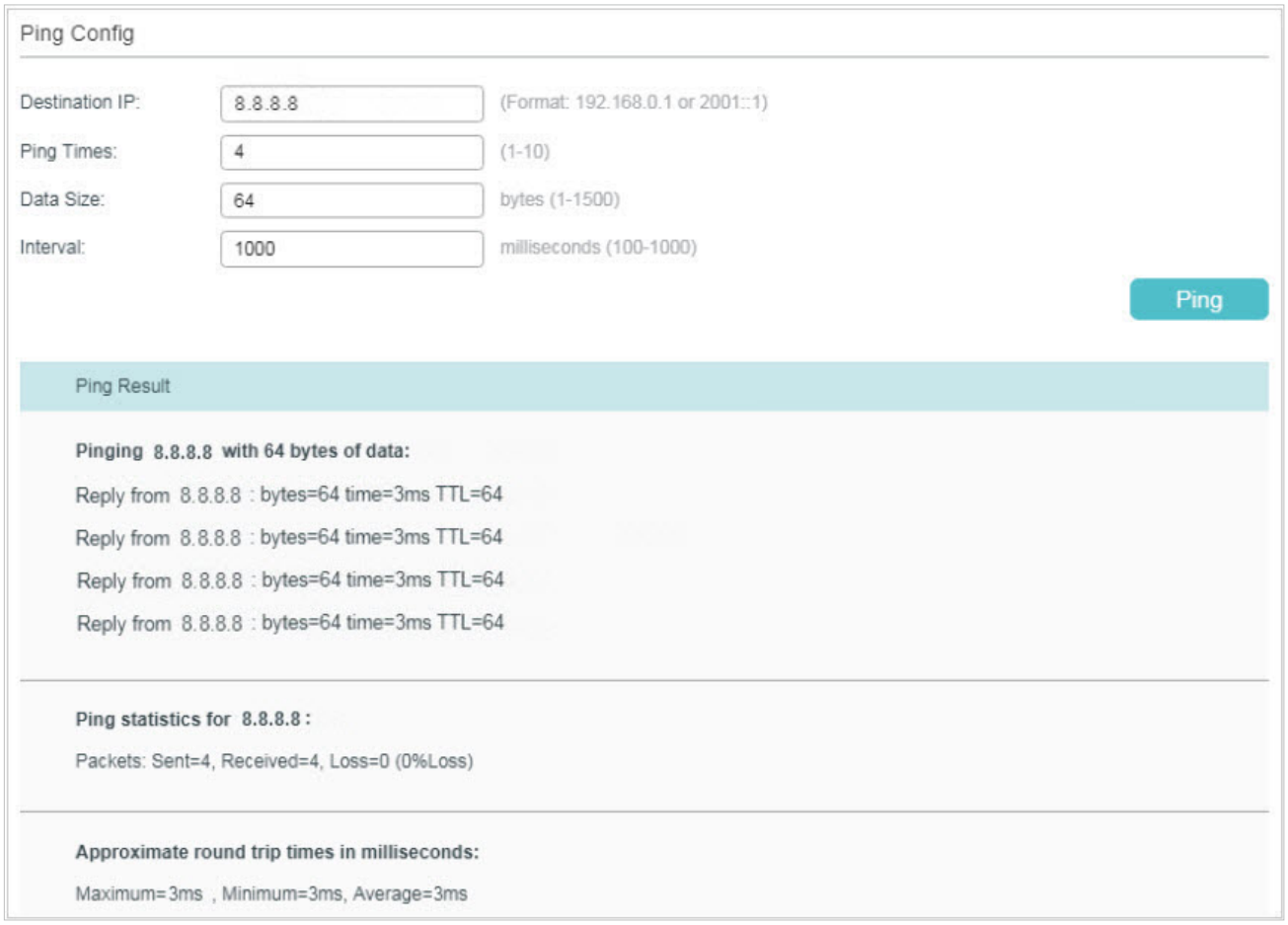


If you are using firewalls in your network, make sure that the firewall doesn't block traffic from the controller. To configure your firewall policy, you may want to know the URL of the controller. After you open the web page of the controller, you can get the URL from the address bar of the browser.

2. (Optional) Test the network.

   If you are not sure whether the devices are connected to the internet, it's recommended to do the ping test from the devices to a public IP address, such as 8.8.8.8.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Go to MAINTENANCE > Network Diagnostics > Ping to load the following page. Specify Destination IP as a public IP address, such as 8.8.8.8. Then click Ping.



If the ping result shows the packets are received, it implies that the devices are connected to the internet. Otherwise, the devices are not connected to the internet, then you need to check your network.

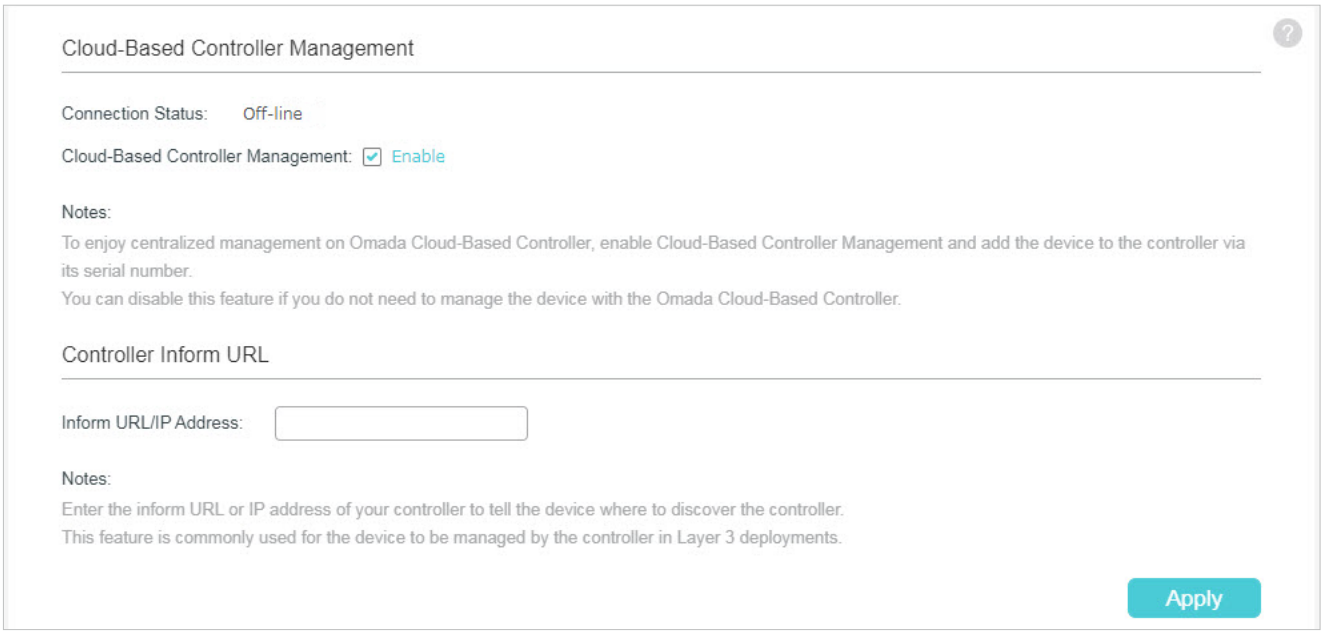
Step 2: Prepare for Controller Management

Note:

If your devices are on the factory default setting, skip this step.

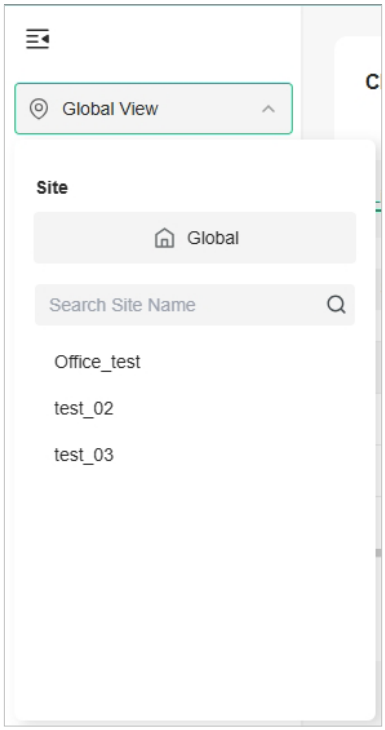
The Cloud-Based Controller Management feature allows the devices to be adopted by the Cloud-Based Controller. Make sure Cloud-Based Controller Management is enabled on the devices. For details, refer to the User Guide of your devices, which can be downloaded from https://support.omadanetworks.com/product/.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Go to SYSTEM > Controller Settings to load the following page. In Cloud-Based Controller Management, enable Cloud-Based Controller Management and click Apply.

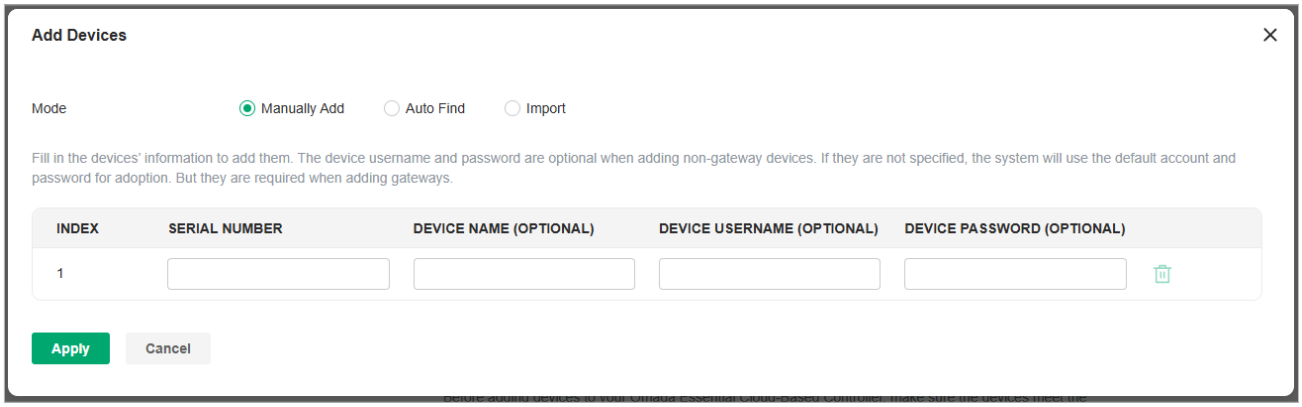


Step 3: Adopt the Devices

1. Ensure your devices are compatible with your Cloud-Based Controller.
   - Essentials version: https://www.omadanetworks.com/omada-cloud-essentials/product-list/
   - Standard version: https://www.omadanetworks.com/omada-cloud-based-controller/product-list/
2. Launch the controller and access a site.



3. Go to Devices and click Add Devices.



4. Choose a method to add your devices.

   - **Manually Add**

     Fill in the devices' information to add them. The device username and password are optional when adding non-gateway devices. If they are not specified, the system will use the default account and password for adoption. But they are required when adding gateways.

   - **Auto Find**

     Automatically find the Omada devices with Inform URL configured to add them.

   - **Import**

     Download the template and fill in your devices' information. Then import the file. Up to 1500 devices can be imported at a time.

5. Once the devices are adopted, they are subject to central management in the site.

3. 4 Navigate the Controller UI

As you start using the management interface of the controller (Controller UI) to configure and monitor your network, it is helpful to familiarize yourself with the Controller UI.

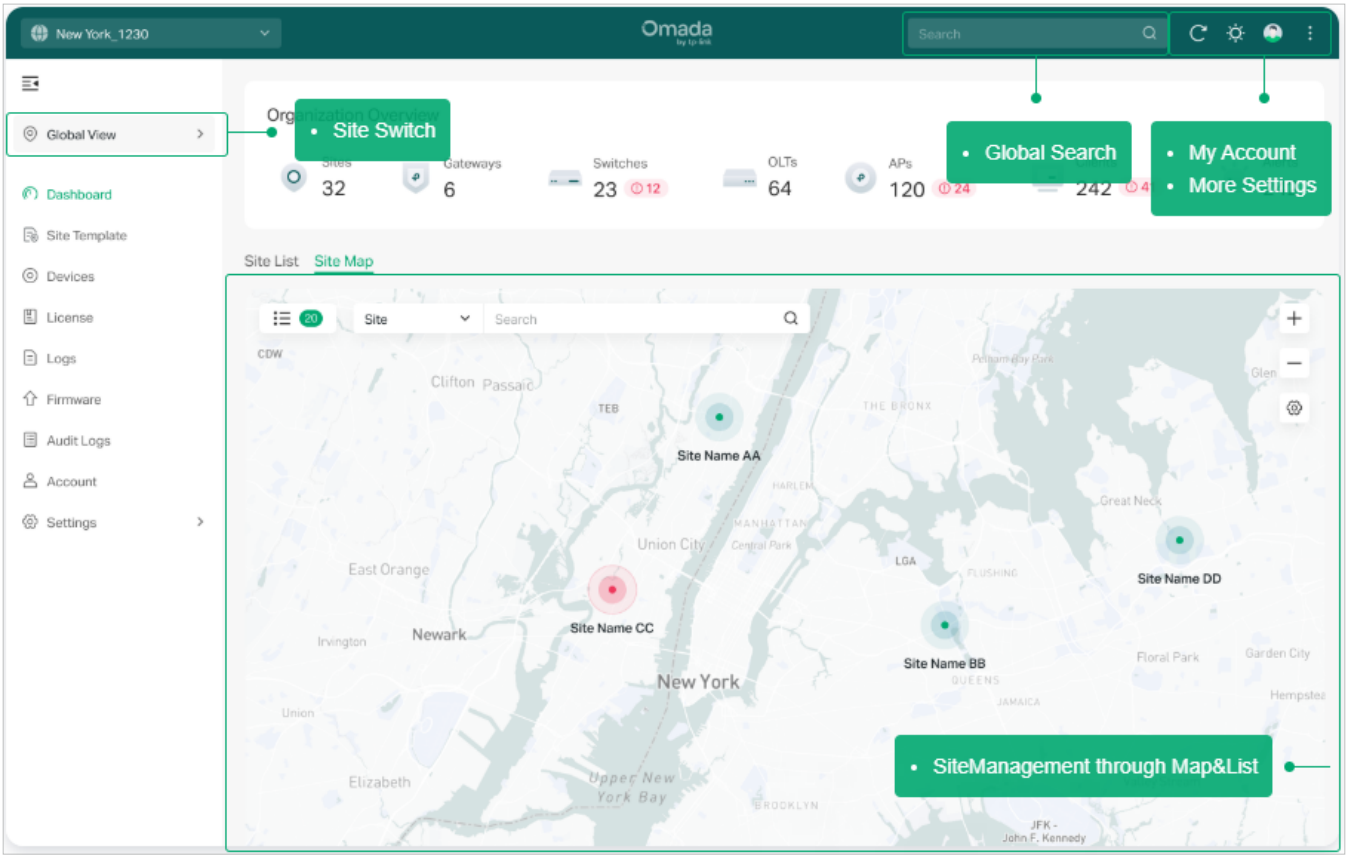
Note:

Features available in the Omada SDN Controller may vary due to your region, controller type and version, and device model.

- **Global Overview**

  Know the status of your sites at a glance, and manage sites in the platform.

  - Site Monitoring—Keep you informed of accurate, real-time status of every site.
  - Site Management—Manage all sites to deploy the whole network.
  - Account Settings—Manage all administrative accounts.



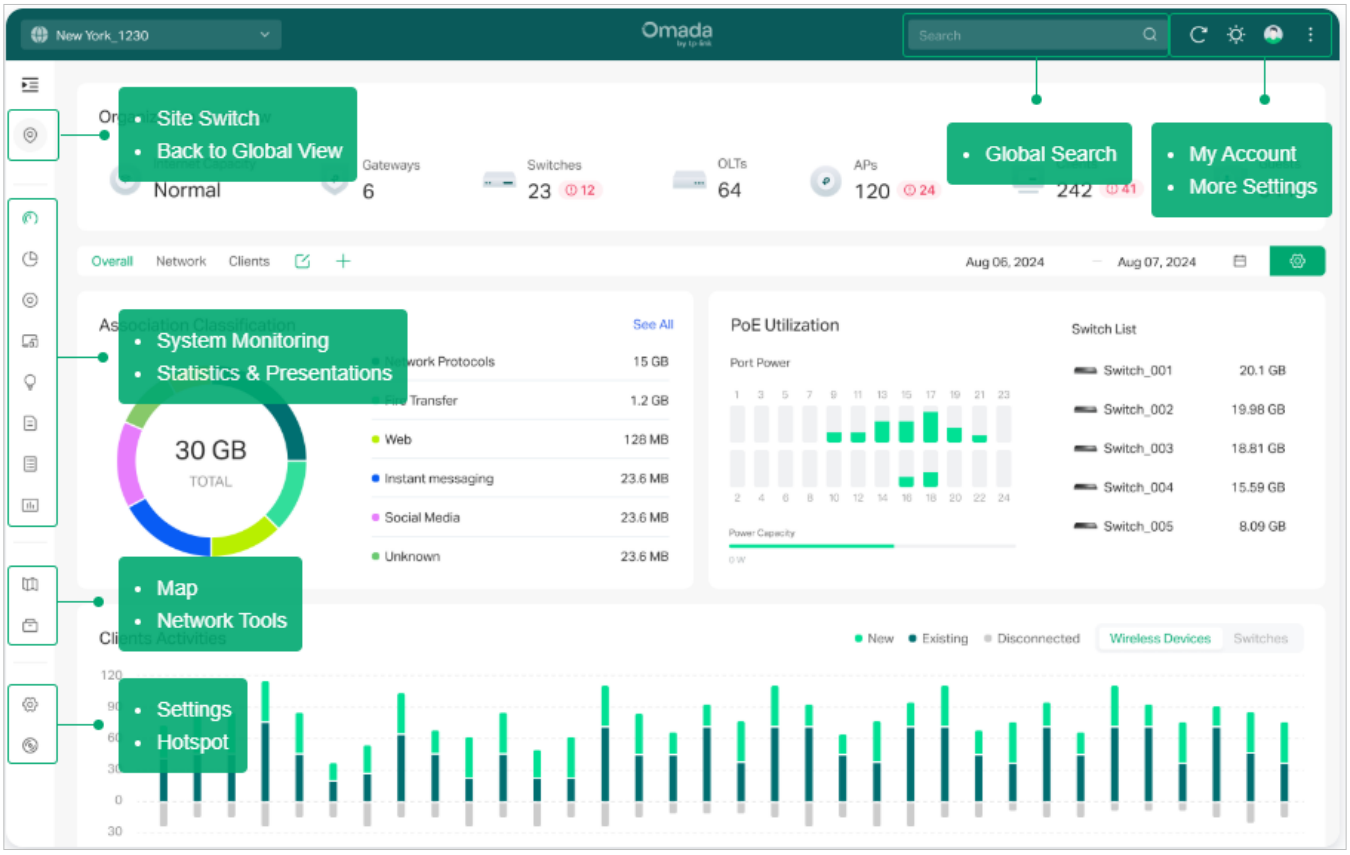
- **Site Overview**

  Know the status of your network at a glance, gain insights, and manage network devices all in the platform.

  - Statistics & Monitoring—Keep you informed of accurate, real-time status of every network

device and client.

- Settings—Configure all your network devices centrally.



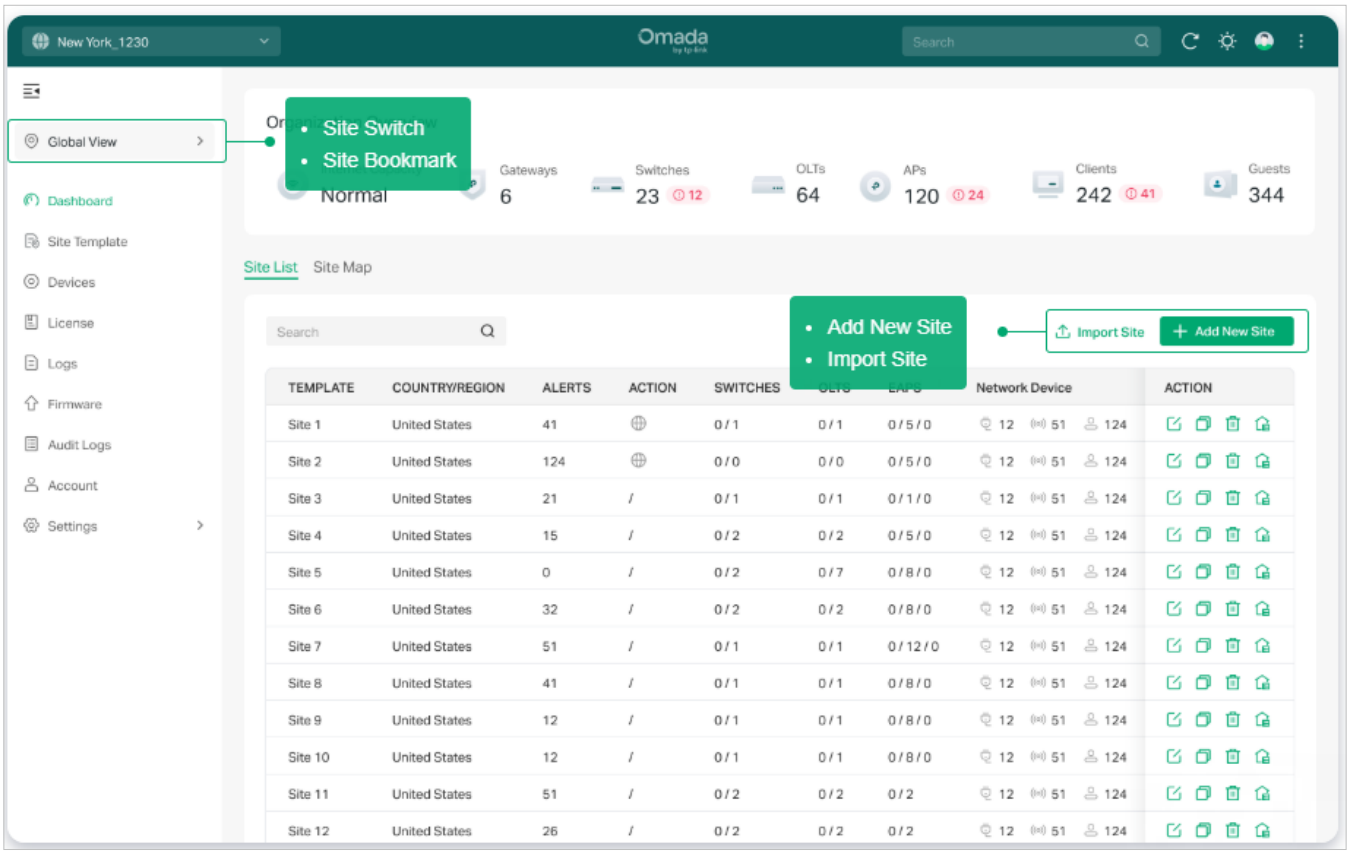
Site Management

Site, which means logically separated network location, is the largest unit for managing networks with the SDN Controller. You can simultaneously configure features for multiple devices at a site.

- Add New Site — Click Add New Site to add a new site, which is the logically separated network

location. The site is the largest unit for managing the network.

- Import Site — Click Import Site to import the site from another controller.
- Site Bookmark – Click Bookmark to place frequently-used sites on the top of the list.



Network Monitoring

Visual data keeps the network administrator informed about accurate status of every network device and client on the wired and wireless network.

The Controller UI is grouped into task-oriented menus. These menus are located in the left-hand navigation bar of the page. Note that the settings and features that appear in the UI depend on your user account permissions. The following image depicts the main elements of the Controller UI.

The elements in the top right corner of the screen give quick access to:



Global Search Feature

Click the Search icon and enter the keywords to quickly look up the functions or devices that you want to configure. And you can search for the devices by their MAC addresses and device names.

Refresh Page

Click the Refresh icon to refresh the page.

Theme Settings

Change theme settings to light mode, dark mode, or system theme to improve your overall screen experience.

My Account

Click the Account icon to display account information, Account Settings and Log Out. You can change your password on Account Settings.

More Settings

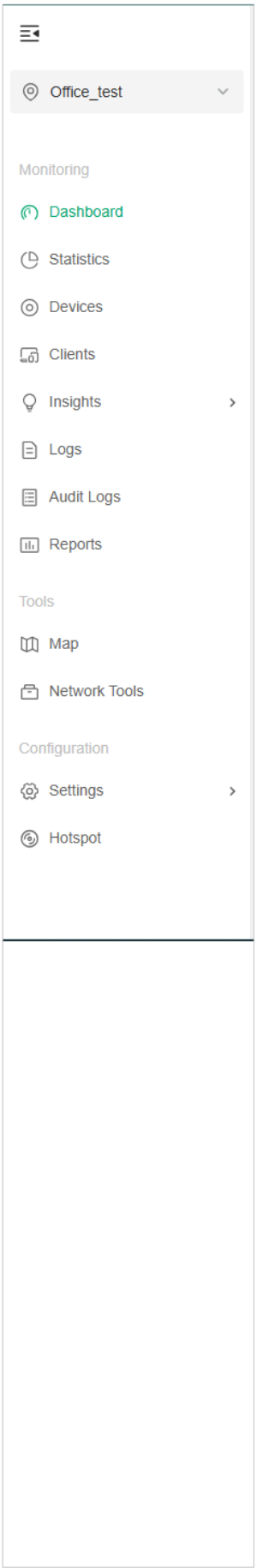
Click the More icon for more settings.Z

Feedback: Click to send your feedback to us.

About: Click to display the controller info.

Tutorial: Click to view the quick Getting Started guide which demonstrates the navigation and tools available for the controller.

The left-hand navigation bar provides access to:



Global/Site View drop-down list: allows you to access the Global View or access a site quickly.

Global View — Know the status of your Site at a glance, and manage sites in the platform.

Site View — Know the status of your network at a glance, gain insights, and manage network devices all in the platform.

Dashboard: displays a summarized view of the network status through different visualizations. The customizable and widget-driven dashboard is a powerful tool that arms you with real-time data for monitoring the network. With the drag and drop feature, you can modify your dashboard and re-arrange it to let you track all the important metrics.

Statistics: provides a visual representation of the clients and network managed by the controller. The run charts show changes in device performances over time, including the status of switches and speed test results.

Devices: displays all TP-Link devices discovered on the site and their general information. This list view can change depending on your monitoring need through customizing the columns. You can click any device on the list to reveal the Properties window for more detailed information of each device and provisioning individual configurations to the device.

Clients: displays a list view of wired and wireless clients that are connected to the network. This list view can change depending on your monitoring need through customizing the columns. You can click any clients on the list to reveal the Properties window for more detailed information of each client and provisioning individual configurations to the client.

Insights: displays a list of statistics of your network device, clients and services during a specified period. You can change the range of date in one-day increments.

Logs: shows log lines about varied activities of users, devices, and systems events, such as administrative actions and abnormal device behaviors. Comprehensive logs make historical information more accurate, readily accessible, and usable, which allows for proactive troubleshooting. And you can determine alert-level events and enable pushing notifications.

Audit Logs: records information about which accounts have accessed the site, and what operations they have performed during a given period of time.

Reports: provides intuitive charts and detailed statistics concerning your network situation, managed devices, and connected clients.

Map: generates the system topology automatically and you can look over the provisioning status of devices. By clicking on each node, you can view the detailed information of each device. You can also upload images of your location for a visual representation of your network.

Network Tools: provides various network tools for you to test the device connectivity, capture packets for troubleshooting, and open Terminal to execute CLI or Shell commands.

Settings allows you to provision and configure all your network devices on the same site in minutes and maintain the controller system for best performance.

Hotspot: allows you to centrally monitor and manage the clients authorized by portal authentication.

Chapter 4

Configure the Network with the SDN Controller

This chapter guides you on how to configure the network with the SDN Controller. As the command center and management platform at the heart of the SDN network, the Controller provides a unified approach to configuring enterprise networks comprised of routers, switches, and wireless access points. The chapter includes the following sections:

- 4. 1 Modify the Current Site SettingsSettings
- 4. 2 Configure Wired Networks
- 4. 3 Configure Wireless Networks
- 4. 4 Network Security
- 4. 5 Transmission
- 4. 6 Configure VPN
- 4. 7 Create Profiles
- 4. 8 Authentication
- 4. 9 Services
- 4. 10 SIM
- 4. 11 CLI Configuration

4. 1 Modify the Current Site Settings

You can view and modify the configurations of the current site in Site, including the basic site information, centrally-managed device features, and the device account. The features and device account configured here are applied to all devices on the site, so you can easily manage the devices centrally.

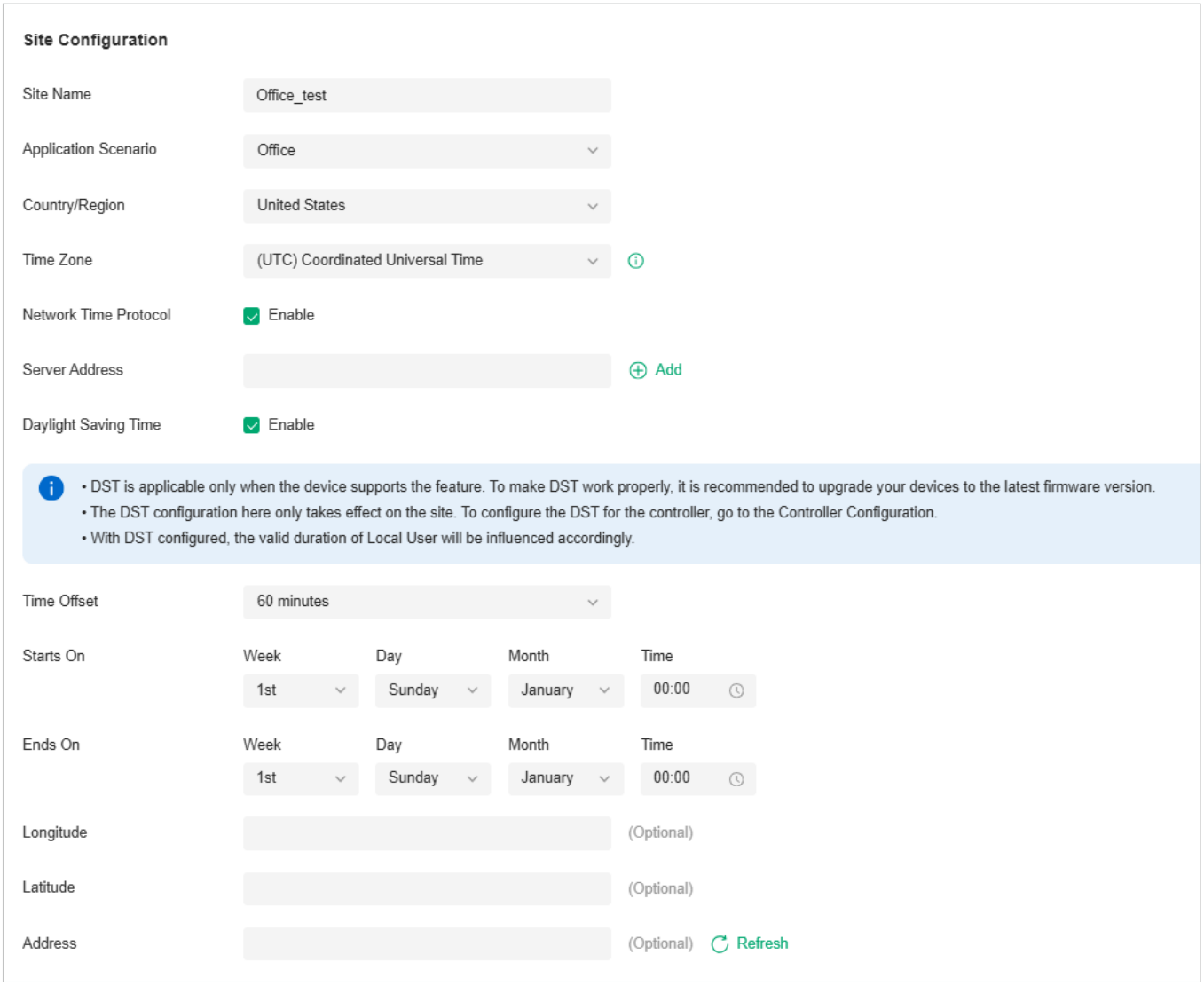
4. 1. 1 Site Configuration

Overview

In Site Configuration, you can view and modify the site name, location, time zone, and application scenario of the current site.

Configuration

Launch the controller and access a site. Go to Settings > General Settings > Site Settings, and configure the following information of the site in Site Configuration. Click Save.



Site Name	Specify the name of the current site. It should be no more than 64 characters.
Application Scenario	Specify the application scenario of the site. To customize your scenario, click Create New Scenario in the drop-down list.
Country/Region	Select the location of the site.
Time Zone	Select the time zone of the site.
Network Time Protocol	Enter the IP address(es) of the NTP (Network Time Protocol) server. NTP server assigns network time to the EAP devices.
Daylight Saving Time	Enable the feature if your country/region implements DST.
Time Offset	Select the time added in minutes when Daylight Saving Time starts.
Starts On	Specify the time when the DST starts. The clock will be set forward by the time offset you specify.
Ends On	Specify the time when the DST ends.The clock will be set back by the time offset you specify.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.

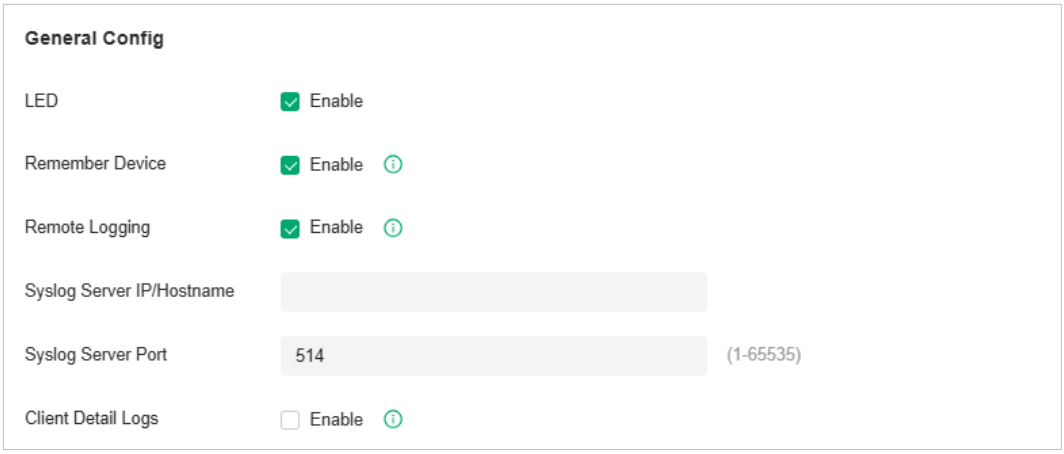
4. 1. 2 General Config

Overview

In General Config, you can control the LED status of devices in the site, remember all devices in the site, configure the controller to send generated system logs to the log server.

Configuration

Launch the controller and access a site. Go to Settings > General Settings > Site Settings, and configure the following features for the current site in General Config. Click Save.



LED	Enable or disable LEDs of all devices in the site. By default, the device follows the LED setting of the site it belongs to. To change the LED setting for certain devices, refer to Chapter 6. Configure and Monitor Controller-Managed Devices.
Remember Device	When enabled, the controller will remember all devices in the site. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.
Remote Logging	With this feature configured, the controller will send generated site logs to the log server. When enabled, the following items are required: Syslog Server IP/Hostname: Enter the IP address or hostname of the log server. Syslog Server Port: Enter the port of the server. Client Detail Logs: With this feature enabled, the logs of clients will be sent to the syslog server.

4. 1. 3 Wireless Features

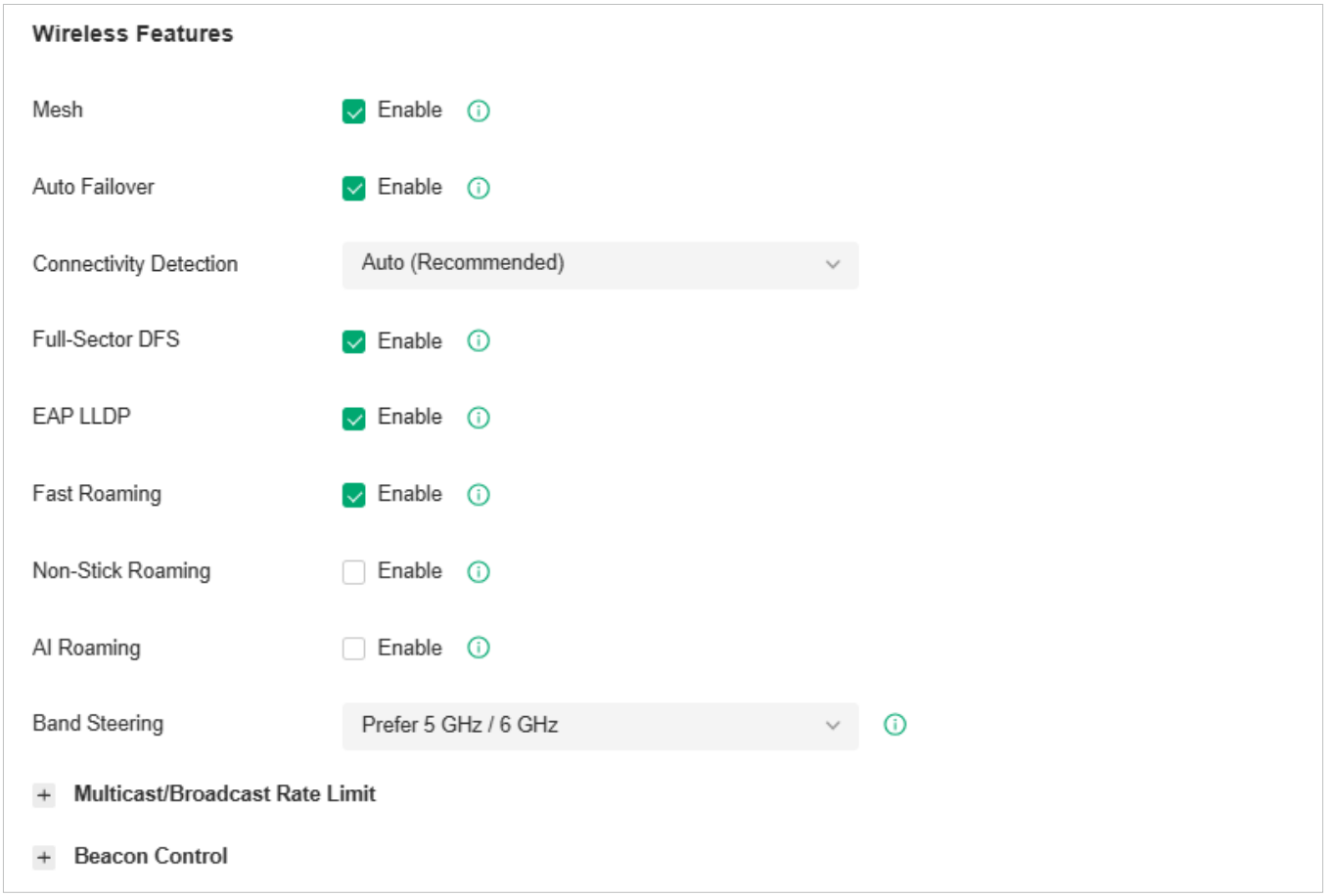
Overview

Wireless features include Mesh, Auto Failover, Connectivity Detection, Full-Sector DFS, EAP LLDP, Fast Roaming, Non-Stick Roaming, AI Roaming, Band Steering, Multicast/Broadcast Rate Limit and Beacon Control. They are applicable to APs and wireless gateways/routers. With these wireless features configured properly, you can improve the network's stability, reliability and communication efficiency.

Wireless features are recommended to be configured by network administrators with the WLAN knowledge. If you are not sure about your network conditions and the potential impact of all settings, keep Wireless Features as their default configurations.

Configuration

Launch the controller and access a site. Go to Settings > General Settings > Site Settings, and configure the following features in Wireless Features. Click Save.



Mesh	When enabled, APs supporting Mesh can establish the mesh network at the site.
Auto Failover	(For APs in the mesh network) Auto Failover is used to automatically maintain the mesh network. When enabled, the controller will automatically select a new wireless uplink for the AP if the original uplink fails. To enable this feature, enable Mesh first.
Connectivity Detection	(For APs in the mesh network) Specify the method of Connection Detection when mesh is enabled. In a mesh network, the APs can send ARP request packets to a fixed IP address to test the connectivity. If the link fails, the status of these APs will change to Isolated. Auto (Recommended): Select this method and the mesh APs will send ARP request packets to the default gateway for the detection. Custom IP Address: Select this method and specify a desired IP address. The mesh APs will send ARP request packets to the custom IP address to test the connectivity. If the IP address of the AP is in different network segments from the custom IP address, the AP will use the default gateway IP address for the detection.
Full-Sector DFS	(For APs in the mesh network) With this feature enabled, when radar signals are detected on current channel by one AP, the other APs in the mesh network will be also informed. Then all APs in the mesh network will switch to an alternate channel. To enable this feature, enable Mesh first.

EAP LLDP	Click the checkbox to enable EAP LLDP (Link Layer Discovery Protocol) for device discovery and auto-configuration of VoIP devices.
Fast Roaming	With this feature enabled, wireless clients that support 802.11k/v can improve fast roaming experience when moving among different APs and wireless gateways/routers. By default, it is disabled. This feature is available for some certain devices.
Non-Stick Roaming	This feature helps disconnect "sticky clients" receiving weak signals from their suboptimal Wireless Device, allowing them to switch to a superior Wireless Device and improve network efficiency. Note that this may cause temporary disconnections or hinder re-association in rare cases.
AI Roaming	With Fast Roaming enabled, you can enable AI Roaming to facilitate Fast Roaming, which improves roaming experience of the wireless clients that support 802.11k/v. This feature is available for certain models.
Band Steering	Band steering can adjust the number of clients in 2.4 GHz, 5 GHz and 6 GHz bands to provide better wireless experience. When enabled, multi-band clients will be steered to the 5 GHz and 6 GHz band according to the configured parameters. This function can improve the network performance because the 5 GHz and 6 GHz band supports a larger number of non-overlapping channels and is less noisy.
Multicast/Broadcast Rate Limit	With rate limit configured for Other Multicast, multicast services such as multicast video will be affected.

Beacon Control	Beacons are transmitted periodically by the AP and wireless gateway/router to announce the presence of a wireless network for the clients. Click [+], select the band, and configure the following parameters of Beacon Control. Beacon Interval: Specify how often the APs and wireless gateways/routers send a beacon to clients. By default, it is 100. DTIM Period: Specify how often the clients check for buffered data that are still on the AP or wireless gateway/router awaiting pickup. By default, the clients check for them at every beacon. DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames indicating whether the AP or wireless gateway/router has buffered data for client devices. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend that you keep the default interval, 1. RTS Threshold: RTS (Request to Send) can ensure efficient data transmission by avoiding the conflict of packets. If a client wants to send a packet larger than the threshold, the RTS mechanism will be activated to delay packets of other clients in the same wireless network. We recommend that you keep the default threshold, which is 2347. If you specify a low threshold value, the RTS mechanism may be activated more frequently to recover the network from possible interference or collisions. However, it also consumes more bandwidth and reduces the throughput of the packet. Fragmentation Threshold: Fragmentation can limit the size of packets transmitted over the network. If a packet to be sent exceeds the Fragmentation threshold, the Fragmentation function will be activated, and the packet will be fragmented into several packets. By default, the threshold is 2346. Fragmentation helps improve network performance if properly configured. However, too low fragmentation threshold may result in poor wireless performance because of the increased message traffic and the extra work of dividing up and reassembling frames. Airtime Fairness: With this option enabled, each client connecting to the AP or wireless gateway/router can get the same amount of time to transmit data so that low-data-rate clients do not occupy too much network bandwidth and network performance improves as a whole. We recommend you enable this function under multi-rate wireless networks.

4. 1. 4 Device Account

You can specify a device account for all adopted devices on the site in batches. Once the devices are adopted by the controller, their username and password become the same as settings in Device Account to protect the communication between the controller and devices. By default, the username is admin and the password is generated randomly.

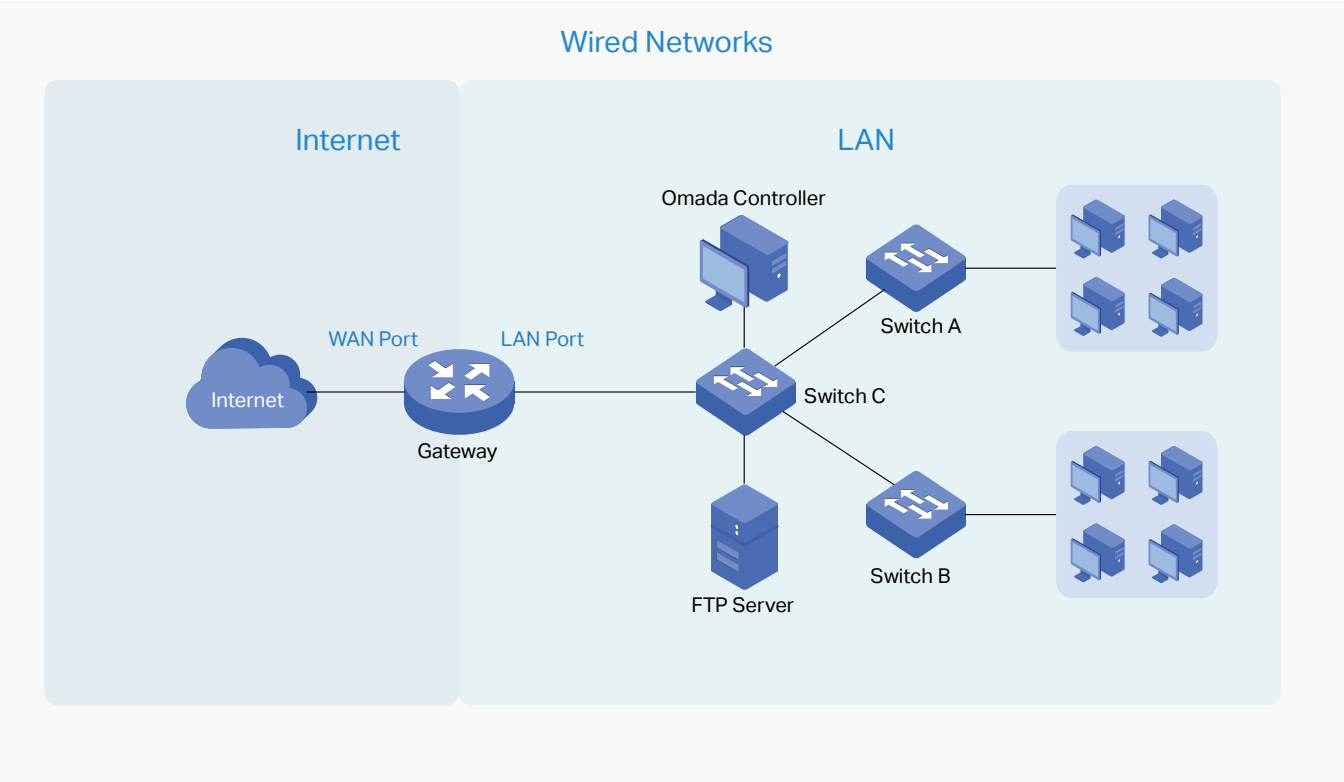
Launch the controller and access a site. Go to Settings > Site Settings and modify the username and password in Device Account. Click Save and the new username and password are applied to all devices on the site.


Device Account
Username
admin
Password
••••••••••••

4. 2 Configure Wired Networks

Wired networks enable your wired devices and clients including the gateway, switches, APs and PCs to connect to each other and to the internet.

As shown in the following figure, wired networks consist of two parts: Internet and LAN.



For Internet, you determine the number of WAN ports on the gateway and how they connect to the internet. You can set up an IPv4 connection and IPv6 connection to your internet service provider (ISP) according to your needs. The parameters of the internet connection for the gateway depend on which connection types you use. For an IPv4 connection, the following internet connection types are available: Dynamic IP, Static IP, PPPoE, L2TP, and PPTP. For an IPv6 connection, the following internet connection types are available: Dynamic IP (SLAAC/ DHCPv6), Static IP, PPPoE, 6to4 Tunnel, and Pass-Through (Bridge). And, when more than one WAN port is configured, you can configure Load Balancing to optimize the resource utilization if needed.

For LAN, you configure the wired internal network and how your devices logically separate from or connect to each other by means of VLANs and interfaces. Advanced LAN features include IGMP Snooping, DHCP Server and DHCP Options, PoE, Voice Network, 802.1X Control, Port Isolation, Spanning Tree, LLDP-MED, and Bandwidth Control.

4. 2. 1 Set Up an Internet Connection

Configuration

To set up an internet connection, follow these steps:

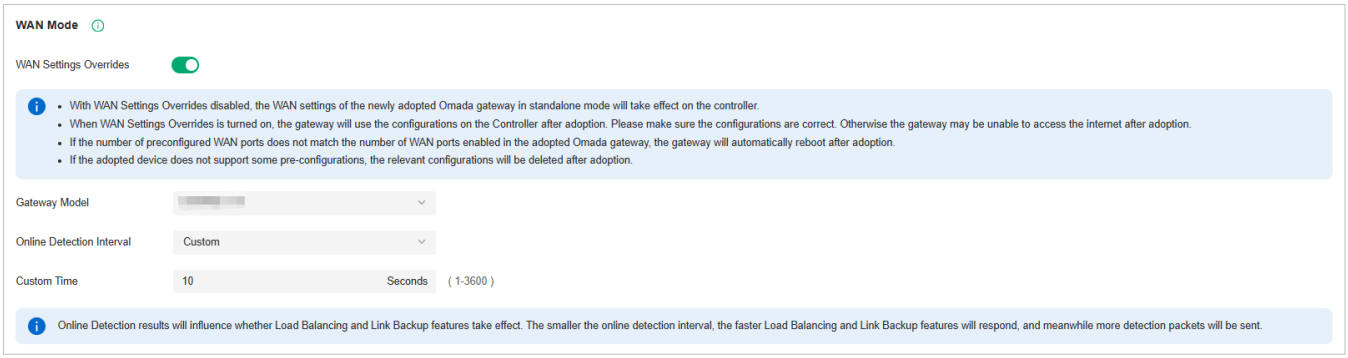
1) Configure the number of WAN ports on the gateway based on needs.

2) Configure WAN Connections. You can set up the IPv4 connection, IPv6 connection, or both.

3) (Optional) Configure Load Balancing if more than one WAN port is configured.

Step 1: Select WAN Mode

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet to load the following page. In the WAN Mode section, configure the number of WAN ports deployed by the gateway and other parameters. Then click Apply.



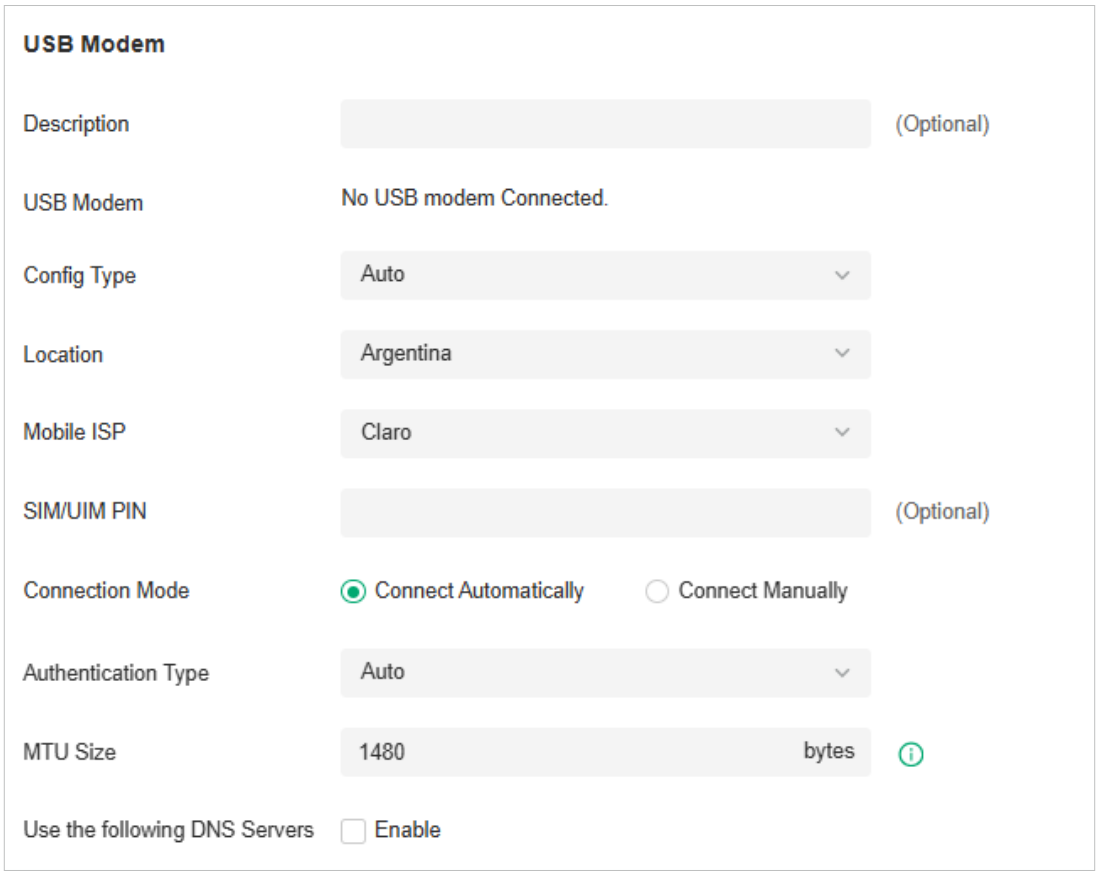
WAN Settings Overrides	With this option disabled, the WAN settings of the newly adopted Omada gateway in standalone mode will take effect on the controller. When this option is turned on, the gateway will use the configurations on the Controller after adoption. Please make sure the configurations are correct. Otherwise the gateway may be unable to access the internet after adoption. If the adopted device does not support some pre-configurations, the relevant configurations will be deleted after adoption.
Gateway Model	Specify the gateway model and version. If you change the gateway, follow the web instructions to select WAN ports and copy WAN port settings. If the number of preconfigured WAN ports does not match the number of WAN ports enabled in the adopted Omada gateway, the gateway will automatically reboot after adoption.
Online Detection Interval	Select how often the WAN ports detect WAN connection status. If you don't want to enable online detection, select Disable. Online Detection results will influence whether Load Balancing and Link Backup features take effect. The smaller the online detection interval, the faster Load Balancing and Link Backup features will respond, and meanwhile more detection packets will be sent.

Step 2: Configure WAN Connections

Note: The number of configurable WAN ports is decided by WAN Mode.

- Set Up DSL WAN Connection

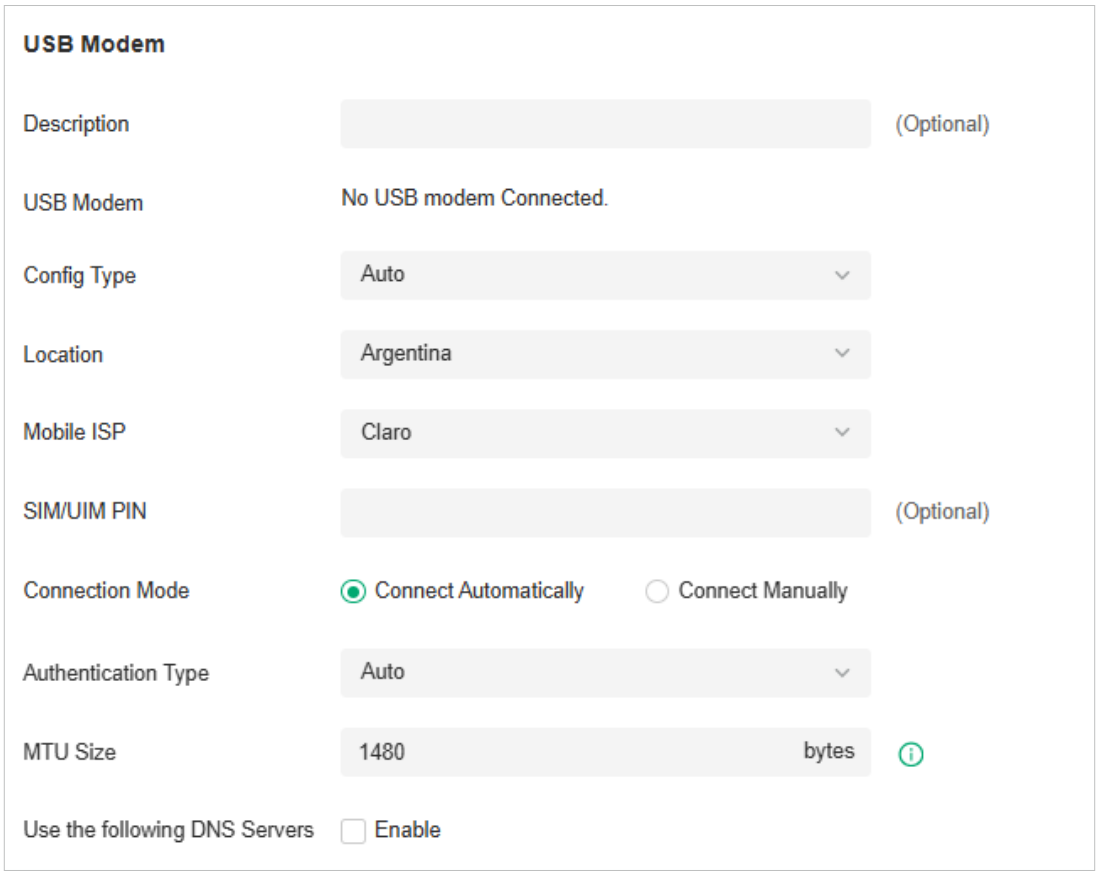
Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports Config section, click the edit icon of USB Modem and configure the parameters.



Description	Enter a description for identification.
Location	Select your location.
ISP	Select your ISP (internet service provider).
DSL Modulation Type	Select the modulation type for your DSL connection.
VPI	Enter the VPI assigned by your ISP to specify the virtual path between enpoints in an ATM network.
VCI	Enter the VCI assigned by your ISP to specify the virtual path between channels in an ATM network.

- Set Up USB Modem Connection

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports Config section, click the edit icon of USB Modem and configure the parameters.



Description	Enter a description for identification.
USB Modem	Display whether a USB modem is connected to the device and the name of the connected USB modem.
Config Type	Select a configuration type for the USB modem. Auto: Use the Location and Mobile ISP information below for configuration. Manually: Enter the Dial Number, APN, Username, and password provided by your Mobile ISP.
Location	Select your location.
Mobile ISP	Select your mobile ISP.
Message	Display the current status of the SIM card.
SIM/UIM PIN	(Optional) Enter the PIN of your SIM card. The field is required when the following information appears in the Message: PIN protection is enabled and the PIN is invalid.

Connection Mode	Select the connection mode. Connect Automatically: The router will use the USB modem to connect to the internet automatically. Connect Manually: You need to turn on/off the internet manually for the gateway on the device page.
Authentication Mode	Select the Authentication mode for the USB modem. The default value is Auto, and it is recommended to keep the default value.
MTU Size	Specify the MTU (Maximum Transmission Unit) of the USB WAN port. The default value is 1480, and it is recommended to keep the default value. MTU is the maximum data unit transmitted in the physical network.
Use the following DNS Servers	Enable the feature if you want to specify the Primary and Secondary DNS servers manually.

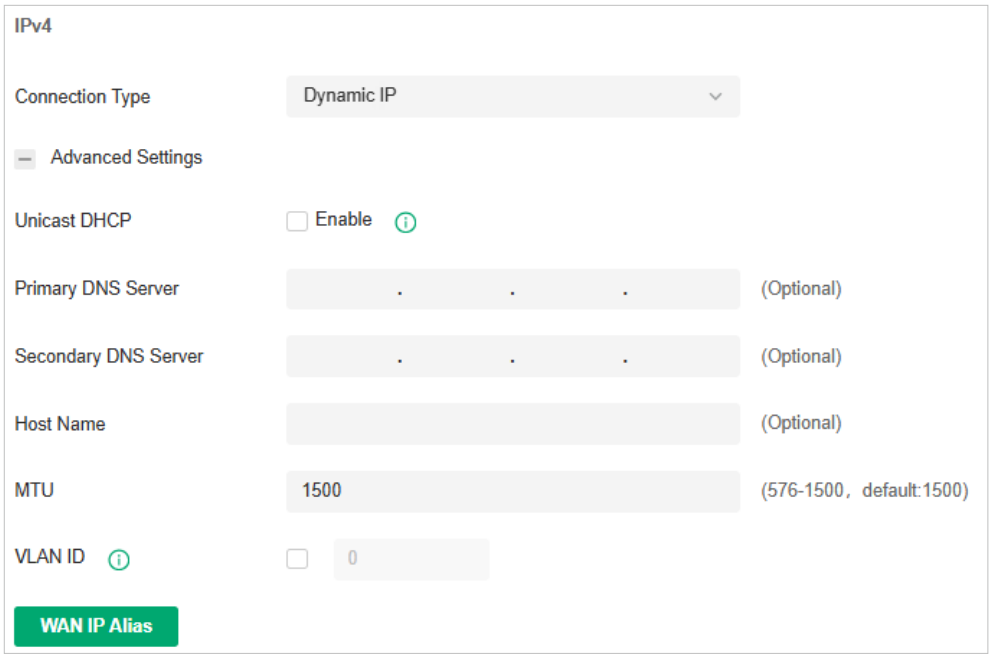
- Set Up IPv4 Connection

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports Config section, click the edit icon of a WAN port and configure the Connection Type according to the service provided by your ISP.

Connection Type	Dynamic IP: If your ISP automatically assigns the IP address and the corresponding parameters, choose Dynamic IP. Static IP: If your ISP provides you with a fixed IP address and the corresponding parameters, choose Static IP. PPPoE: If your ISP provides you with a PPPoE account, choose PPPoE. L2TP: If your ISP provides you with an L2TP account, choose L2TP. PPTP: If your ISP provides you with a PPTP account, choose PPTP.

- **Dynamic IP**

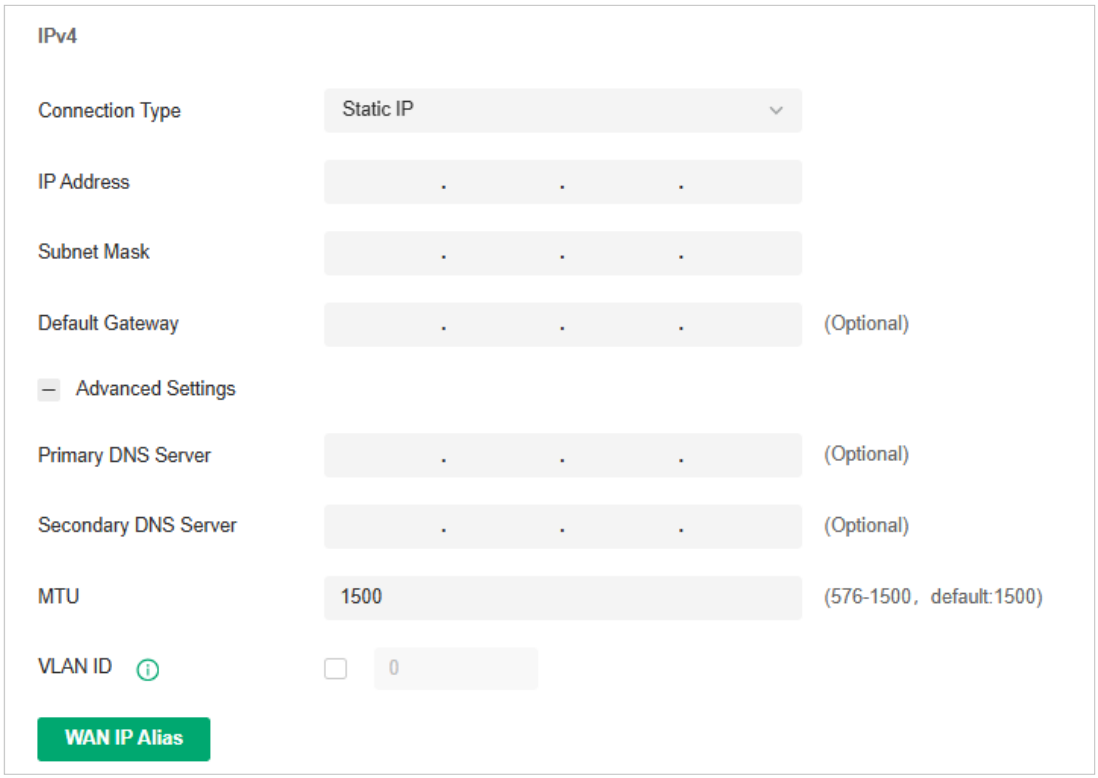
  Choose Connection Type as Dynamic IP and configure the parameters.



Unicast DHCP	With this option enabled, the gateway will require the DHCP server to assign the IP address by sending unicast DHCP packets. Usually you need not to enable the option.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
Host Name	Enter a name for the gateway.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is Dynamic IP, MTU can be set in the range of 576-1500 bytes. The default value is 1500.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 0 to 7. None means the packet will be forwarded without any operation.
WAN IP Alias	WAN IP Alias supports configuring multiple IP addresses on one WAN port, and these IP addresses can be used to configure virtual server and other functions.

- **Static IP**

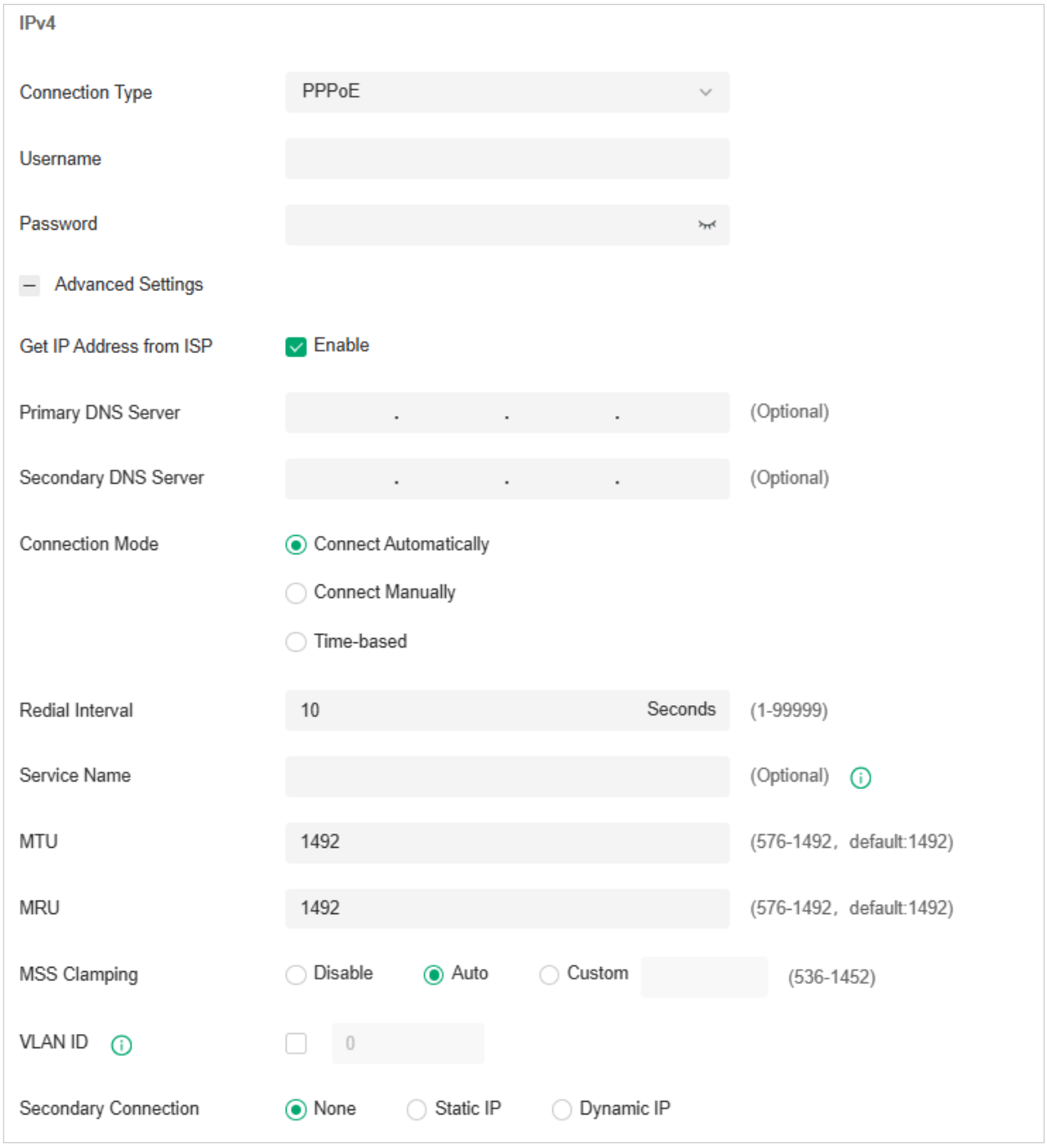
  Choose Connection Type as Static IP and configure the parameters.



IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is Static IP, MTU can be set in the range of 576-1500 bytes. The default value is 1500.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 0 to 7. None means the packet will be forwarded without any operation.
WAN IP Alias	WAN IP Alias supports configuring multiple IP addresses on one WAN port, and these IP addresses can be used to configure virtual server and other functions.

- **PPPoE**

  Choose Connection Type as PPPoE and configure the parameters.

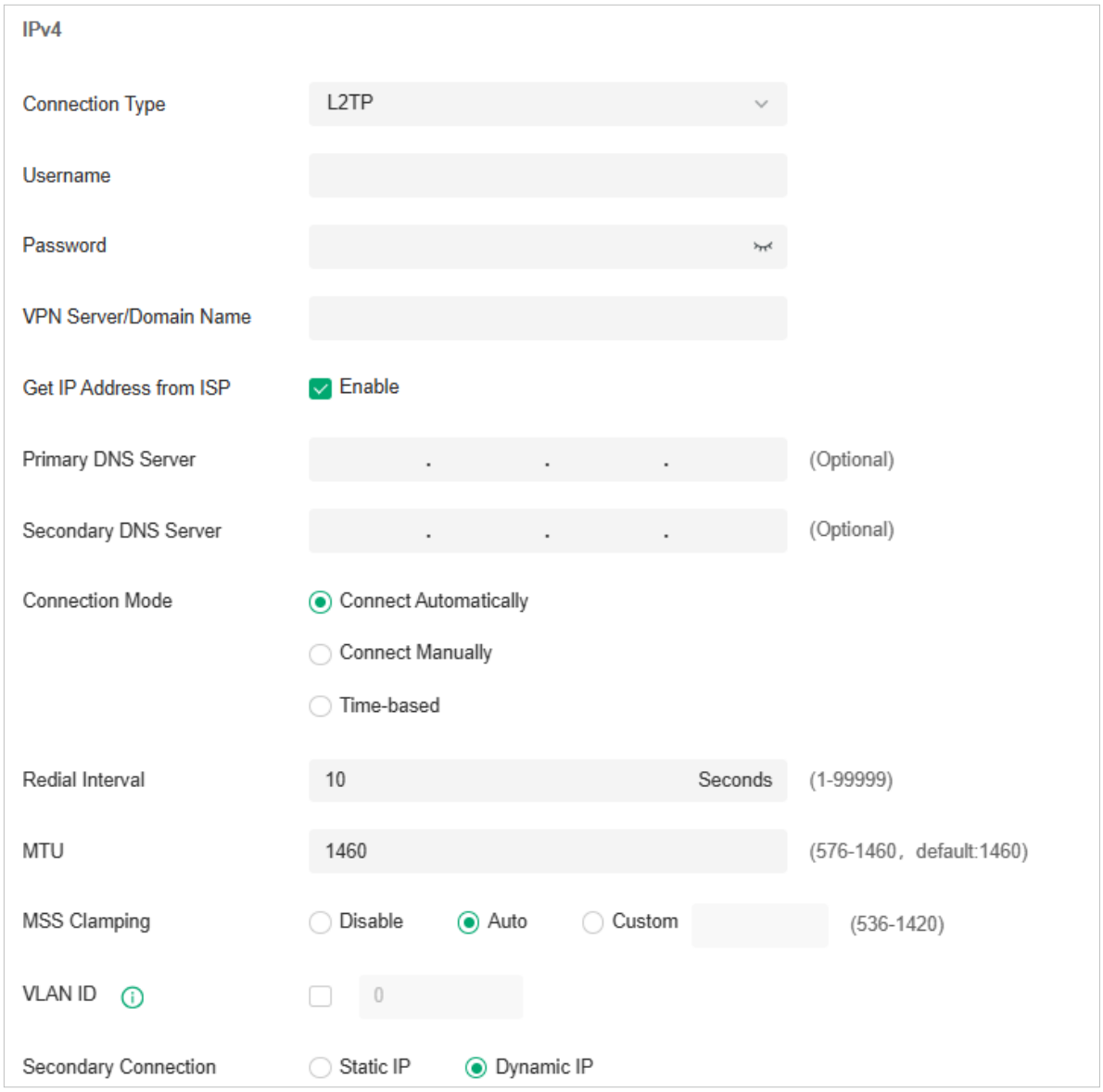


Username	Enter the PPPoE username provided by your ISP.
Password	Enter the PPPoE password provided by your ISP.
Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection. With this option disabled, you need to specify the IP Address provided by your ISP.

Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
Connection Mode	Connect Automatically: The gateway activates the connection automatically when the connection is down. You need to specify the Redial Interval, which decides how often the gateway tries to redial after the connection is down. Connect Manually: You can manually activate or terminate the connection. Time-Based: During the specified period, the gateway will automatically activate the connection. You need to specify the Time Range when the connection is up.
Service Name	Keep it blank unless your ISP requires you to configure it.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is PPPoE, MTU can be set in the range of 576-1492 bytes. The default value is 1492.
MRU	Specify the MRU (Maximum Receive Unit) of the WAN port. MRU is the maximum data unit transmitted in the Data link layer.
MSS Clamping	Specify the upper limit of the value of the MSS (Maximum Segment Size) field negotiated by the sending and receiving parties when establishing TCP connection to avoid IP fragmentation. If the value of the MSS field negotiated by the communication parties exceeds the specified value, the gateway will change the negotiated MSS field to the specified value Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties. Auto: Automatically calculate MSS value based on path MTU. Custom: Select this option to specify the MSS value. It should not exceed the MTU value.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 0 to 7. None means the packet will be forwarded without any operation.
Secondary Connection	Secondary connection is required by some ISPs. Select the connection type required by your ISP. None: Select this if the secondary connection is not required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address and Subnet Mask provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.

- **L2TP**

Choose Connection Type as L2TP and configure the parameters.

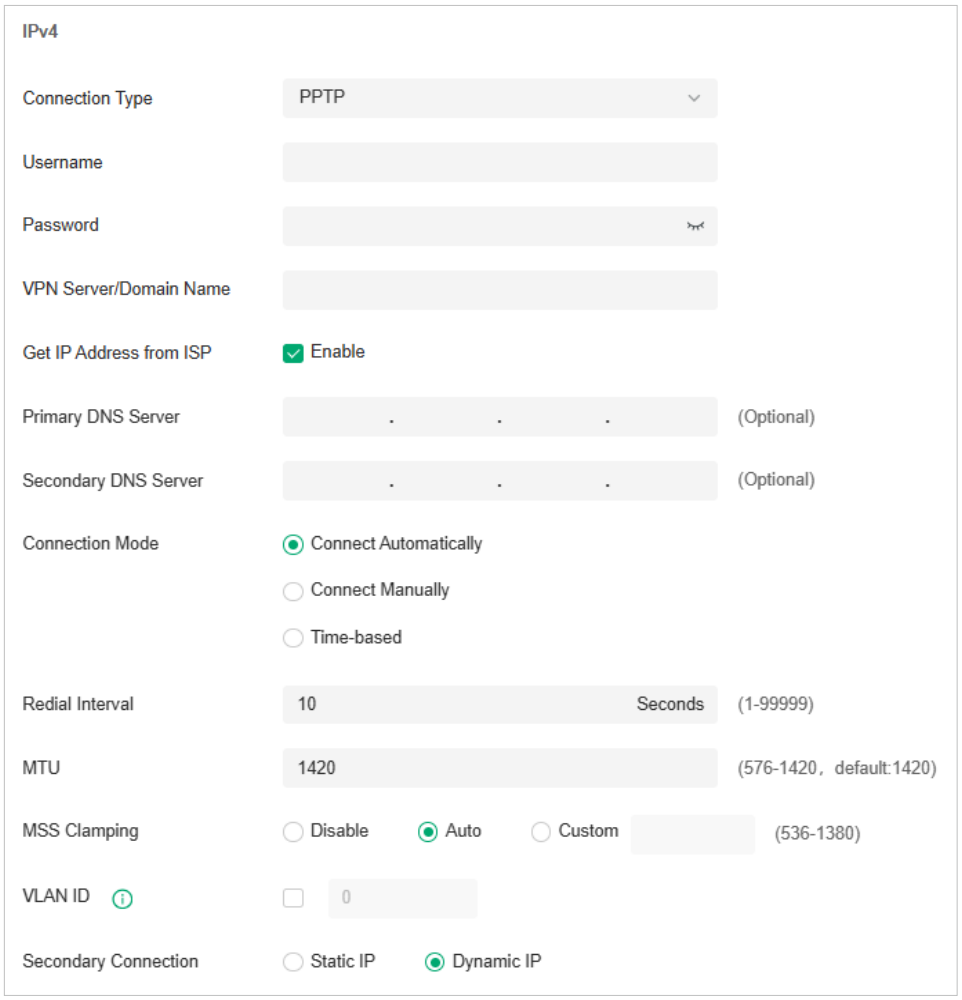


Username	Enter the L2TP username provided by your ISP.
Password	Enter the L2TP password provided by your ISP.
VPN Server / Domain Name	Enter the VPN Server/Domain Name provided by your ISP.
Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection. With this option disabled, you need to specify the IP address provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.

Connection Mode	Connect Automatically: The gateway activates the connection automatically when the connection is down. You need to specify the Redial Interval, which decides how often the gateway tries to redial after the connection is down. Connect Manually: You can manually activate or terminate the connection. Time-Based: During the specified period, the gateway will automatically activate the connection. You need to specify the Time Range when the connection is up.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is L2TP, MTU can be set in the range of 576-1460 bytes. The default value is 1460.
MSS Clamping	Specify the upper limit of the value of the MSS (Maximum Segment Size) field negotiated by the sending and receiving parties when establishing TCP connection to avoid IP fragmentation. If the value of the MSS field negotiated by the communication parties exceeds the specified value, the gateway will change the negotiated MSS field to the specified value Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties. Auto: Automatically calculate MSS value based on path MTU. Custom: Select this option to specify the MSS value. It should not exceed the MTU value.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 0 to 7. None means the packet will be forwarded without any operation.
Secondary Connection	Select the connection type required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address, Subnet Mask, Default Gateway (Optional), Primary DNS Server (Optional), and Secondary DNS Server (Optional) provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.

- **PPTP**

Choose Connection Type as PPTP and configure the parameters.



Username	Enter the PPTP username provided by your ISP.
Password	Enter the PPTP password provided by your ISP.
VPN Server / Domain Name	Enter the VPN Server/Domain Name provided by your ISP.
Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection. With this option disabled, you need to specify the IP address provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
Connection Mode	Connect Automatically: The gateway activates the connection automatically when the connection is down. You need to specify the Redial Interval, which decides how often the gateway tries to redial after the connection is down. Connect Manually: You can manually activate or terminate the connection. Time-Based: During the specified period, the gateway will automatically activate the connection. You need to specify the Time Range when the connection is up.

MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is PPTP, MTU can be set in the range of 576-1420 bytes. The default value is 1420.
MSS Clamping	Specify the upper limit of the value of the MSS (Maximum Segment Size) field negotiated by the sending and receiving parties when establishing TCP connection to avoid IP fragmentation. If the value of the MSS field negotiated by the communication parties exceeds the specified value, the gateway will change the negotiated MSS field to the specified value Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties. Auto: Automatically calculate MSS value based on path MTU. Custom: Select this option to specify the MSS value. It should not exceed the MTU value.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 0 to 7. None means the packet will be forwarded without any operation.
Secondary Connection	Select the connection type required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address, Subnet Mask, Default Gateway (Optional), Primary DNS Server (Optional), and Secondary DNS Server (Optional) provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.

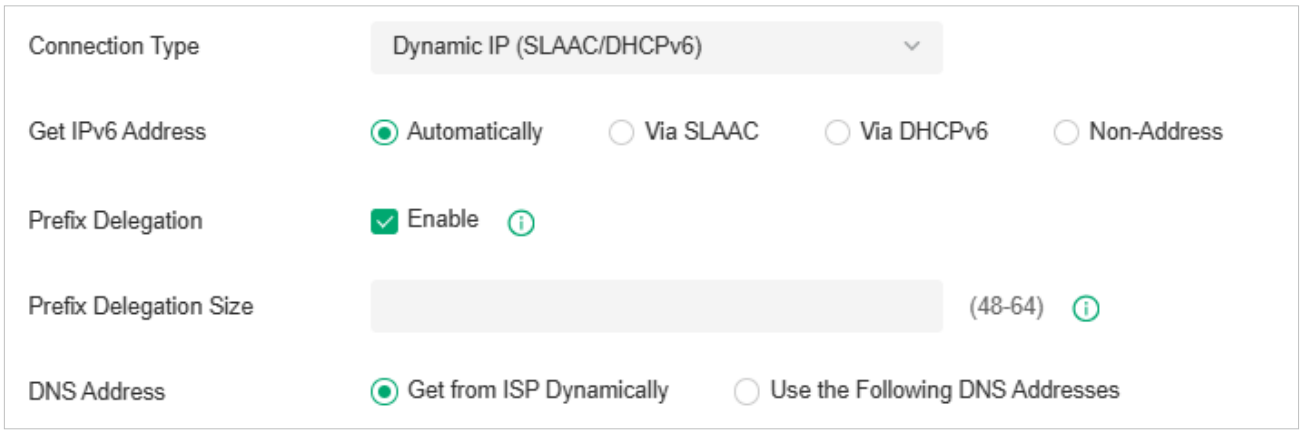
- Set Up IPv6 Connection

For IPv6 connections, check the box to enable the IPv6 connection, select the internet connection type according to the requirements of your ISP.

Connection Type	Dynamic IP (SLAAC/DHCPv6): If your ISP uses Dynamic IPv6 address assignment, either DHCPv6 or SLAAC+Stateless DHCP, select Dynamic IP (SLAAC/DHCPv6). Static IP: If your ISP provides you with a fixed IPv6 address, select Static IP. PPPoE: If your ISP uses PPPoEv6, and provides a username and password, select PPPoE. 6to4 Tunnel: If your ISP uses 6to4 deployment for assigning IPv6 address, select 6to4 Tunnel. 6to4 is an internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network. The IPv6 packet will be encapsulated in the IPv4 packet and transmitted to the IPv6 destination through IPv4 network. Pass-Through (Bridge): In Pass-Through (Bridge) mode, the gateway works as a transparent bridge. The IPv6 packets received from the WAN port will be transparently forwarded to the LAN port and vice versa. No extra parameter is required.

■ Dynamic IP (SLAAC/DHCPv6)

Choose Connection Type as Dynamic IP (SLAAC/DHCPv6) and configure the parameters.



Get IPv6 Address	Select the proper method whereby your ISP assigns IPv6 address to your gateway. Automatically: With this option selected, the gateway will automatically select SLAAC or DHCPv6 to get IPv6 addresses. Via SLAAC: With SLAAC (Stateless Address Auto-Configuration) selected, your ISP assigns the IPv6 address prefix to the gateway and the gateway automatically generates its own IPv6 address. Also, your ISP assigns other parameters including the DNS server address to the gateway. Via DHCPv6: With DHCPv6 selected, your ISP assigns an IPv6 address and other parameters including the DNS server address to the gateway using DHCPv6. Non-Address: With this option selected, the gateway will not get an IPv6 address.
Prefix Delegation	Select Enable to get an address prefix by DHCPv6 server from your ISP, or Disable to designate an address prefix for your LAN port manually. Clients in LAN will get an IPv6 address with this prefix.

Prefix Delegation Size	With Prefix Delegation enabled, enter the Prefix Delegation Size to determine the length of the address prefix. If you are not sure about the value, you can ask your ISP.
DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

- **Static IP**

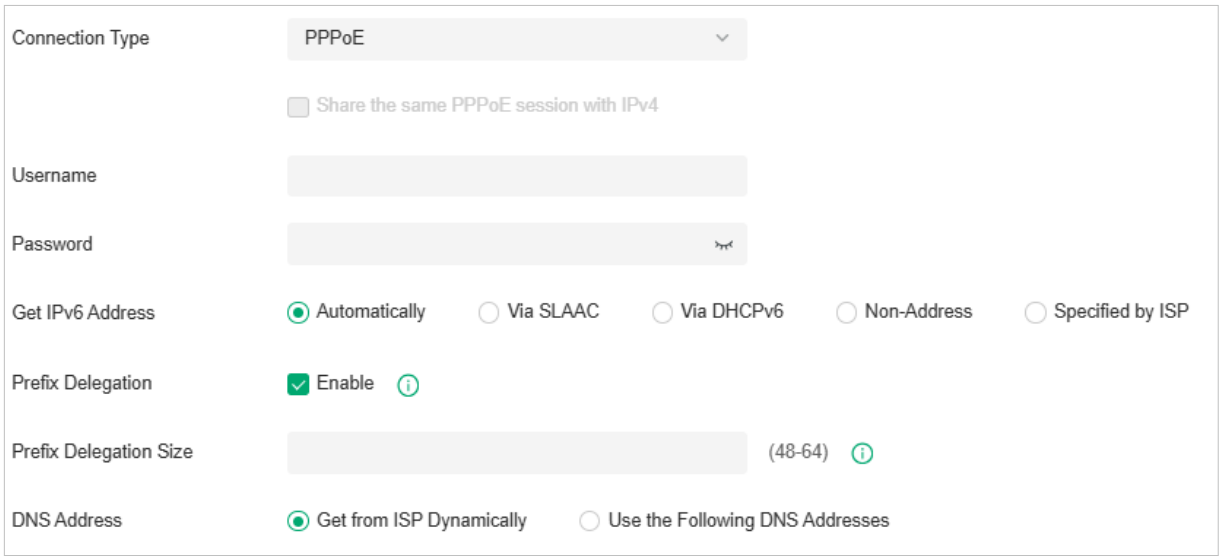
Choose Connection Type as Static IP and configure the parameters.



IPv6 Address	Enter the static IPv6 address information received from your ISP.
Prefix Length	Enter the prefix length of the IPv6 address received from your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

- **PPPoE**

Choose Connection Type as PPPoE and configure the following parameters. Then click Apply.

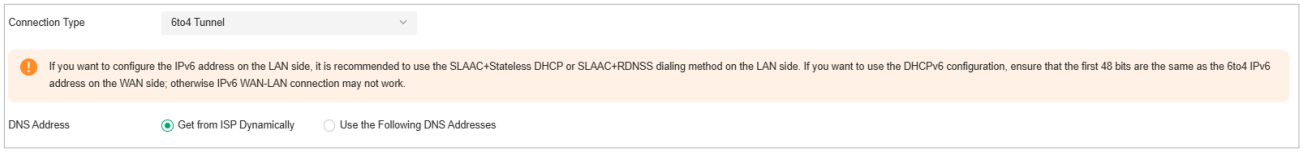


Share the same PPPoE session with IPv4	If your ISP provides only one PPPoE account for both IPv4 and IPv6 connections, and you have already established an IPv4 connection on this WAN port, you can check the box, then the WAN port will use the PPP session of IPv4 PPPoE connection to get the IPv6 address. In this case, you do not need to enter the username and password of the PPPoE account. If your ISP provides two separate PPPoE accounts for the IPv4 and IPv6 connections, or the IPv4 connection of this WAN port is not based on PPPoE, do not check the box and manually enter the username and password for the IPv6 connection.
Username	Enter the username of your PPPoE account provided by your ISP.
Password	Enter the password of your PPPoE account provided by your ISP.
Get IPv6 Address	Select the proper method whereby your ISP assigns IPv6 address to your gateway. Automatically: With this option selected, the gateway will automatically select the method to get IPv6 addresses between SLAAC and DHCPv6. Via SLAAC: With SLAAC (Stateless Address Auto-Configuration) selected, your ISP assigns the IPv6 address prefix to the gateway and the gateway automatically generates its own IPv6 address. Also, your ISP assigns other parameters including the DNS server address to the gateway. Via DHCPv6: With DHCPv6 selected, your ISP assigns an IPv6 address and other parameters including the DNS server address to the gateway using DHCPv6. Non-Address: With this option selected, the gateway will not get an IPv6 address. Specified by ISP: With this option selected, enter the IPv6 address you get from your ISP.
Prefix Delegation	Select Enable to get an address prefix by DHCPv6 server from your ISP, or Disable to designate an address prefix for your LAN port manually. Clients in LAN will get an IPv6 address with this prefix.
Prefix Delegation Size	With Prefix Delegation enabled, enter the Prefix Delegation Size to determine the length of the address prefix. If you are not sure about the value, you can ask your ISP.

DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

- **6to4 Tunnel**

  Choose Connection Type as 6to4 Tunnel and configure the parameters.



DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

- **Pass-Through (Bridge)**

  Choose Connection Type as Pass-Through (Bridge) and no configuration is required for this type of connection.



- Set Up MAC Address

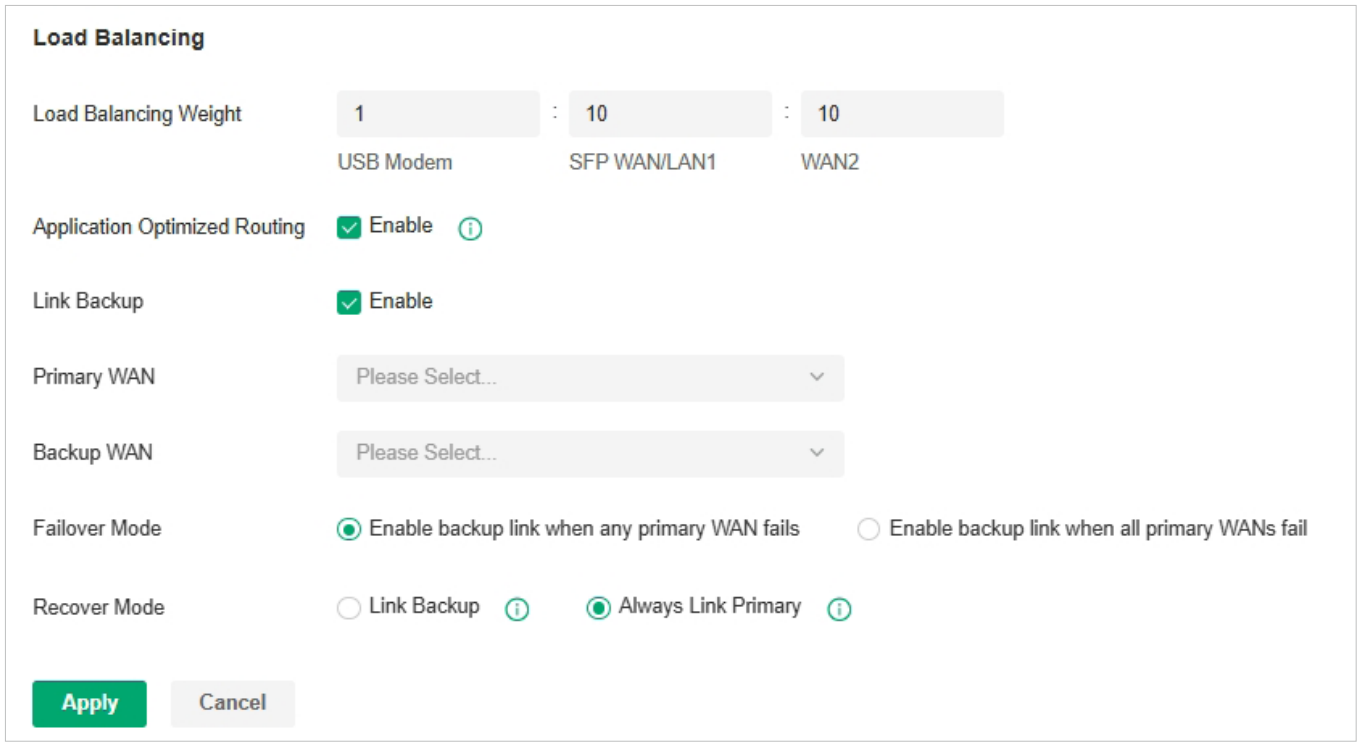
Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports Config section, click the edit icon of a WAN port and configure the MAC address according to actual needs.

MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need to specify the MAC address. Typically, this is required when your ISP bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

Step 3: (Optional) Configure Load Balancing

Note: Loading Balancing is only available when you configure more than one WAN port.

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In Load Balancing, configure the following parameters and click Apply.



Load Balancing Weight	Specify the ratio of network traffic that each WAN port carries.
Application Optimized Routing	With Application Optimized Routing enabled, the router will consider the source IP address and destination IP address (or destination port) of the packets as a whole and record the WAN port they pass through. Then the packets with the same source IP address and destination IP address (or destination port) will be forwarded to the recorded WAN port. This feature ensures that multi-connected applications work properly.
Link Backup	With Link Backup enabled, the router will switch all the new sessions from dropped lines automatically to another to keep an always on-line network.
Backup WAN / Primary WAN	The backup WAN port backs up the traffic for the primary WAN ports under the specified condition.
Failover Mode	Select whether to enable backup link when any primary WAN fails or all primary WANs fail.
Recover Mode	Link Backup: The system will switch all the new sessions from dropped line automatically to another to keep an always on-link network. Always Link Primary: Traffic is always forwarded through the primary WAN port unless it fails. The system will try to forward the traffic via the backup WAN port when it fails, and switch back when it recovers.

4. 2. 2 Configure LAN Networks

Overview

The **LAN** function allows you to configure wired internal network. Based on 802.1Q VLAN, the Controller provides a convenient and flexible way to separate and deploy the network. The network can be logically segmented by departments, application, or types of users, without regard to geographic locations.

Configuration

To create a LAN, follow the guidelines:

1) Create a Network with specific purpose. For Layer 2 isolation, create a network as **VLAN.** To realize inter-VLAN routing, create a network as **Interface**, which is configured with a VLAN interface.

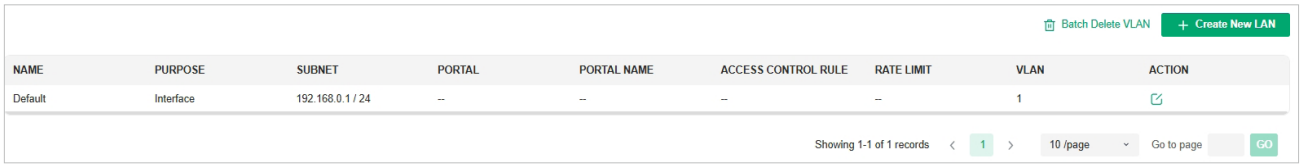
2) Create a port profile for the network. The profile defines how the packets in both ingress and egress directions are handled.

3) Assign the port profile to the desired ports of the switch to activate the LAN.

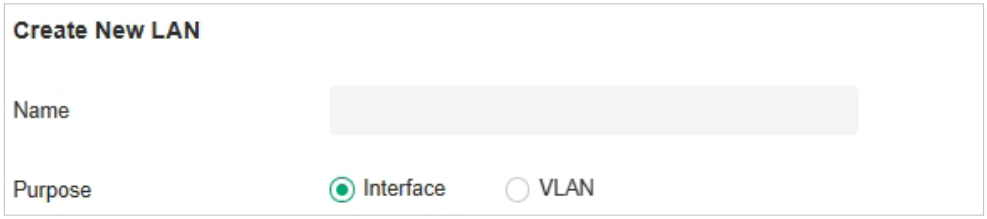
Step 1: Create a Network

Note: A default Network (default VLAN) named LAN is preconfigured as Interface and is associated with all LAN ports of the Gateway and all switch ports. The VLAN ID of the default Network is 1. The default Network can be edited, but not deleted.

1. Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > LAN to load the following page.



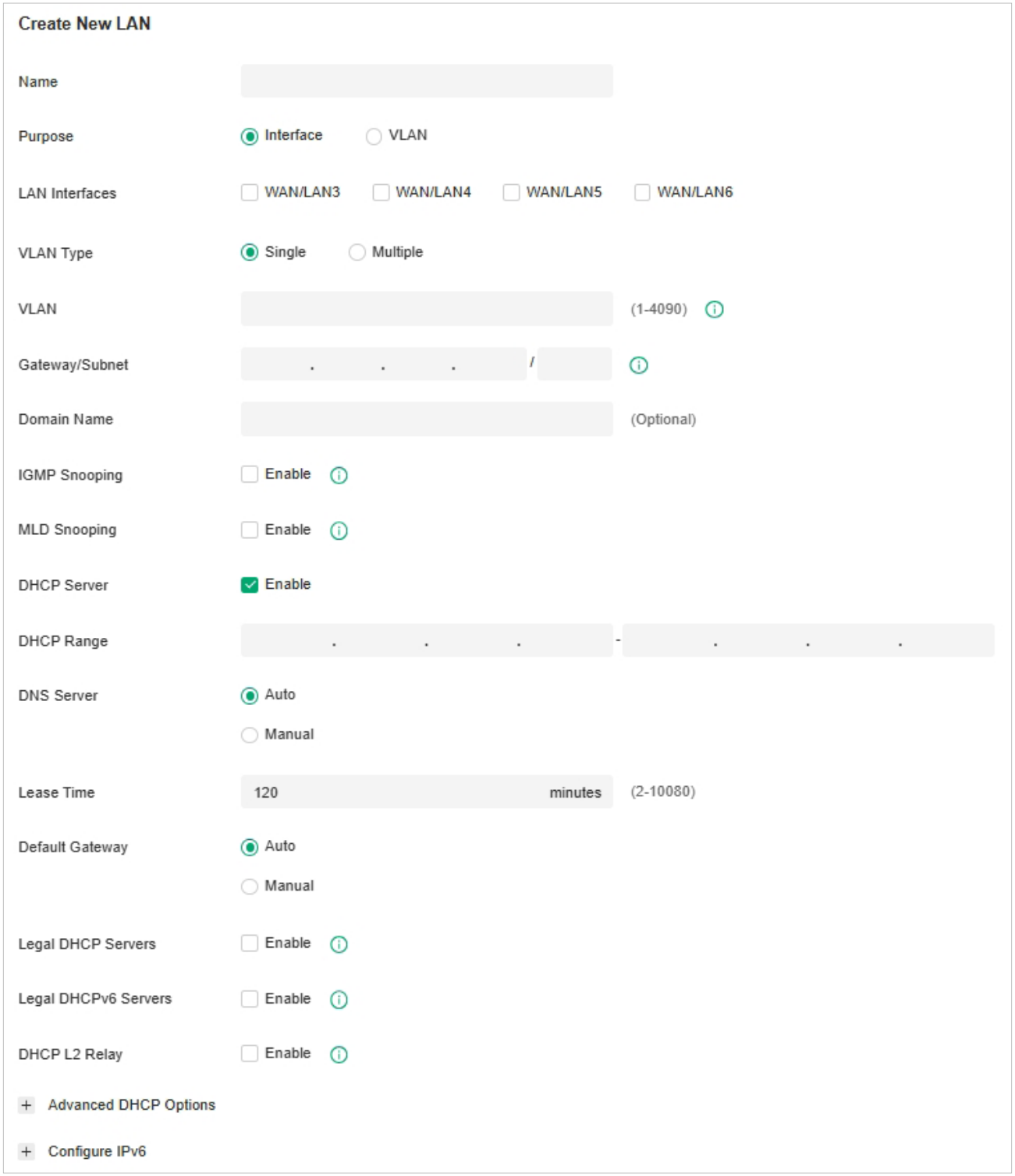
2. Click Create New LAN to load the following page, enter a name to identify the network, and select the purpose for the network.



Purpose	Interface: Create the network with a Layer 3 interface, which is required for inter-VLAN routing. VLAN: Create the network as a Layer 2 VLAN.

3. Configure the parameters according to the purpose for the network.

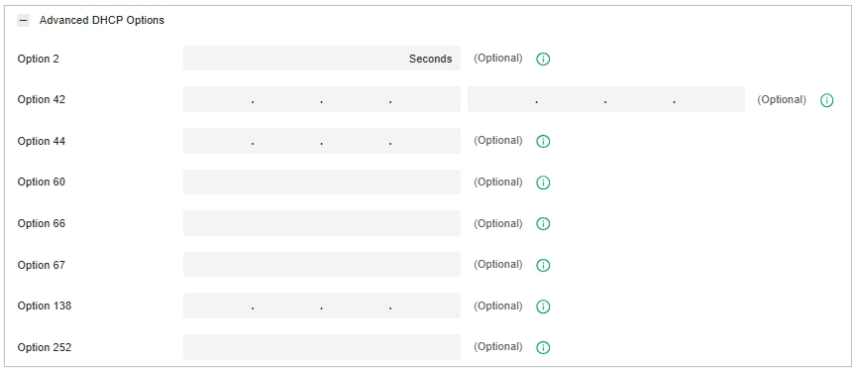
■ Interface



LAN Interface	Select the physical interfaces of the Gateway that this network will be associated with.
VLAN	Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.

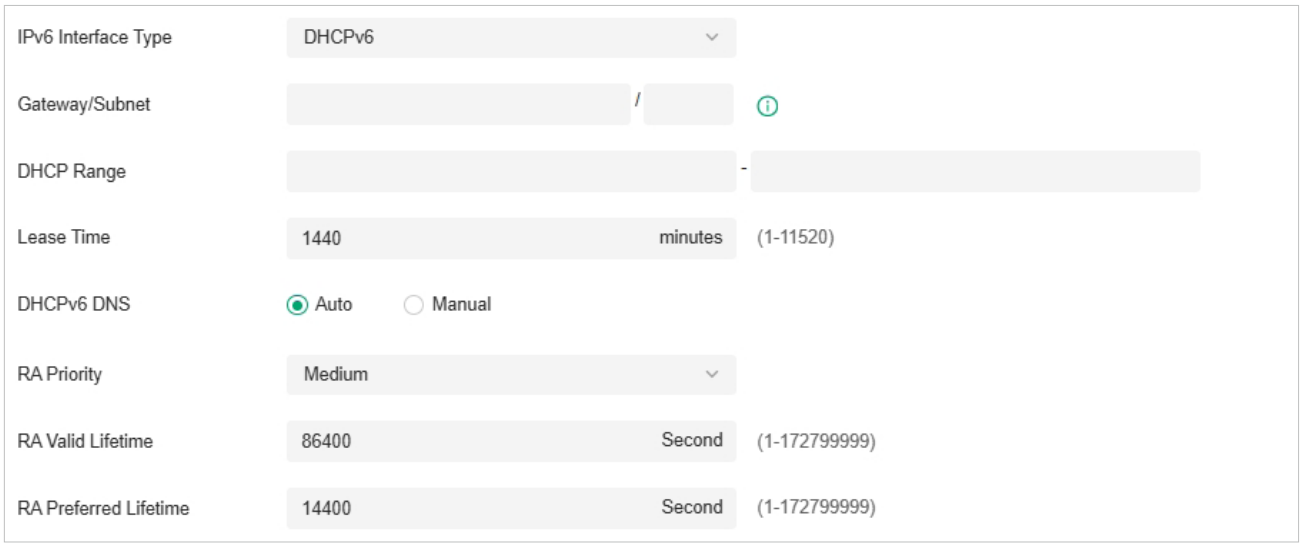
Gateway/Subnet	Enter the IP address and subnet mask in the CIDR format. The CIDR Notation here includes the IP address and subnet mask of the default gateway. The summary of the information that you entered will show up below in real time.
Domain Name	Enter the domain name.
IGMP Snooping	Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
MLD Snooping	Click the checkbox to monitor MLD (Multicast Listener Discovery) traffic and thereby manage IPv6 multicast traffic.
DHCP Server	Click the checkbox to allow the Gateway to serve as the DHCP server for this network. A DHCP server assigns IP addresses, DNS server, default gateway, and other parameters to all devices in the network. Deselect the box if there is already a DHCP server in the network.
DHCP Range	Enter the starting and ending IP addresses of the DHCP address pool in the fields provided. For quick operation, click the Update DHCP Range beside the Gateway/Subnet entry to get the IP address range populated automatically, and edit the range according to your needs.
DNS Server	Select a method to configure the DNS server for the network. Auto: The DHCP server automatically assigns DNS server for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the DNS server address. Manual: Specify DNS servers manually. Enter the IP address of a server in each DNS server field.
Lease TIme	Specify how long a client can use the IP address assigned from this address pool.
Default Gateway	Enter the IP address of the default gateway. Auto: The DHCP server automatically assigns default gateway for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the default gateway address. Manual: Specify default gateway manually. Enter the IP address of the default gateway in the field.
Legal DHCP Servers	Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here.
Legal DHCPv6 Servers	Click the checkbox to specify legal DHCPv6 servers for the network. With legal DHCPv6 servers configured, Gateways and Switches ensure that clients get IPv6 addresses only from the DHCPv6 servers specified here.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.

You can expand and configure Advanced DHCP Options if needed.



Option 2	DHCP clients use DHCP option 2 to configure the time offset. The time offset field specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Option 42	DHCP clients use DHCP option 42 to configure the NTP server address.
Option 44	DHCP clients use DHCP option 44 to configure the NetBIOS over TCP/IP name server.
Option 60	Enter the value for DHCP Option 60. DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs.
Option 66	Enter the value for DHCP Option 66. It specifies the TFTP server information and supports a single TFTP server IP address.
Option 67	Option 67 tells the client a path to a file from a TFTP server (option 66) that will be retrieved and used to boot. That file needs to be a basic boot loader that will do any other required work.
Option 138	Enter the value for DHCP Option 138. It is used in discovering the devices by the controller.
Option 252	Option 252 provides a DHCP client a URL to use to configure its proxy settings. It's defined in draft-ietf-wrec-wpad-01. If it was a statement like 'wpad-proxy-url' then only systems that understood it could use it (they'd have to recognize that string and know how to handle it)

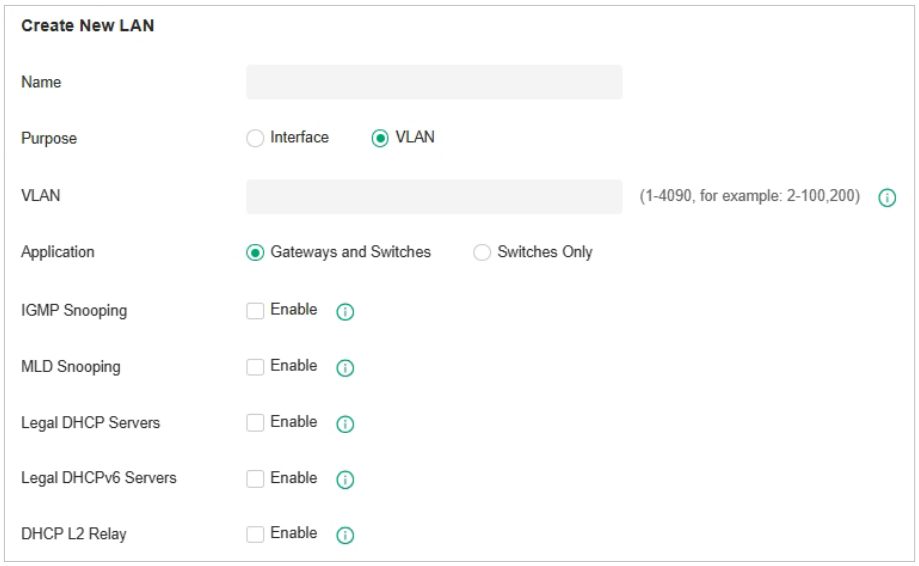
You can expand and configure IPv6 connections for the LAN clients if needed. First, determine the method whereby the gateway assigns IPv6 addresses to the clients in the local network. Some clients may support only a few of these connection types, so you should choose it according to the compatibility of clients in the local network.



IPv6 Interface Type	Configure the type of assigning IPv6 address to the clients in the local network. None: IPv6 connection is not enabled for the clients in the local network. DHCPv6: The gateway assigns an IPv6 address and other parameters including the DNS server address to each client using DHCPv6. SLAAC+Stateless DHCP: The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using DHCPv6. SLAAC+RDNSS: The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using the RDNSS option in RA (Router Advertisement). Pass-Through: Select this type if the WAN ports of the gateway use the Pass-Through for IPv6 connections.
With DHCPv6 selected, configure the following parameters.	
Gateway/Subnet	Enter the IP address and subnet mask in the CIDR format. The CIDR notation here includes the IP address and subnet mask of the default gateway. The summary of the information that you entered will show up below in real time.
DHCP Range	Enter the starting and ending IP addresses of the DHCP address pool in the fields provided. For quick operation, click the Update DHCP Range beside the Gateway/Subnet entry to get the IP address range populated automatically, and edit the range according to your needs.
Lease Time	This entry determines how long the assigned IPv6 address remains valid. Either keep the default 1440 minutes or change it if required by your ISP.
DHCPv6 DNS	Select a method to configure the DNS server for the network. With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. With Manual selected, enter the IP address of a server in each DNS server field.

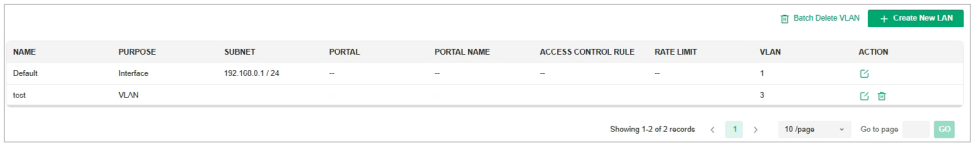
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.
With SLAAC+Stateless DHCP selected, configure the following parameters.	
Prefix	Configure the IPv6 address prefix for each client in the local network. Manual Prefix: With Manual Prefix selected, enter the prefix in the Address Prefix field. Get from Prefix Delegation: With Get from Prefix Delegation selected, select the WAN port with Prefix Delegation configured, and the clients will get the address prefix from the Prefix Delegation.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be added to the prefix to obtain a /64 subnet. The range of IPv6 Prefix ID is determined by the larger value of Prefix Delegation Size and Prefix Delegation Length (obtained from the ISP). Note that if the Prefix Delegation Length is larger than 64, the IPv6 Prefix ID cannot be obtained from Prefix Delegation, please select another method. In site view, go to Settings > Wired Network > Internet to configure Prefix Delegation Size.
DNS Server	Select a method to configure the DNS server for the network. Auto: With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. Manual: With Manual selected, enter the IP address of a server in each DNS server field.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.

With SLAAC+RDNSS selected, configure the following parameters.	
Prefix	Configure the IPv6 address prefix for each client in the local network. Manual Prefix: With Manual Prefix selected, enter the prefix in the Address Prefix field. Get from Prefix Delegation: With Get from Prefix Delegation selected, select the WAN port with Prefix Delegation configured, and the clients will get the address prefix from the Prefix Delegation.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be added to the prefix to obtain a /64 subnet.
DNS Server	Select a method to configure the DNS server for the network. Auto: With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. Manual: With Manual selected, enter the IP address of a server in each DNS server field.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.
With Pass-Through selected, configure the following parameters.	
IPv6 Prefix Delegation Interface	Select the WAN port using Pass-Through (Bridge) for the IPv6 connection.



VLAN	Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.
Application	Choose the device type that this entry applies to.
IGMP Snooping	Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
MLD Snooping	Click the checkbox to monitor MLD (Multicast Listener Discovery) traffic and thereby manage IPv6 multicast traffic.
Legal DHCP Servers	Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here.
Legal DHCPv6 Servers	Click the checkbox to specify legal DHCPv6 servers for the network. With legal DHCPv6 servers configured, Gateways and Switches ensure that clients get IPv6 addresses only from the DHCPv6 servers specified here.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.

4. Click Save. The new LAN will be added to the LAN list. In the ACTION column, you can click to edit the LAN and click the Delete icon to delete the LAN. You can click Batch Delete VLANs to delete VLANs.



Step 2: Create a Port Profile

Note:

- Three default port profiles are preconfigured on the controller. They can be viewed, but not edited or deleted.

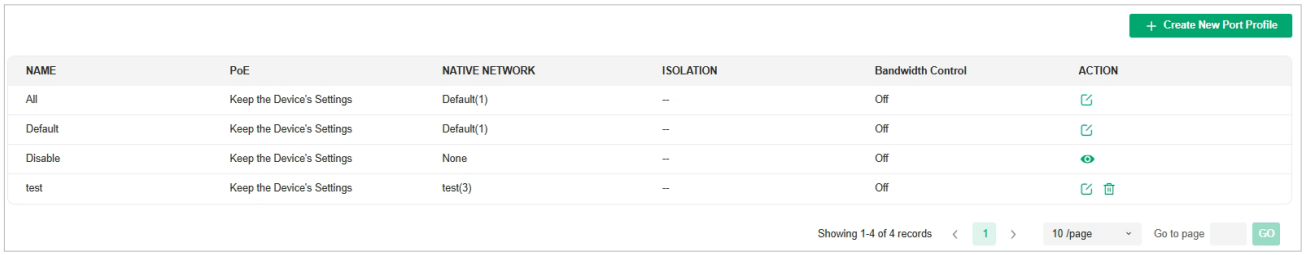
All: In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN). This profile is assigned to all switch ports by default.

Disable: In the Disable profile, no networks are configured as the native network, Tagged Networks and Untagged Networks. With this profile assigned to a port, the port does not belong to any VLAN.

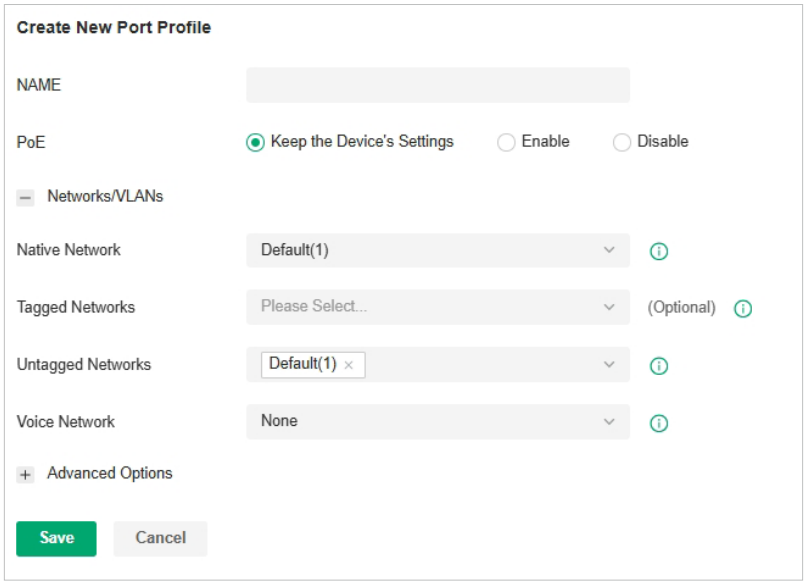
LAN: In the LAN profile, the native network is the default network (LAN), and no networks are configured as Tagged Networks and Untagged Networks.

- When a network is created, the system will automatically create a profile with the same name and configure the network as the native network for the profile. In this profile, the network itself is configured as the Untagged Networks, while no networks are configured as Tagged Networks. The profile can be viewed and deleted, but not edited.

1. Go to Settings > Wired&Wireless Networks > LAN > Switch Profile to load the following page.



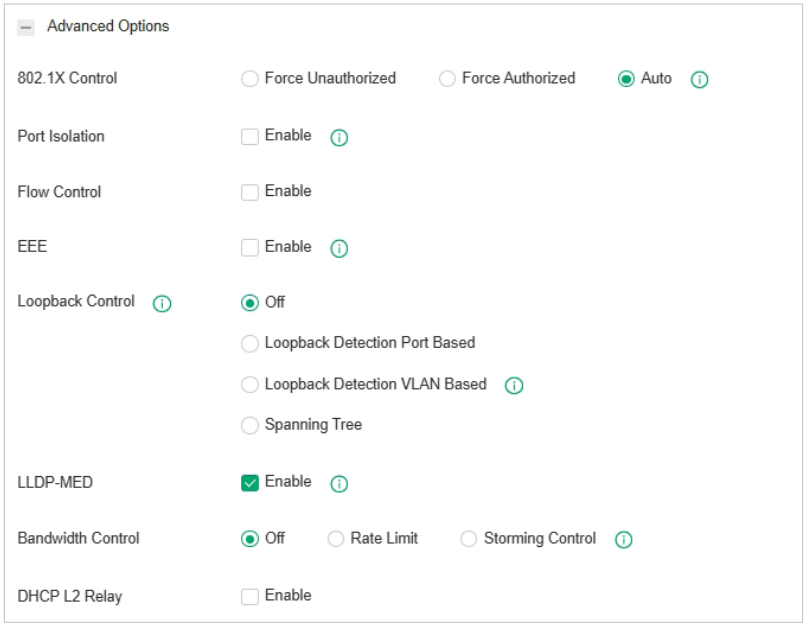
2. Click Create New Port Profile to load the following page, and configure the following parameters.



Name	Enter a name to identify the port profile.
PoE	Select the PoE mode for the ports. Keep the Device's Settings: PoE keep enabled or disabled according to the switches' settings. By default, the switches enable PoE on all PoE ports. Enable: Enable PoE on PoE ports. Disable: Disable PoE on PoE ports.

Native Network	Select the native network from all networks. The native network determines the Port VLAN Identifier (PVID) for switch ports. When a port receives an untagged frame, the switch inserts a VLAN tag to the frame based on the PVID, and forwards the frame in the native network. Each physical switch port can have multiple networks attached, but only one of them can be native.
Tagged Networks	Select the Tagged Networks. Frames sent out of a Tagged Network are kept with VLAN tags. Usually networks that connect the switch to network devices like routers and other switches, or VoIP devices like IP phones should be configured as Tagged Networks.
Untagged Networks	Select the Untagged Networks. Frames that sent out of an Untagged Network are stripped of VLAN tags. Usually networks that connect the switch to endpoint devices like computers should be configured as Untagged Networks. Note that the native network is untagged.
Voice Network	Select the network that connects VoIP devices like IP phones as the Voice Network. Switches will prioritize the voice traffic by changing its 802.1p priority. To configure a network as Voice Network, configure it as Tagged Network first, and then enable LLDP-MED. Only tagged networks can be configured as Voice Network, and Voice Network will take effect with LLDP-MED enabled.

3. Expand and configure Advanced Options if needed.

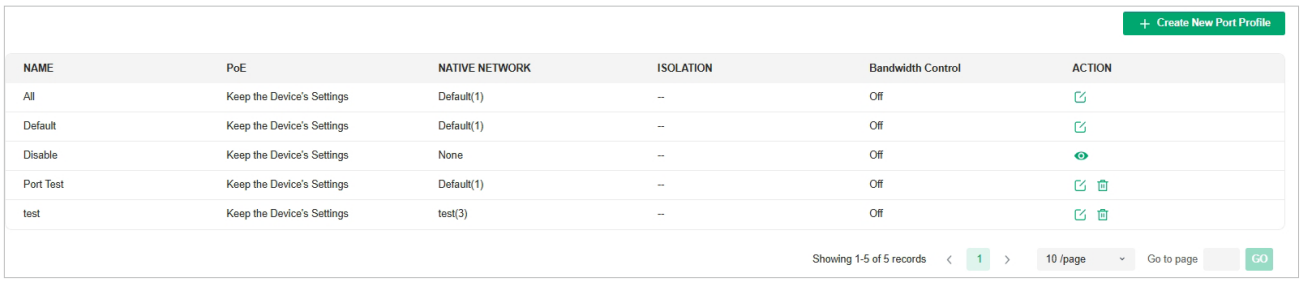


802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, enter the site view and go to **Settings** > **Authentication** > **802.1X**. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the current port will be removed from the VLAN. Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. If you want to enable Spanning Tree for the switch, you also need to select the Spanning Tree protocol in the Device Config page. For details, refer to 6. 3 Configure and Monitor Switches.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP devices.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the set rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	When Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.

Multicast Threshold	When Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
UL-Frame Threshold	When Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations..
Action	When Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.
Format	Select the format of option 82 sub-option value field. Normal: The format of sub-option value field is TLV (type-length-value). Private: The format of sub-option value field is just value.

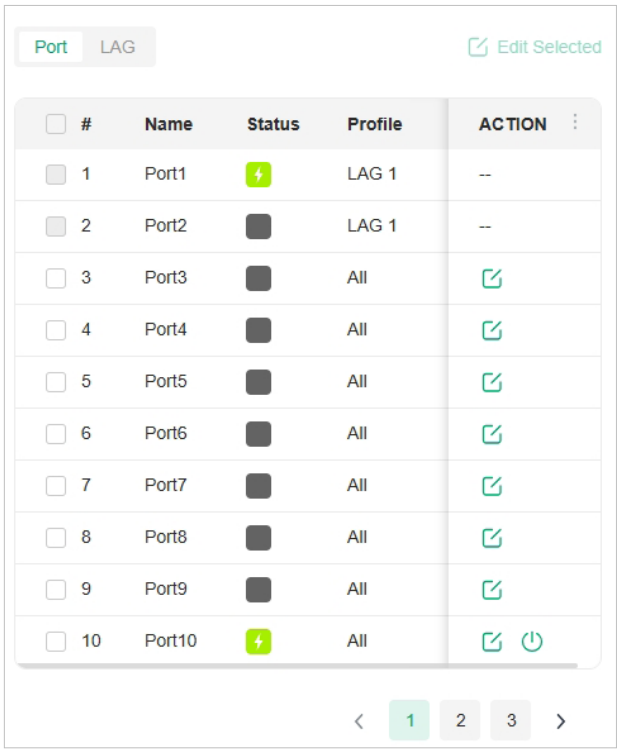
5. Click Save. The new port profile is added to the profile list. You can click Edit button in the ACTION icon to edit the port profile. You can click the Delete icon in the ACTION column to delete the port profile.



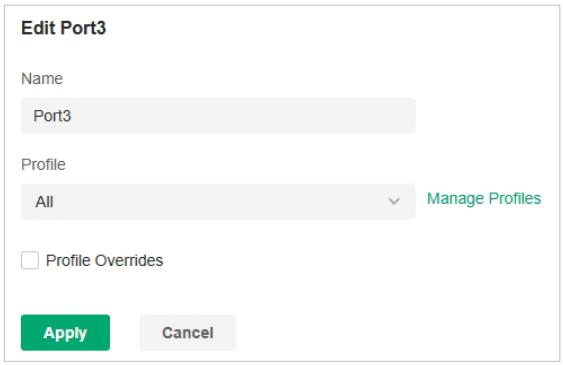
Step 3: Assign the Port Profile to the Ports

Note: By default, there is a port profile named All, which is assigned to all switch ports by default. In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN).

1. Go to Devices, and click the switch in the devices list to reveal the Properties window. Go to Ports, you can either click the Edit button in the Action column to assign the port profile to a single port, or select the desired ports and click Edit Selected on the top to assign the port profile to multiple ports in batch.

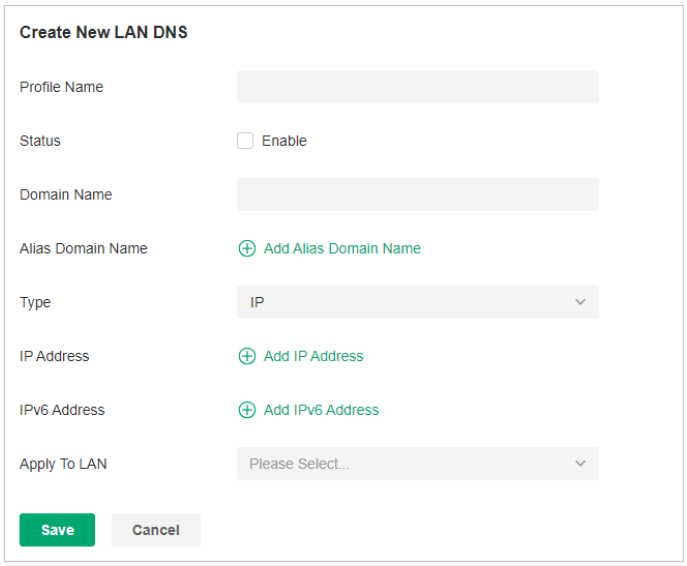


2. Select the profile from the drop-down list to assign the port profile to the desired ports of the switch. You can enable profile overrides to customize the settings for the ports, and all the configuration here overrides the port profile. For details, refer to Chapter 6. Configure and Monitor Controller-Managed Devices.



4. 2. 3 Configure LAN DNS

1. Launch the controller and access a site.
2. Go to Settings > Wired&Wireless Networks > LAN > LAN DNS.
3. Click Create New LAN DNS to load the following page, set the parameters, and save the settings.



Profile Name	Specify the name of the profile.
Status	Whether to enable this entry.
Domain Name	Enter the domain name.
Alias Domain Name	If a server provides different services and has multiple domain names, you can enter them here.
Type	There are three options, IP, CNAME, and FORWARD. IP: When selected, the gateway will respond to the DNS query of the specified domain name, and use the configured IP address as the DNS response to directly reply to the LAN host. Select this type when there is a web server in the intranet and you want hosts in the LAN to access the web server through private IP addresses instead of public IP addresses. CNAME: When selected, the gateway will map the domain name to the configured CNAME domain name, send it to the DNS server for query, and then reply to the LAN host with the IP corresponding to the CNAME domain name. FORWARD: When selected, the gateway will forward the DNS query of the LAN host to the specified DNS server, and reply the DNS response to the LAN host. The forwarding priority is higher than other public configurations, such as the DNS Server configured on the WAN port.
IP Address	When the Type is IP, it is the IPv4 address of the returned DNS response.
IPv6 Address	When the Type is IP, it is the IPv6 address of the returned DNS response.
Apply To LAN	When the Type is IP or CNAME, it is the LAN network to which the rule applies. You can choose to apply all LANs or apply to a single LAN or multiple LANs.
CNAME	When Type is CNAME, set the domain name to which Domain Name and Alias Domain Name need to be mapped.
DNS Server	When the Type is FORWARD, set the Domain Name and Alias Domain Name to be forwarded to a specific DNS Server, up to two DNS Servers can be configured.

4. 3 Configure Wireless Networks

Wireless networks enable your wireless clients to access the internet. Once you set up a wireless network, your APs typically broadcast the network name (SSID) in the air, through which your wireless clients connect to the wireless network and access the internet.

A WLAN group is a combination of wireless networks. Configure each group so that you can flexibly apply these groups of wireless networks to different APs according to your needs.

After setting up basic wireless networks, you can further configure WLAN Schedule, 802.11 Rate Control, MAC Filter, and other advanced settings.

4. 3. 1 Set Up Basic Wireless Networks

Configuration

To create, configure and apply wireless networks, follow these steps:

1) Create a WLAN group.

2) Create Wireless Networks

3) Apply the WLAN group to your APs

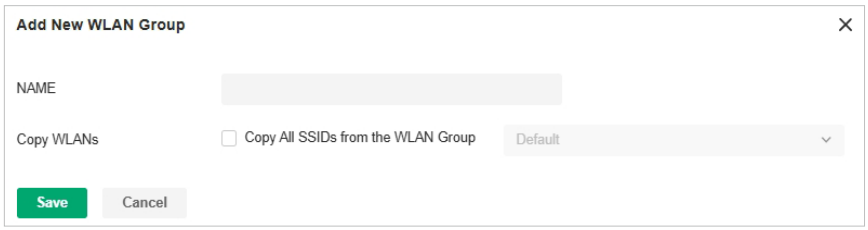
Step 1: Create a WLAN Group

Note: The controller provides a default WLAN group. If you simply want to configure wireless networks for the default WLAN group and apply it to all your APs, skip this step.

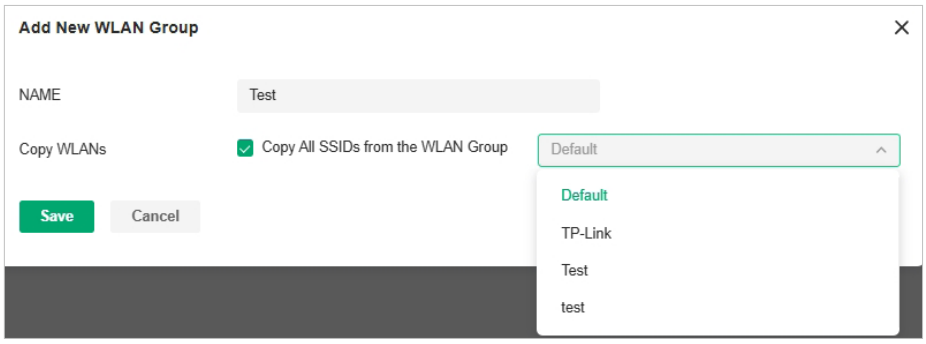
1. Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN to load the following page.



2. Select Create New Group from the drop-down list of WLAN Group to load the following page. Enter a name to identify the WLAN group.



3. (Optional) If you want to create a new WLAN group based on an existing one, check Copy All SSIDs from the WLAN Group and select the desired WLAN group. Then you can further configure wireless networks based on current settings.



4. Click Save. The new WLAN Group is added to the WLAN Group list. You can select a WLAN Group from the list to further create and configure its wireless networks. You can click the Edit icon to edit the name of the WLAN Group. You can click the Delete icon to delete the WLAN Group.



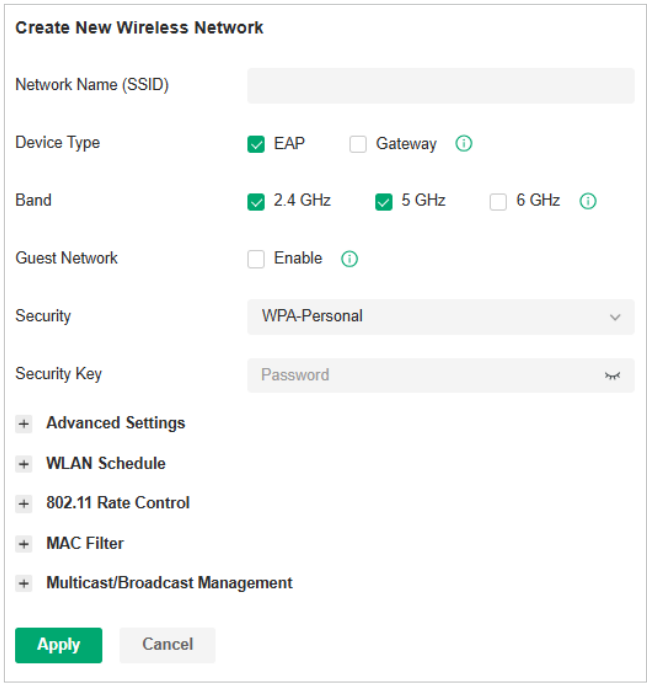
Step 2: Create Wireless Network

1. Select the WLAN group for which you want to configure wireless networks from the drop-down list of WLAN Group.



2. Click Create New Wireless Network to load the following page. Configure the basic parameters for the network.

Note: The 6 GHz band is only available for certain devices.

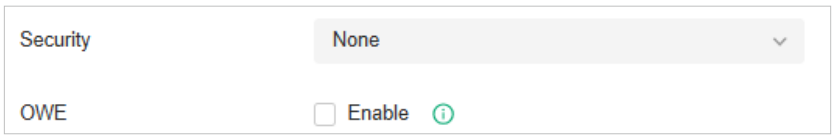


Network Name (SSID)	Enter the network name (SSID) to identify the wireless network. The users of wireless clients choose to connect to the wireless network according to the SSID, which appears on the WLAN settings page of wireless clients.
Device Type	Select the type of devices that the wireless network can apply to.
Band	Enable the radio band(s) for the wireless network. When 6GHz is turned on, Security cannot be PPSK with/without RADIUS since 6GHz does not support them.
Guest Network	With Guest Network enabled, all the clients connecting to the SSID are blocked from reaching any private IP subnet.
Security	Select the encryption method for the wireless network based on needs.

3. Select the security strategy for the wireless network.

- **None**

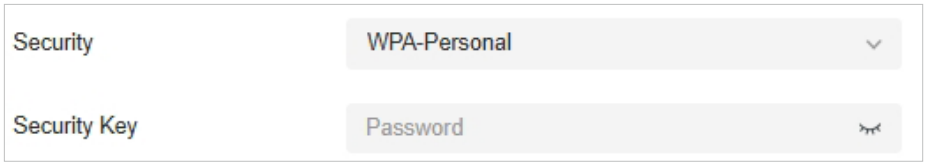
  With None selected, the hosts can access the wireless network without authentication, which is applicable to lower security requirements.



OWE	Opportunistic Wireless Encryption, also known as Enhanced Open, is a certification provided by the Wi-Fi Alliance as part of the WPA3 wireless security standard. OWE will enable two wireless VAPs per radio, one for access of OWE-supported stations, and one for access of other stations. An SSID with OWE enabled will be counted as two SSID entries.

- **WPA-Personal**

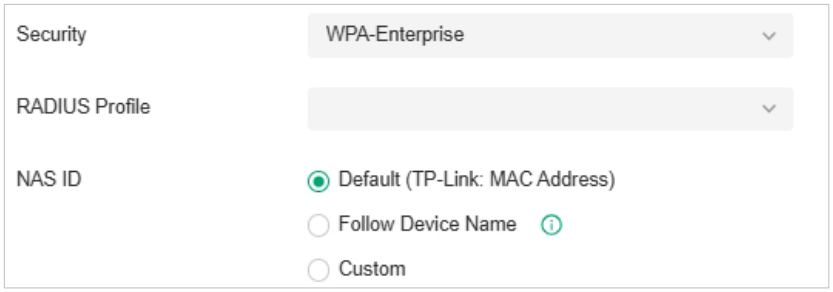
With WPA-Personal selected, traffic is encrypted with a Security Key you set,



Security Key	Specify a security key to encrypt the traffic.

- **WPA-Enterprise**

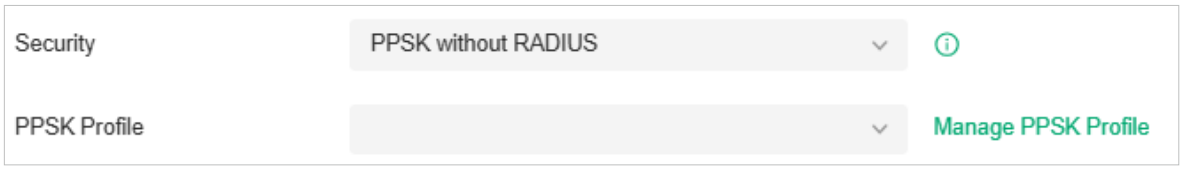
WPA-Enterprise requires an authentication server to authenticate wireless clients, and probably an accounting server to record the traffic statistics.



RADIUS Profile	Select a RADIUS Profile, which records the settings of the authentication server and accounting server. You can create a RADIUS Profile by clicking Create New Radius Profile from the drop-down list of RADIUS Profile. For details, refer to 4. 8 Authentication.
NAS ID	Configure a Network Access Server Identifier (NAS ID) for the authentication. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups. The NAS ID can be a default one (TP-Link: MAC Address), follow the device name, or a customized one.

- **PPSK without RADIUS**

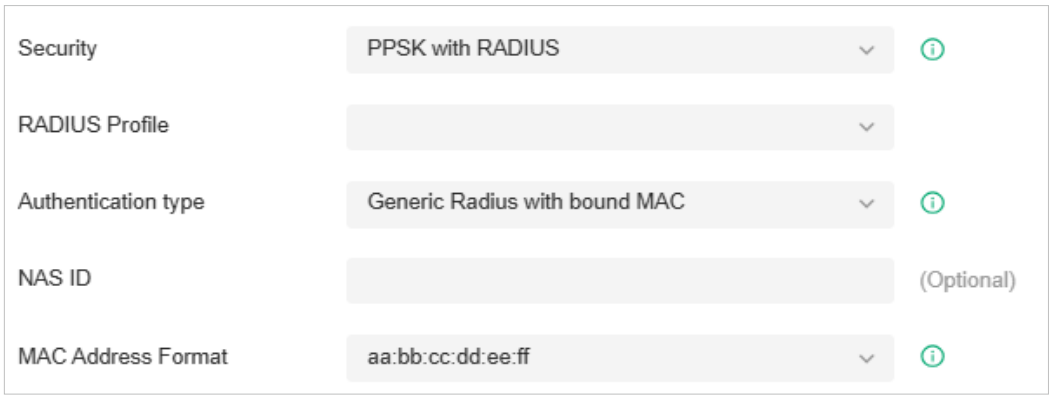
PPSK (private pre-shared key) can provide a unique PSK for each wireless user. Compared with the traditional SSID solution with one password for all users, it is more secure.



PPSK Profile	Select a PPSK Profile, which records the PPSK settings. You can create a PPSK Profile by clicking Create New PPSK Profile from the drop-down list of PPSK Profile. For details, refer to 4. 7. 4 PPSK.

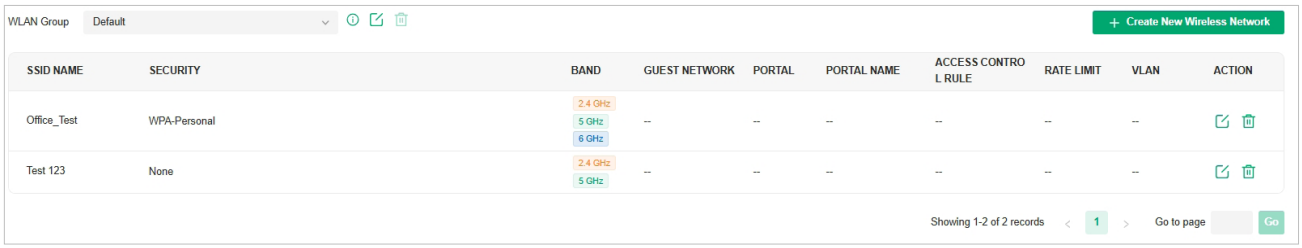
- **PPSK with RADIUS**

PPSK (private pre-shared key) can provide a unique PSK for each wireless use. PPSK with RADIUS requires an authentication server to authenticate wireless clients and probably an accounting server to record the traffic statistics. The SSID will not be applied to the device firmware not supporting PPSK.



RADIUS Profile	Select a RADIUS Profile, which records the settings of the authentication server and accounting server. You can create a RADIUS Profile by clicking + Create New Radius Profile from the drop-down list of RADIUS Profile. For details, refer to 4. 8 Authentication.
Authentication type	Choose the authentication type. Generic Radius with bound MAC: This type needs to specify device MAC addresses.
NAS ID	Configure a Network Access Server Identifier (NAS ID) for the authentication. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups.
MAC Address Format	Select clients' MAC address format which the controller uses for authentication. Then configure the MAC addresses in the specified format as usernames for the clients on the RADIUS server.

4. (Optional) You can also configure Advanced Settings, WLAN Schedule, 802.11 Rate Control, and MAC Filter, and more according to your needs. Related topics are covered later in this chapter.
5. Click Apply. The new wireless network is added to the wireless network list under the WLAN group. You can click the Edit icon in the ACTION column to edit the wireless network. You can click the Delete icon in the ACTION column to delete the wireless network.

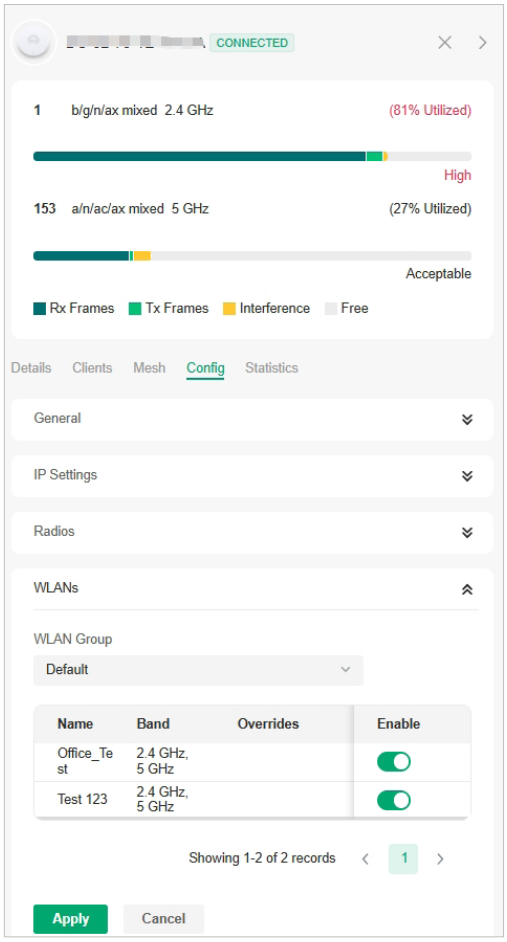


Step 3: Apply the WLAN Group

Note: The controller provides a default WLAN group. If you simply want to configure wireless networks for the default WLAN group and apply it to all your APs, skip this step.

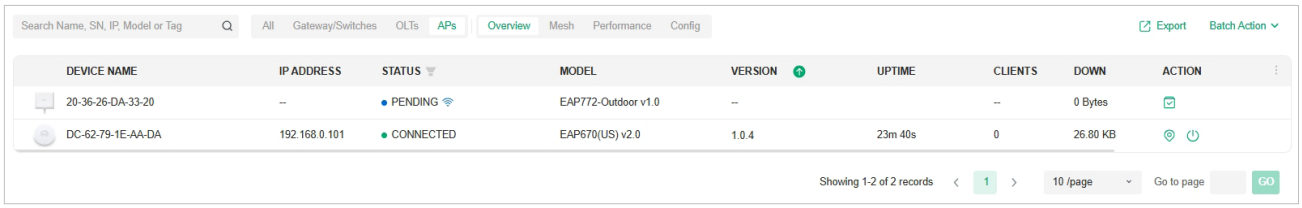
- **Apply to a Single AP**

  Go to Devices, select the AP. In the Properties window, go to Config > WLANs, select the WLAN group to apply.



- **Apply to APs in batch**

1. Go to Devices, select the APs tab, click Batch Action, and then select Batch Config, check the boxes of APs which you want to apply the WLAN group to, and click Done.

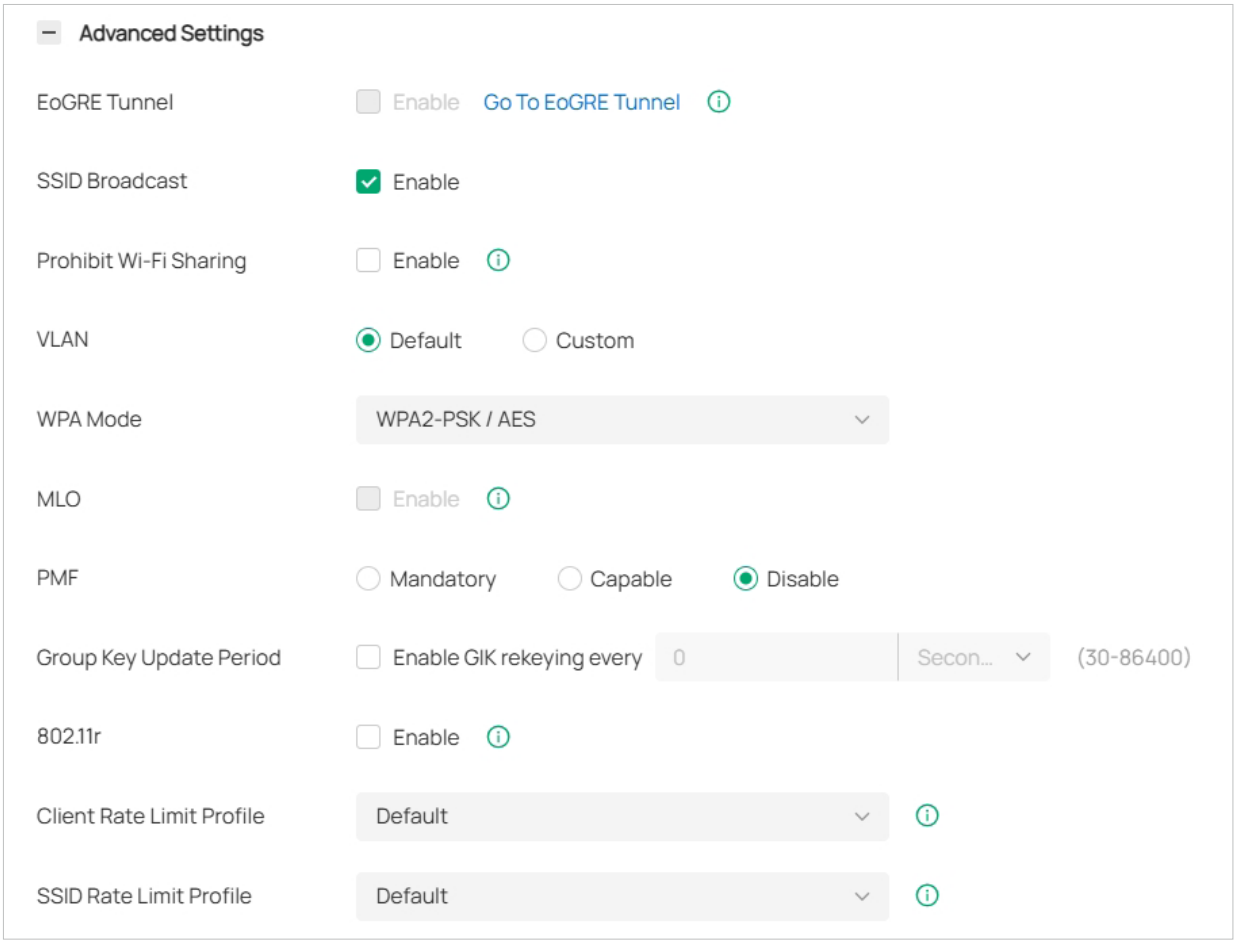


2. In the Properties window, go to Config > WLANs, select the WLAN group which you want to apply to the AP.



4. 3. 2 Advanced Settings

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click Advanced Settings to load the following page. Configure the parameters and click Apply.



SSID Broadcast	With SSID Broadcast enabled, APs broadcast the SSID (network name) in the air so that wireless clients can connect to the wireless network, which is identified by the SSID. With SSID Broadcast disabled, users of wireless clients must enter the SSID manually to connect to the wireless network.
Prohibit Wi-Fi Sharing	When enabled, the connected clients will be prohibited to share the Wi-Fi with other clients.
VLAN	Configure the uplink port VLAN(s) corresponding to the SSID. Default: Using untagged transmission. Custom: Configure an SSID-based VLAN pool by binding one or multiple networks (by network) or manually entering one or multiple VLAN IDs (by VLAN). When a client connects to the SSID, it will be assigned to a VLAN in the VLAN pool you configured. If a device does not support multiple VLANs, the smallest VLAN you configured will be applied to the SSID.
WPA Mode	If you select WPA-Personal or WPA-Enterprise as the security strategy, you can select the WPA Mode including the version of WPA, and the encryption type. Select the version of WPA according to your needs. Select the encryption type. Some encryption type is only available under certain circumstances. AES: AES stands for Advanced Encryption Standard. Auto: APs automatically decide the encryption type in the authentication process.
MLO	MLO (Multi-Link Operation) enables Wi-Fi 7 devices to simultaneously send and receive data across different frequency bands and channels. This ensures fast and reliable connections even in dense network environments.
PMF	Protected Management Frames (PMF) provide protection for unicast and multicast management action frames. When Mandatory is selected, non-PMF-capable clients may fail to connect to the network. Disable: Disables PMF for a network. It is not recommended to use this setting, only in case non-PMF-capable clients experience connection issues with the “Capable” option. Capable: Both types of clients, capable of PMF or not, can connect to the network. Clients capable of PMF will negotiate it with the AP. Mandatory: Only PMF-capable clients can connect to the network.
Group Key Update Period	If you select WPA-Personal or WPA-Enterprise as the security strategy, you can specify whether and how often the security key changes. If you want the security key to change periodically, enable GIK rekeying and specify the time period.
802.11r	Enable this feature to allow faster roaming when both the AP and client have 802.11r capabilities. Currently 802.11r does not support WPA3 encryption.
Client Rate Limit Profile	Specify the profile to limit the download and upload rates of each client to balance bandwidth usage. You can use the default profile or custom a profile.

SSID Rate Limit Profile	Specify the profile to limit the download and upload rates of each wireless band. Bandwidth is shared among all clients connected to the same wireless band of the same AP. You can use the default profile or custom a profile. **Note:** This feature requires new firmware updates for Omada APs, and the rate limit settings will only take effect on those APs running firmware that supports the feature.

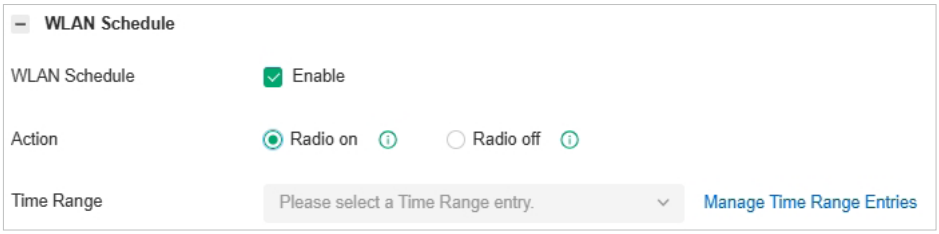
4. 3. 3 WLAN Schedule

Overview

WLAN Schedule can turn on or off your wireless network in the specific time period as you desire.

Configuration

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click WLAN Schedule to load the following page. Enable WLAN schedule and configure the parameters. Then click Apply.



Action	Radio On: Turn on your wireless network within the time range you set, and turn it off beyond the time range. Radio Off: Turn off your wireless network within the time range you set, and turn it on beyond the time range.
Time Range	Select the Time Range for the action to take effect. You can create a Time Range entry by clicking Create New Time Range Entry from the drop-down list of Time Range. For details, refer to 4. 7 Create Profiles.

4. 3. 4 802.11 Rate Control

Overview

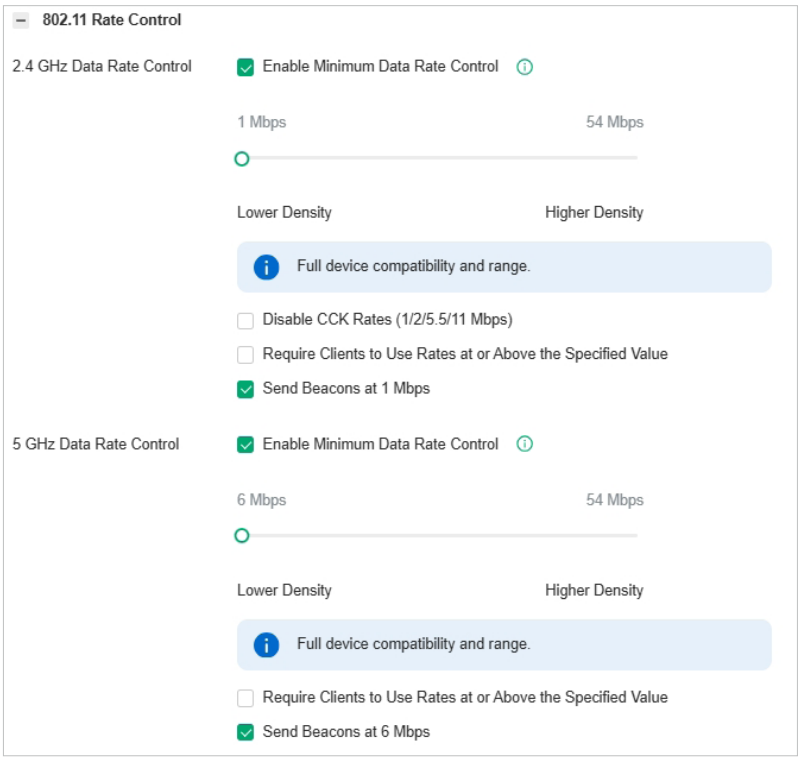
Note: 802.11 Rate Control is only available for certain devices.

802.11 Rate Control can improve performance for higher-density networks by disabling lower bit rates and only allowing the higher. However, 802.11 Rate Control might make some legacy devices incompatible with your networks, and limit the range of your wireless networks.

Configuration

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click 802.11 Rate Control to load the following page. Select one or multiple bands to enable minimum data rate control according to your needs, move the slider to determine what bit rates your wireless network allows, and configure the parameters. Then click Apply.

Note: The 6 GHz band is only available for certain devices.



Disable CCK Rates (1/2/5.5/11 Mbps)	Select whether to disable CCK (Complementary Code Keying), the modulation scheme which works with 802.11b devices. Disable CCK Rates (1/2/5.5/11 Mbps) is only available for 2.4 GHz band.
Require Clients to Use Rates at or Above the Specified Value	Select whether or not to require clients to use rates at or above the value specified on the minimum data rate controller slider.
Send Beacons at 1 Mbps/6 Mbps	Select whether or not to send Beacons at the minimum rate of 1Mbps for 2.4 GHz band or 6Mbps for 5 GHz band.

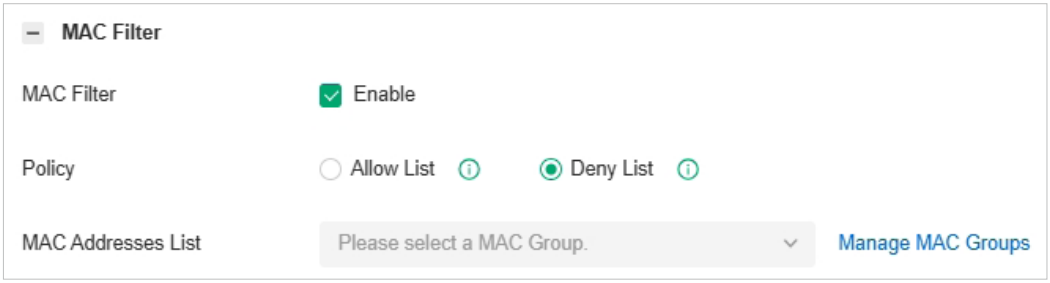
4. 3. 5 MAC Filter

Overview

MAC Filter allows or blocks connections from wireless clients of specific MAC addresses.

Configuration

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click MAC Filter to load the following page. Enable MAC Filter and configure the parameters .Then click Apply.



Policy	Allow List: Allow the connection of the clients whose MAC addresses are in the specified MAC Address List, while blocking others. Deny List: Block the connection of the clients whose MAC address are in the specified MAC Addresses List, while allowing others.
MAC Address List	Select the MAC Group which you want to allow or block according to the policy. You can create new MAC group by clicking + Create New MAC Group from the drop-down list of MAC Address List. For details, refer to 4. 7 Create Profiles.

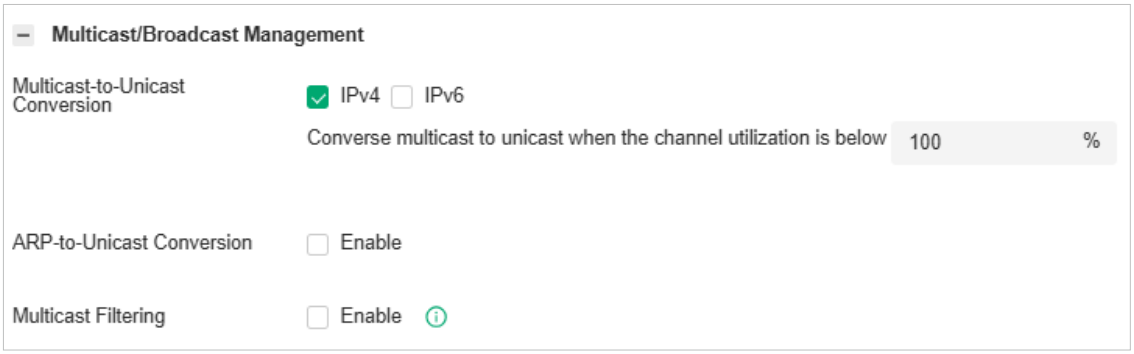
4. 3. 6 Multicast/Broadcast Management

Overview

Multicast/Broadcast Management allows packet conversion and multicast filtering.

Configuration

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click Multicast/Broadcast Management to load the following page. Configure the parameters .Then click Apply.



Multicast-to-Unicast Conversion	When enabled, the controller will convert multicast packets into unicast packets when the channel utilization is below the specified threshold.
ARP-to-Unicast Conversion	When enabled, the controller will convert ARP packets into unicast packets.
IPv6-Multicast-to-Unicast Conversion	Enable this option if you have high requirements for IPv6 multicast streaming transmission, such as high-definition video on demand. When enabled, the AP maintains IPv6 multicast-to-unicast entries by listening to MLD report packets and MLD leave packets reported by clients. When the AP sends an IPv6 multicast packet to a client, it converts the packet into an IPv6 unicast packet according to the multicast-to-unicast entry, thereby improving the IPv6 transmission efficiency for better wireless experience.
Multicast Filtering	When enabled, the controller will block IPv4 multicast packets of the specified protocols. Improper settings may cause network issues.

4. 3. 7 WLAN Optimization

Overview

WLAN Optimization helps improve the wireless network performance. With the WLAN Optimization feature, the controller will detect WiFi interference and monitor the wireless environment. Based on the environmental factors including network topology, deployment size, traffic, and client factors, the controller can determine the optimum wireless configurations (such as channel, power, etc.) for the access points (APs), and thus ensures that wireless clients of each AP can enjoy better WiFi experience.

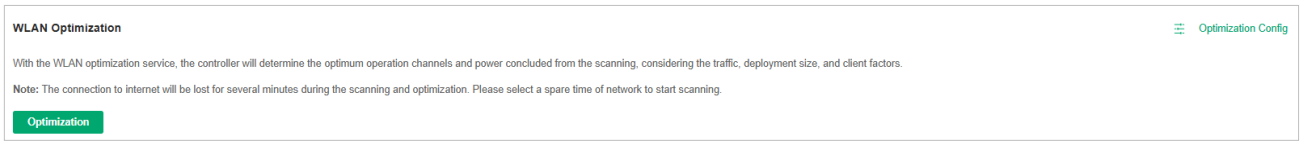
In WLAN Optimization, the results of the last 10 scans are displayed. You can also enable automatic optimization to allow the controller to conduct RF optimization automatically and set optimization schedules. In Optimization Log, the past optimization records are displayed, and you can also restore the previous optimization results as needed.

Configuration

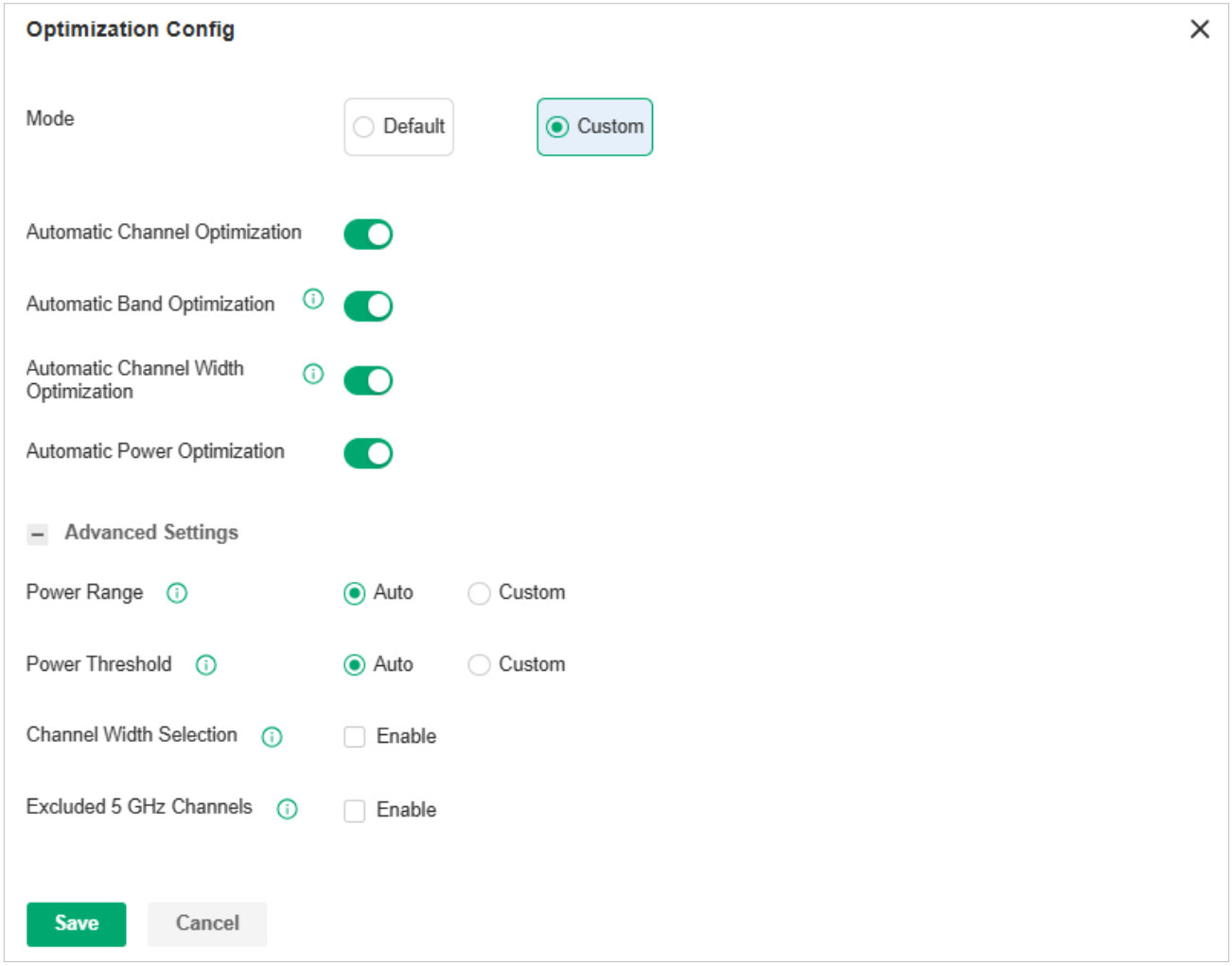
Note:

1. WiFi experience may be influenced during optimization. Please select the spare time to scan and optimize to reduce its impact on user experience.
2. Because the APs should stay connected during optimization, please set a different time for WLAN Optimization and Reboot Schedule. It is recommended to stagger at least 10 minutes to avoid dissatisfactory results.

1. Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN Optimization.
2. Click Optimization to begin the optimization. The controller will scan the wireless environment to conclude the optimum WLAN network configurations. You can view the optimization results in Optimization Log.



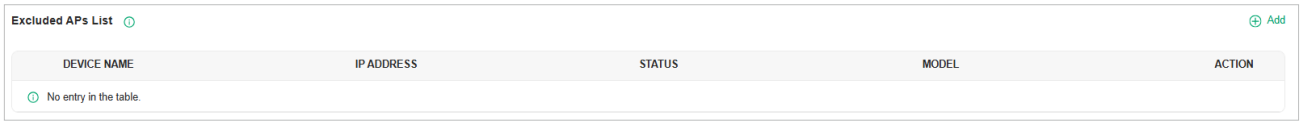
3. (Optional) Click Optimization Config if you want to custom configurations.



Mode	Specify the optimization mode. Default: The controller will conduct the optimization with the default configurations. Custom: The controller will conduct the optimization with the configurations you set.
Automatic Channel Optimization	Enable this function, and the controller will scan the wireless environment to conclude the optimum operation channels for the APs.
Automatic Band Optimization	Enable this function in a high-density deployment scenario, and the controller will scan the wireless environment and determine whether to turn off some radio bands to reduce network interference, hence improving the performance of the entire network.
Automatic Channel Width Optimization	Enable this function in a high-density deployment scenario, and the controller will scan the wireless environment and determine whether to reduce some radio bandwidth to reduce network interference, hence improving the performance of the entire network.

Automatic Power Optimization	Enable this function, and the controller will scan the wireless environment to conclude the optimum transmission power for the APs.
Power Range	Select Custom if you want to optimize the power within the specified range. You can limit the transmit power range of each AP/wireless routers after the power deployment is completed. For high-density deployment, you can try to set a smaller power range. An over-low value may lead to limited coverage, while an over-high value may lead to strong interference. (Note: The deployment may fail if the minimum power you select exceeds the maximum power of the AP to be deployed.)
Power Threshold	Select Custom if you want to optimize the power within the specified threshold. You can adjust the power deployment override threshold according to the actual deployment height and spacing of APs/wireless routers, achieving optimal wireless coverage after RF optimization. The larger the threshold, the larger the adjusted overall power value.
Channel Width Selection	Select the channel width for each band, and the optimization will maintain the selected channel width.
Excluded 5 GHz Channels	When enabled, you can specify the channels so they will not execute the automatic optimization.

4. (Optional) In the Excluded APs List, click Add to add the APs that will be excluded from WLAN Optimization. The following APs will be added to the list automatically: APs in the mesh network and APs with unsupported firmware.



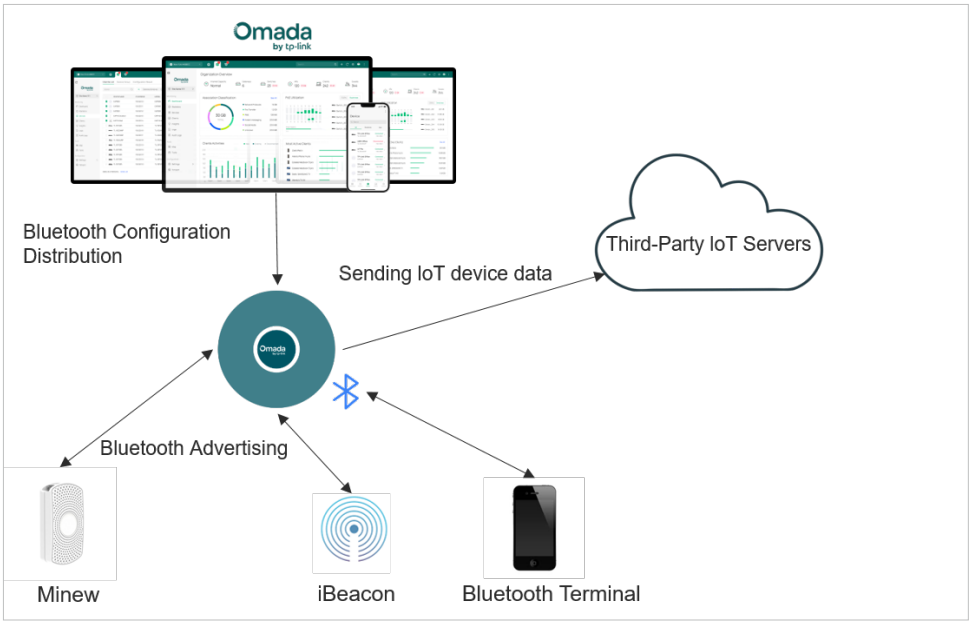
4. 3. 8 Bluetooth Settings

Overview

Omada supports Bluetooth settings to provide IoT (Internet of Things) solutions compatible with the Omada EAP for applications in healthcare, nursing homes, and more.

The Bluetooth Advertising with iBeacon technology turns the Omada EAP into a Bluetooth beacon, enabling location features for iOS apps using the Apple Core Location API.

Bluetooth IoT utilizes the Omada EAP Bluetooth module to easily collect Bluetooth data from third-party beacons and sensors, seamlessly connecting to external IoT servers for improved applications.



Configure IoT Transport Streams

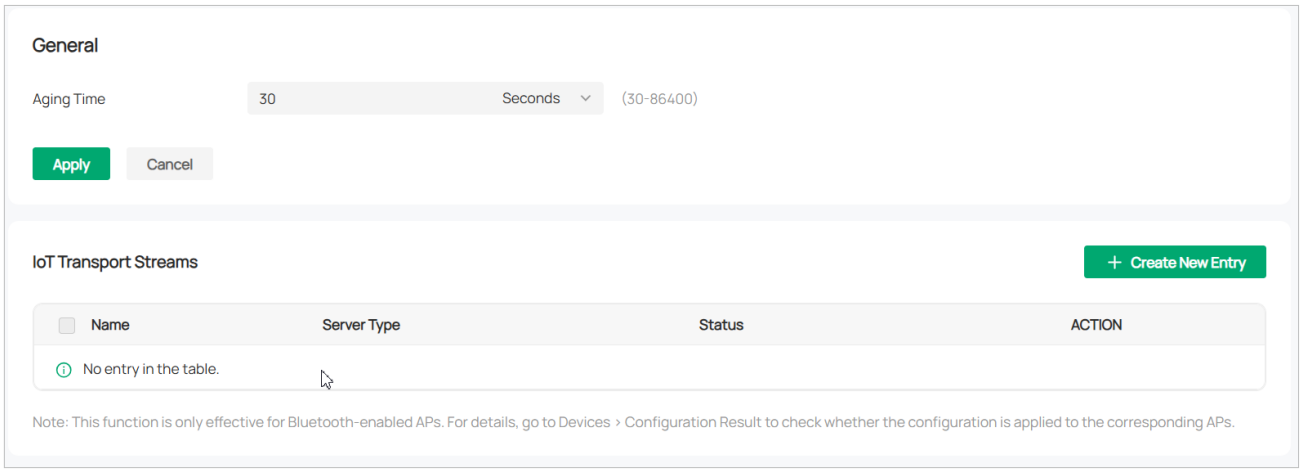
IoT Transport Streams allow Bluetooth-enabled APs to scan BLE Advertising frames in its surrounding environment, collect the required BLE data, and then report the data to the designated third-party IoT server. IoT Transport Streams can be divided into two functions: BLE Periodic Telemetry and BLE Data Forwarding.

BLE Periodic Telemetry: The APs will parse the scanned BLE Advertising frames, extract the valid data, and save the data to their BLE device lists. They will populate BLE device list data into the messages at set intervals and report to the designated third-party IoT server.

BLE Data Forwarding: The APs will automatically forward the scanned BLE Advertising frames of the specified protocol. The forwarded data is the raw data received by the APs, which is forwarded in real time.

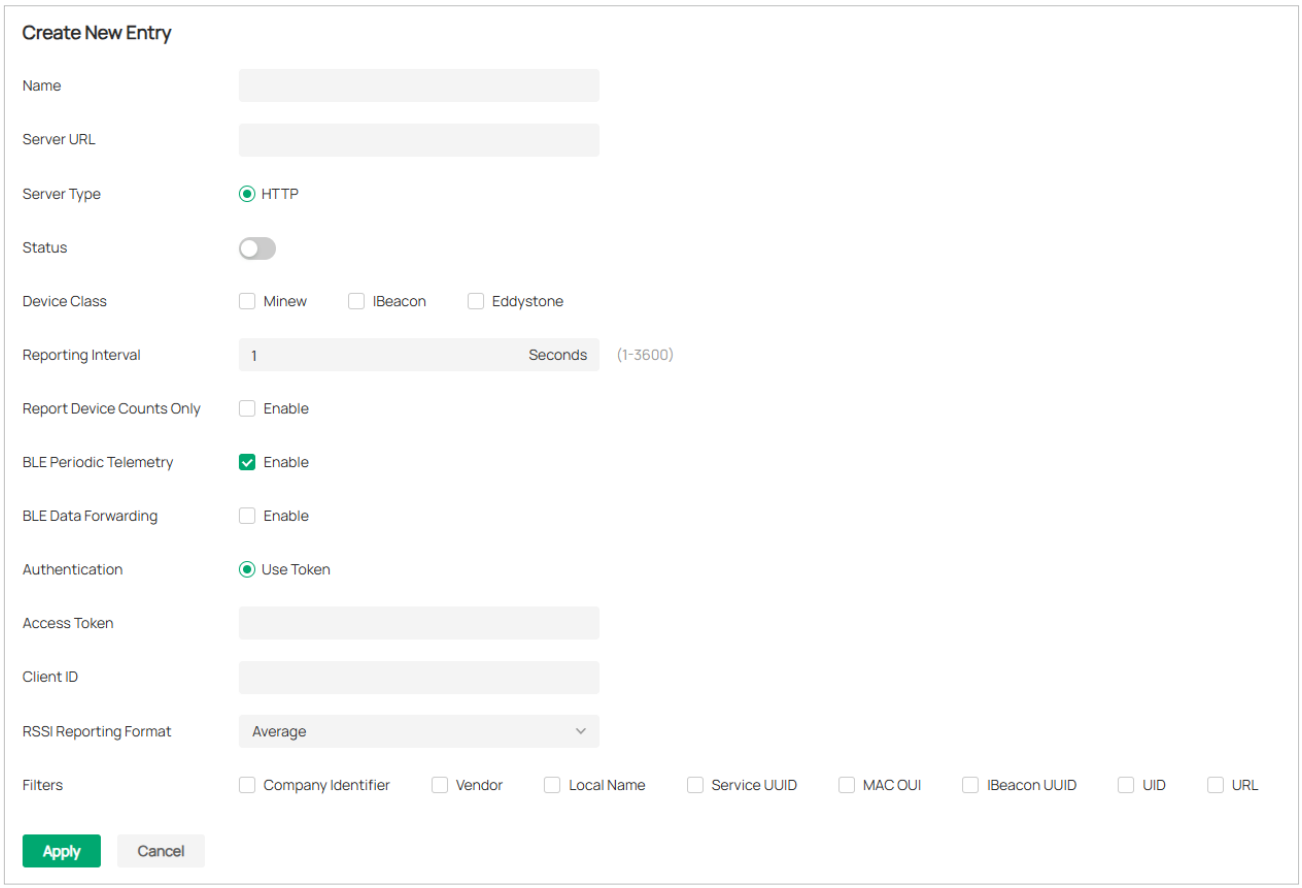
To configure IoT Transport Streams, follow the steps below:

1. Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Bluetooth > IoT Transport Streams.
2. Configure the Aging Time and click Apply.



Aging Time	Set the time in seconds, minutes, or hours to control the aging time of devices. If an AP does not receive the data sent by a device within the aging time, it will delete the device entry and no longer forward it to the IoT application server. If the AP receives the data sent by the device again, it will re-add the device entry and continue to report the Bluetooth data of the device.

3. Click Create New Entry to create a new IoT Transport Streams profile. Configure the parameters.



Name	Enter the name of the profile.
Server URL	Enter the server address for IoT data reporting. Currently, the URL path with http as the prefix is supported.

Server Type	Specify the connection protocol with the IoT server. Currently, only the HTTP type is supported.
Status	Toggle on to enable this profile on Bluetooth-enabled APs.
Device Class	Specify the vendors and protocols. Currently, only iBeacon, Eddystone, and Minew protocols are supported. More protocols will be supported in the future.
Reporting Interval	Specify the interval period for the AP to report IoT data.
Report Device Counts Only	When enabled, the AP only reports the number of IoT devices.
BLE Periodic Telemetry	Toggle on if you want to enable the periodic reporting of the AP.
BLE Data Forwarding	Toggle on if you want to enable the transparent transmission of the AP data.
Authentication	Specify the authentication method. Currently, token authentication is supported.
Access Token	Specify the token used for identity authentication.
Client ID	Specify the ID used for identity authentication.
RSSI Reporting Format	Specify the signal strength reporting format. Currently, Average, Max, Last, Smooth, and Bulk are supported.
Filters	Specify the custom configuration items that control the AP to filter IoT devices. Currently, Company Identifier, Vendor, Local Name, Service UUID, MAC OUI, iBeacon UUID, UID, and URL are supported.

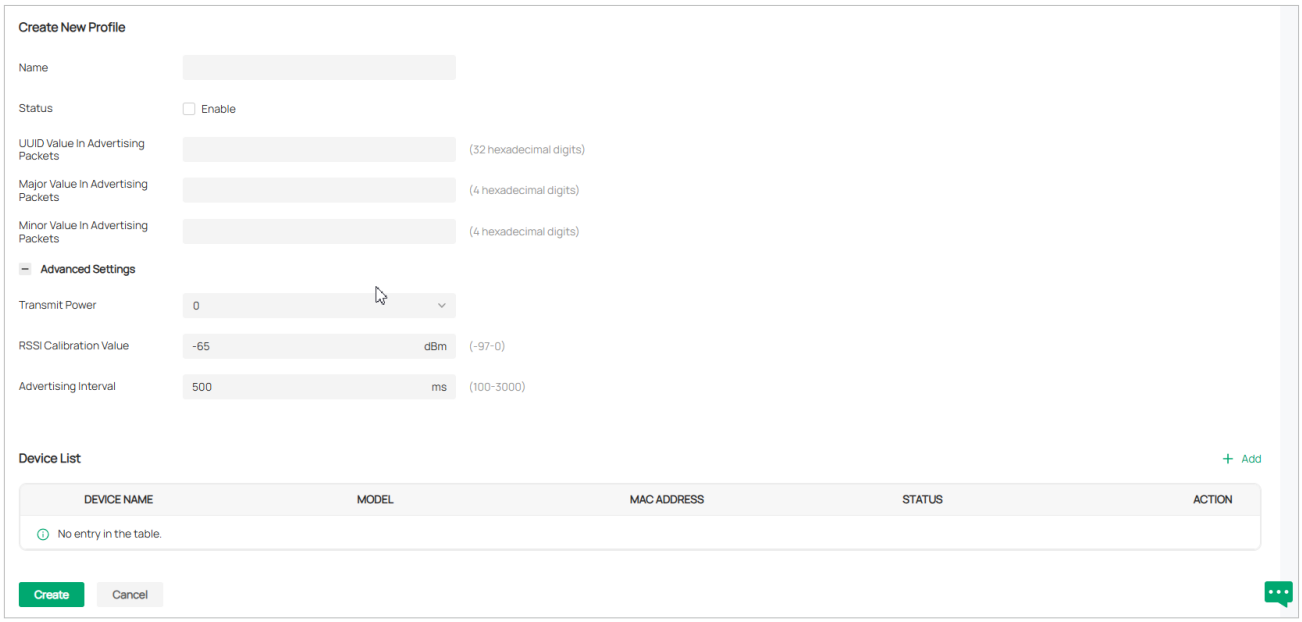
4. Click Apply. The profile will be added and applied to Bluetooth-enabled APs. You can go to Devices > Configuration Result to check whether the configuration is applied to the corresponding APs.

Configure Bluetooth Advertising

The Bluetooth Advertising function allows Bluetooth-enabled APs to send out specific BLE broadcast frames according to the set configuration. Currently, it only supports broadcasting iBeacon frames, and more protocols will be supported in the future. There is a default rule in the initial interface, which can be turned off but cannot be deleted. You can also add Advertising rules and apply them to specific APs.

To configure Bluetooth Advertising, follow the steps below:

1. Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Bluetooth > Bluetooth Advertising.
2. Click Create New Profile to create a Bluetooth Advertising profile. Configure the parameters.



Name	Enter the name of the profile.
Status	Toggle on to enable this profile on Bluetooth-enabled APs.
UUID Value In Advertising Packets	Specify the Universally Unique Identifier (UUID) of the broadcast iBeacon device, which is the unique identifier of the universal device.
Major Value In Advertising Packets	Specify the major value of the broadcast iBeacon device, used to mark larger groups.
Minor Value In Advertising Packets	Specify the minor value of the broadcast iBeacon device, used to mark smaller groups.
Transmit Power	Choose the broadcast transmission power (dB). Currently supported: [-20, -18, -15, -12, -10, -9, -6, -5, -3, 0, 1, 2, 3, 4, 5, 14, 15, 16, 17, 18, 19, 20].
RSSI Calibration Value	Specify the RSSI calibration value (dB).
Advertising Interval	Specify the interval of advertising frames.
Device List	The default site-level entry does not have this configuration item. Only custom entries support the configuration of specific devices. Currently, a single device is supported to configure a Bluetooth Custom configuration entry for advertising.

4. Click Create. The profile will be added and applied to Bluetooth-enabled APs. You can go to Devices > Configuration Result to check whether the configuration is applied to the corresponding APs.

4. 4 Network Security

Network Security is a portfolio of features designed to improve the usability and ensure the safety of your network and data. It implements policies and controls on multiple layers of defenses in the network.

4. 4. 1 ACL

Overview

ACL (Access Control List) allows a network administrator to create rules to restrict access to network resources. ACL rules filter traffic based on specified criteria such as source IP addresses, destination IP addresses, and port numbers, and determine whether to forward the matched packets. These rules can be applied to specific clients or groups whose traffic passes through the gateway, switches and APs.

The system filters traffic against the rules in the list sequentially. The first match determines whether the packet is accepted or dropped, and other rules are not checked after the first match. Therefore, the order of the rules is critical. By default, the rules are prioritized by their created time. The rule created earlier is checked for a match with higher priority. To reorder the rules, select a rule and drag it to a new position. If no rules match, the device forwards the packet because of an implicit Permit All clause.

The system provides three types of ACL:

- **Gateway ACL**

  After Gateway ACLs are configured on the controller, they can be applied to the gateway to control traffic which is sourced from LAN ports and forwarded to the WAN ports.

  You can set the Network, IP address, port number of a packet as packet-filtering criteria in the rule.

- **Switch ACL**

  After Switch ACLs are configured on the controller, they can be applied to the switch to control inbound and outbound traffic through switch ports.

  You can set the Network, IP address, port number and MAC address of a packet as packet-filtering criteria in the rule.

- **AP ACL**

  After AP ACLs are configured on the controller, they can be applied to the APs to control traffic in wireless networks.

  You can set the Network, IP address, port number and SSID of a packet as packet-filtering criteria in the rule.

Configuration

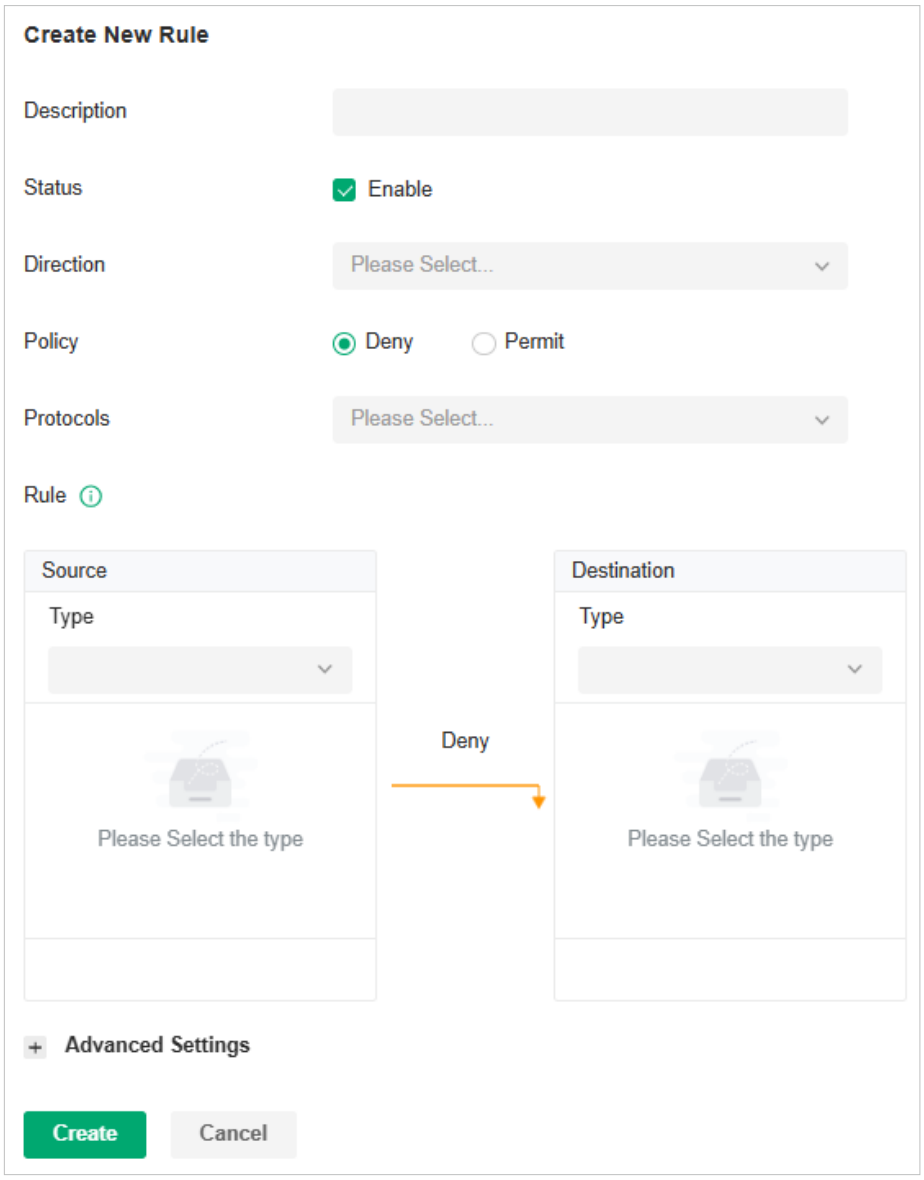
To complete the ACL configuration, follow these steps:

1) Create an ACL with the specified type.

2) Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets.

■ Configuring Gateway ACL

1. Launch the controller and access a site. Go to Settings > Network Security > ACL. On Gateway ACL tab, click Create New Profile to load the following page.



2. Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Description	Enter a description to identify the ACL.
Status	Click the checkbox to enable the ACL.

Direction	Select the direction of ACL application traffic. LAN->LAN: Control packet forwarding between LAN side devices. LAN->WAN: Control packet forwarding in the LAN-WAN direction.
Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Protocols	Select one or more protocol types to which the rule applies from the drop-down list. The default is All, indicating that packets of all protocols will be matched. When you select one of TCP and UDP or both of them, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.
Log	When enabled, the system can collect ACL entry effective log. To use this function, please configure the remote logging function first.

From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired&Wireless Networks > LAN to create one. The gateway will examine whether the packets are sourced from the selected network.
! Network	Select a network you have created and the settings will not applied to that network.
SSID	Select the SSID you have created. If no SSIDs have been created, go to Settings > Wired&Wireless Networks > WLAN to create one.The system will examine whether the SSID of the packet is the SSID selected here.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address of the packet is in the IP Group.
! IP Group	Select an IP group you have created and the settings will not applied to that IP group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address and port number of the packet are in the IP-Port Group.
! IP-Port Group	Select an IP-Port group you have created and the settings will not applied to that IP-Port group.
IPv6 Group	IPv6 Group:Select the IPv6 Group you have created. If no IPv6 Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the source IPv6 address of the packet is in the IPv6 Group.

! IPv6 Group	Select an IPv6 group you have created and the settings will not applied to that IPv6 group.
IPv6-Port Group	IPv6-Port Group:Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the source IPv6 address and port number of the packet are in the IPv6-Port Group.
! IPv6-Port Group	Select an IPv6-Port group you have created and the settings will not applied to that IPv6-Port group.
Location	Select one or multiple locations from the list as the source address, and the system will judge whether the source IP of the data packet belongs to the selected locations.
Location Group	Select a location group you have created, and the system will judge whether the source IP of the data packet belongs to this location group. If no location group has been created, click the create button to create one, or go to Settings > Profiles > Groups to create one.

From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the destination IP address of the packet is in the IP Group.
! IP Group	Select an IP group you have created and the settings will not applied to that IP group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the destination IP address and port number of the packet are in the IP-Port Group.
! IP-Port Group	Select an IP-Port group you have created and the settings will not applied to that IP-Port group.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the destination IPv6 address of the packet is in the IPv6 Group.
! IPv6 Group	Select an IPv6 group you have created and the settings will not applied to that IPv6 group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the destination IPv6 address and port number of the packet are in the IPv6-Port Group.
! IPv6-Port Group	Select an IPv6-Port group you have created and the settings will not applied to that IPv6-Port group.

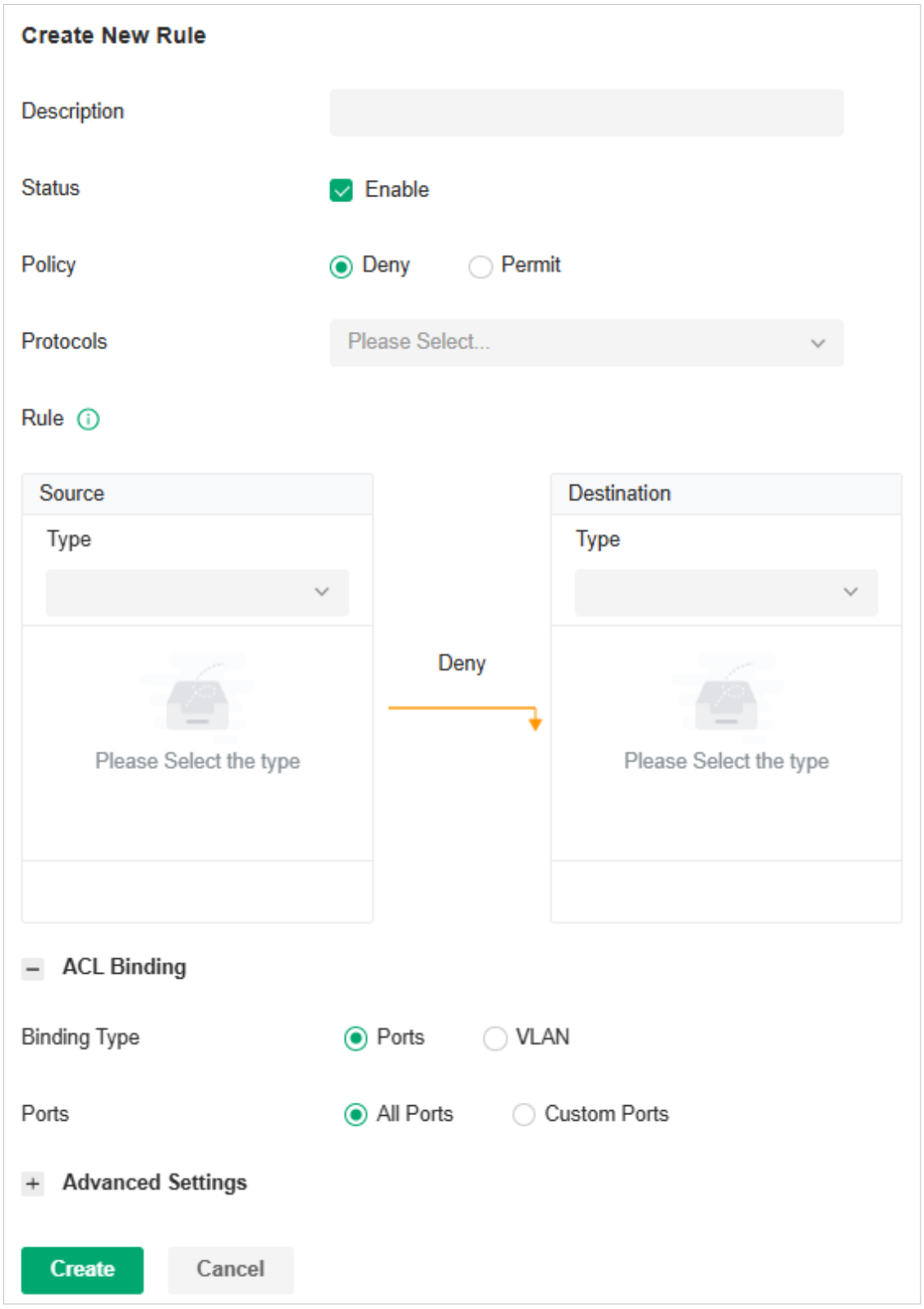
Location	Select one or multiple locations from the list as the destination address, and the system will judge whether the destination IP of the data packet belongs to the selected locations.
Location Group	Select a location group you have created, and the system will judge whether the destination IP of the data packet belongs to this location group. If no location group has been created, click the create button to create one, or go to Settings > Profiles > Groups to create one.
Gateway Management Page	This option will allow/block LAN network devices to access the gateway management page.

Set the advanced settings according to your needs:

Time Range	Select the checkbox to enable time-based ACL. You can create a time range or select an existing time range for the ACL rule to take effect.
Bi-Directional	When Direction is LAN->LAN, you can enable this option to configure bi-directional traffic rule.
States Type	Determine the type of stateful ACL rule. It is recommended to use the default Auto type. Auto (Match Sate New/Established/Related): Match the new, established, and related connection states. Manual: If selected, you can manually specify the connection states to match. Match State New: Match the connections of the initial state. For example, a SYN packet arrives in a TCP connection, or the router only receives traffic in one direction. Match State Established: Match the connections that have been established. In other words, the firewall has seen the bidirectional communication of this connection. Match State Related: Match the associated sub-connections of a main connection, such as a connection to a FTP data channel.

■ Configuring Switch ACL

1. Launch the controller and access a site. Go to Settings > Network Security > ACL. Under the Switch ACL tab, click Create New Profile to load the following page.



2. Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters.

Description	Enter a description to identify the ACL.

Status	Click the checkbox to enable the ACL.
Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Protocols	Select one or more protocol types to which the rule applies from the drop-down list. The default is All, indicating that packets of all protocols will be matched. When you select one of TCP and UDP or both of them, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.
Time Range	Select the checkbox to enable time-based ACL. You can create a time range or select an existing time range for the ACL rule to take effect.
Ethertype	Click the checkbox if you want the switch to check the ethertype of the packets, and configure the Ethertype based on needs.
Bi-Directional	Click the checkbox to enable the switch to create another symmetric ACL with the name "xxx_reverse", where "xxx" is the name of the current ACL. The two ACLs target at packets with the opposite direction of each other.

From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The switch will examine whether the packets are sourced from the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address and port number of the packet are in the IP-Port Group.
MAC Group	Select the MAC Group you have created. If no MAC Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source MAC address of the packet is in the MAC Group.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address of the packet is in the IPv6 Group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address and port number of the packet are in the IPv6-Port Group.

From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

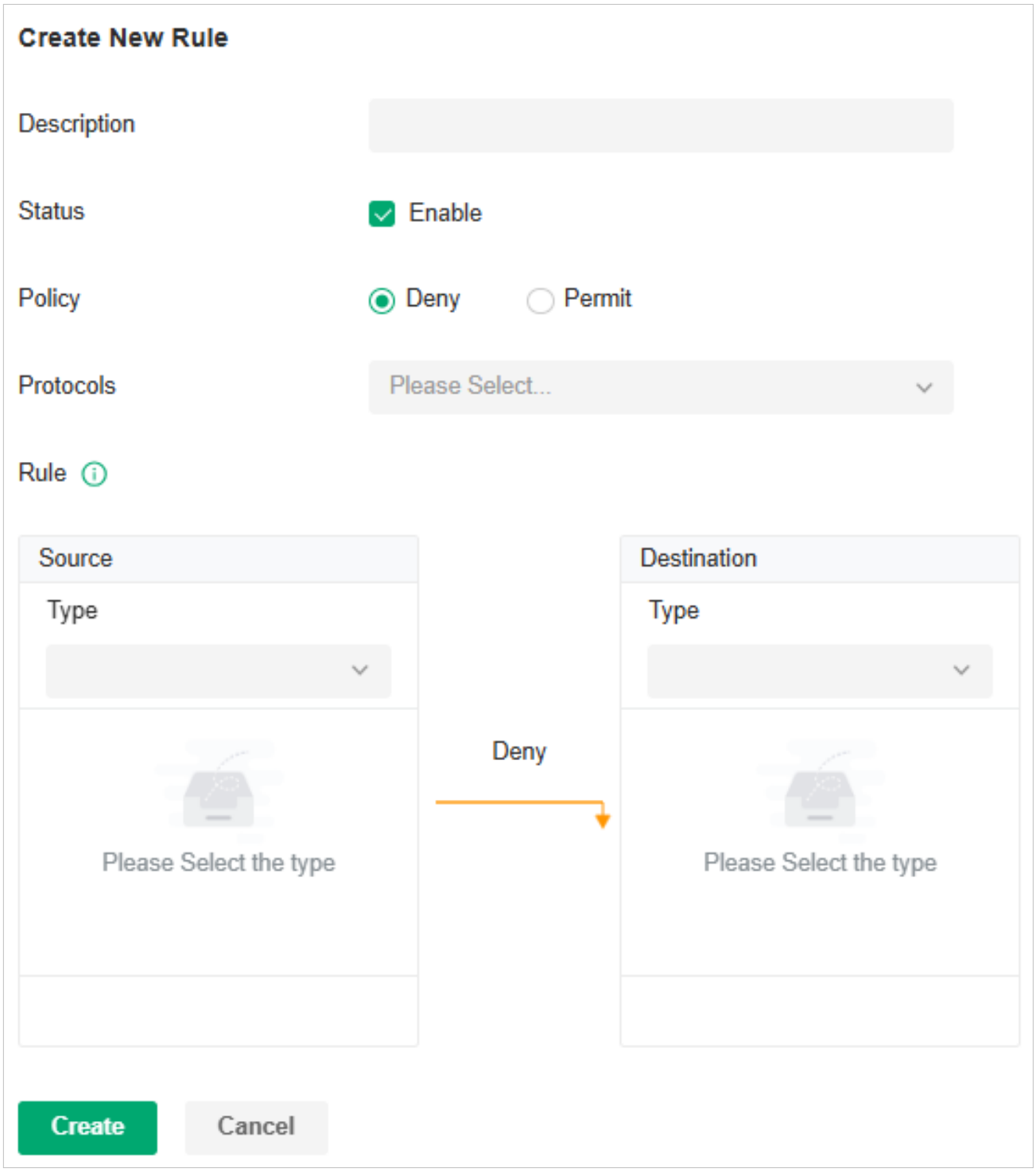
Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The switch will examine whether the packets are forwarded to the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address and port number of the packet are in the IP-Port Group.
MAC Group	Select the MAC Group you have created. If no MAC Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination MAC address of the packet is in the MAC Group.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address of the packet is in the IPv6 Group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address and port number of the packet are in the IPv6-Port Group.

3. Bind the switch ACL to a switch port or a VLAN and click Apply. Note that a switch ACL takes effect only after it is bound to a port or VLAN.

Binding Type	Specify whether to bind the ACL to ports or a VLAN. Ports: Select All Ports or Custom Ports as the interfaces to be bound with the ACL. With All ports selected, the rule is applied to all ports of the switch. With Custom ports selected, the rule is applied to the selected ports of the switch. Click the ports from the Device List to select the binding ports.  VLAN: Select a VLAN and specify the switches as the interface to be bound with the ACL. If no VLANs have been created, you can select the default VLAN 1 (LAN), or go to Settings > Wired Networks > LAN to create one.

■ Configuring AP ACL

1. Launch the controller and access a site. Go to Settings > Network Security > ACL. Under the AP ACL tab, click Create New Profile to load the following page.



2. Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Description	Enter a description to identify the ACL.
Status	Click the checkbox to enable the ACL.

Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Protocols	Select one or more protocol types to which the rule applies from the drop-down list. The default is All, indicating that packets of all protocols will be matched. When you select one of TCP and UDP or both of them, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.

From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The AP will examine whether the packets are sourced from the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address and port number of the packet are in the IP-Port Group.
SSID	Select the SSID you have created. If no SSIDs have been created, go to Settings > Wireless Networks to create one. The AP will examine whether the SSID of the packet is the SSID selected here.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address of the packet is in the IPv6 Group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address and port number of the packet are in the IPv6-Port Group.

From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The AP will examine whether the packets are forwarded to the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the destination IP address of the packet is in the IP Group.

IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the destination IP address and port number of the packet are in the IP-Port Group.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the destination IP address of the packet is in the IPv6 Group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the destination IP address and port number of the packet are in the IPv6-Port Group.

4. 4. 2 URL Filtering

Overview

URL Filtering allows a network administrator to create rules to block or allow certain websites, which protects it from web-based threats, and deny access to malicious websites.

In URL filtering, the system compares the URLs in HTTP, HTTPS and DNS requests against the lists of URLs that are defined in URL Filtering rules, and intercepts the requests that are directed at a blocked URLs. These rules can be applied to specific clients or groups whose traffic passes through the gateway and APs.

The system filters traffic against the rules in the list sequentially. The first match determines whether the packet is accepted or dropped, and other rules are not checked after the first match. Therefore, the order of the rules is critical. By default, the rules are prioritized based on the sequence they are created. The rule created earlier is checked for a match with a higher priority. To reorder the rules, select a rule and drag it to a new position. If no rules match, the device forwards the packet because of an implicit Permit All clause.

Note that URL Filtering rules take effects with a higher priority over ACL rules. That is, the system will process the URL Filtering rule first when the URL Filtering rule and ACL rules are configured at the same time.

Configuration

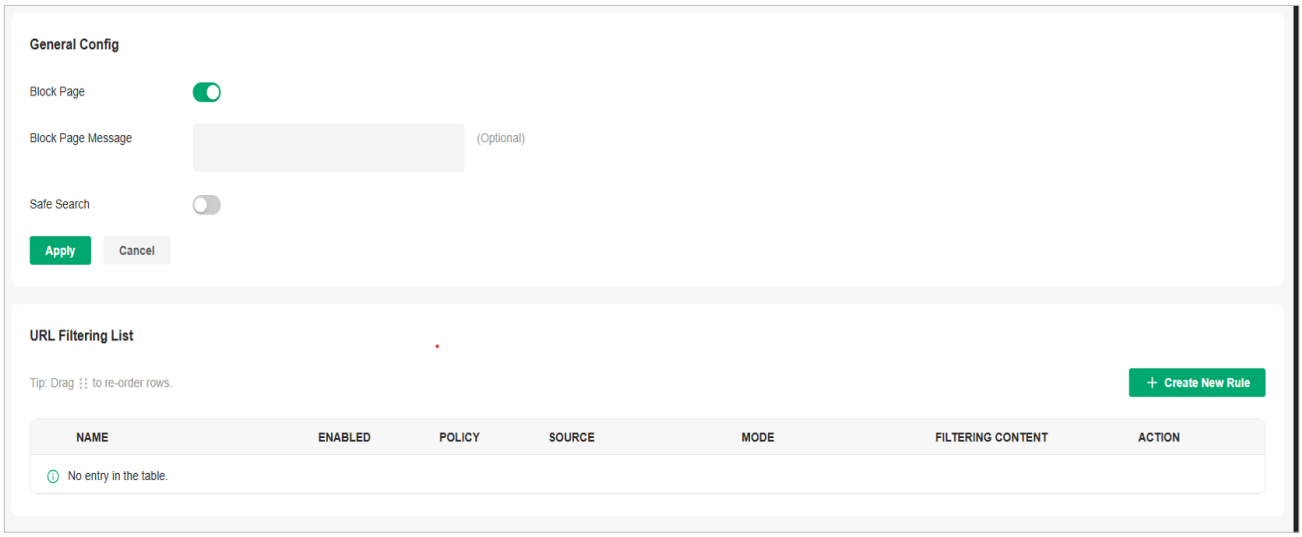
To complete the URL Filtering configuration, follow these steps:

1) Create a new URL Filtering rule with the specified type.

2) Define filtering criteria of the rule, including source, and URLs, and determine whether to forward the matched packets.

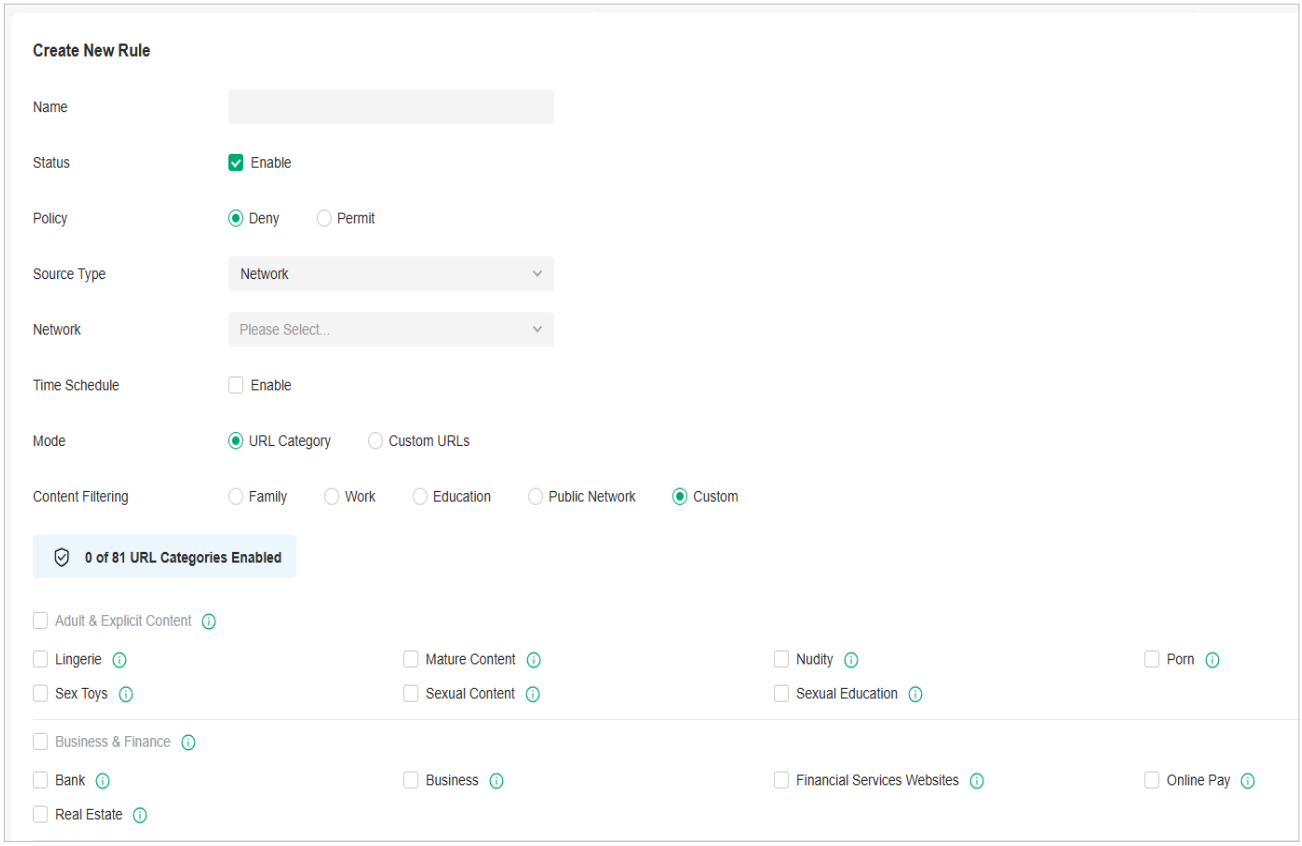
- **Configuring Gateway Rules**

1. Launch the controller and access a site. Go to Settings > Network Security > URL Filtering.
2. Under the Gateway Rules tab, configure the parameters.



Block Page	When enabled, users attempting to access blocked websites will be redirected to a specific page indicating that the website is blocked by access policy.
Block Page Message	When a user tries to access a blocked URL, the block page message will display to tell why access is denied. This can effectively remind users to comply with network usage regulations.
Safe Search	Check this option to enable Safe Search globally. This feature can filter search results to block inappropriate content. It is suitable for family and educational environments.

4. Click Create New Rule to load the following page.

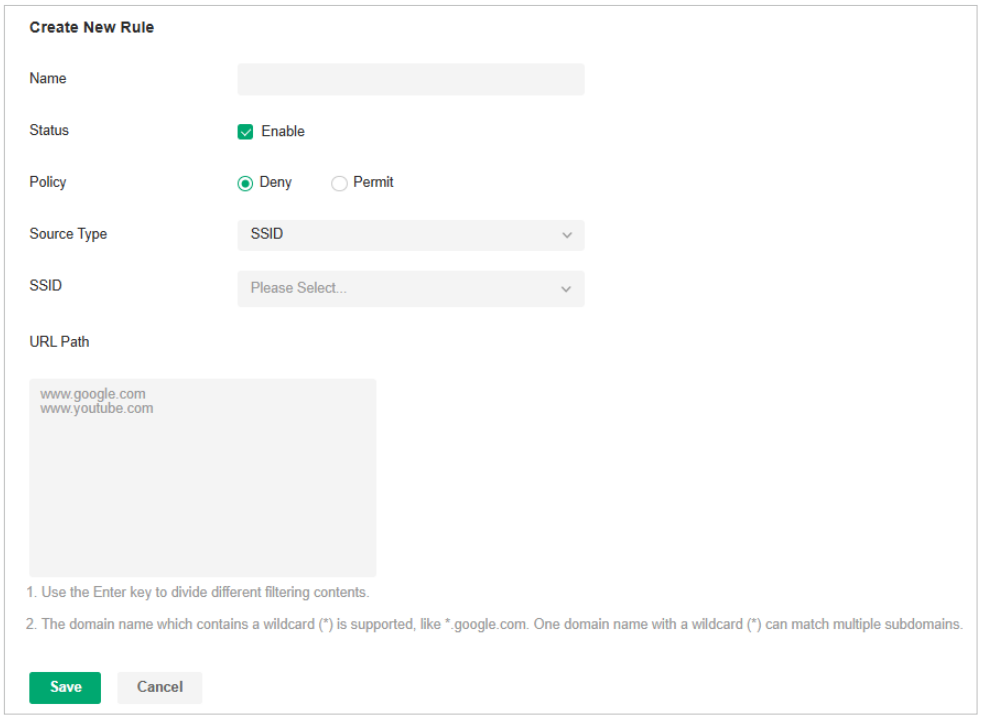


5. Define filtering criteria of the rule, including source and URLs, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the URL Filtering rule.
Status	Click the checkbox to enable the URL Filtering rule.
Policy	Select the action to be taken when a packet matches the rule. Deny: Discard the matched packet and the clients cannot access the URLs. Permit: Forward the matched packet and clients can access the URLs.
Source Type	Select the source of the packets to which this rule applies. Network: With Network selected, select the network you have created from the Network drop-down list. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The gateway will filter the packets sourced from the selected network. IP Group: With IP Group selected, select the IP Group you have created from the IP Group drop-down list. If no IP Groups have been created, click +Create New IP Group on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address of the packet is in the IP Group.
Time Schedule	Enable this option and set a time schedule if needed.
Mode	Choose a mode for the filtering content to match the URL. URL Category: Frequently used URLs such as news, entertainment, and shopping are divided into different categories. This mode is suitable for most common scenarios, but if you find that the required URLs are not in the filtering category, you can add the specific URLs in the custom URL mode. Custom URLs: Manually enter the URL you want to filter. This mode lets you precisely control content access.
Content Filtering	Select a preset scenario. Family: Suitable for homes Work: Suitable for offices. Education: Suitable for schools and educational institutions. Public Network: Suitable for public places. Custom: You can customize filtering rules according to the specific needs of different scenarios.

■ Configuring AP Rules

1. Launch the controller and access a site. Go to Settings > Network Security > URL Filtering. On AP Rules tab, click Create New Rule to load the following page.



2. Define filtering criteria of the rule, including source and URLs, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the URL Filtering rule.
Status	Click the checkbox to enable the URL Filtering rule.
Policy	Select the action to be taken when a packet matches the rule. Deny: Discard the matched packet and the clients cannot access the URLs. Permit: Forward the matched packet and clients can access the URLs.
Source Type	Select the SSID of the packets to which this rule applies.
URLs	Enter the URL address using up to 128 characters. URL address should be given in a valid format. The URL which contains a wildcard(*) is supported. One URL with a wildcard(*) can match mutiple subdomains. For example, with *.tp-link.com specified, community.tp-link.com will be matched.

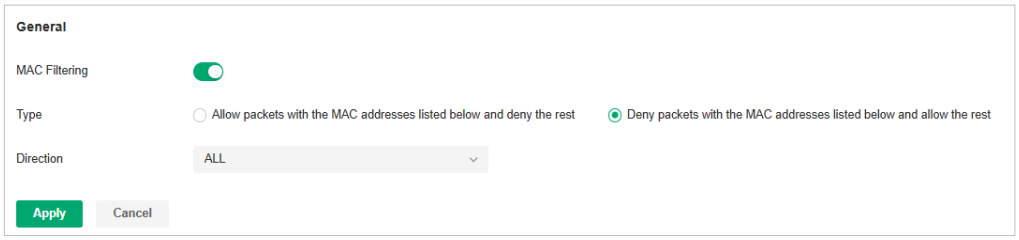
4. 4. 3 MAC Filtering

Overview

MAC Filtering can drop or allow packets from certain devices passing through the router based on the MAC address of the devices. After the MAC filtering policy and MAC filtering list are configured, the router will apply the filter policy to the packets matching the MAC address, and thus limit network traffic and manage network access behaviors.

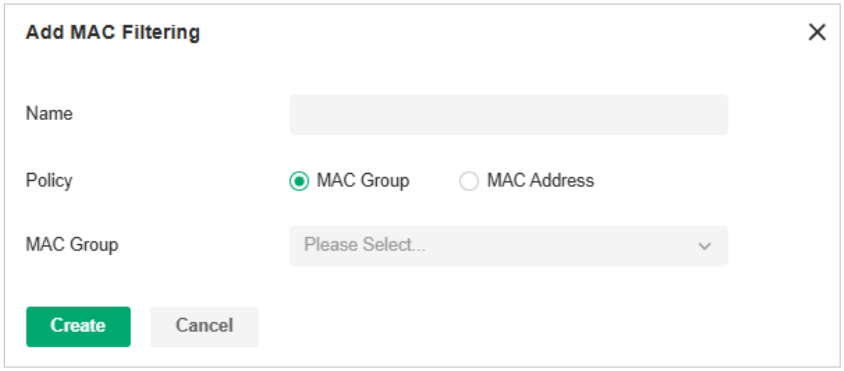
Configuration

1. Launch the controller and access a site. Go to Settings > Network Security > MAC Filtering.
2. Enable MAC Filtering and configure the parameters.



Type	Select the mode of MAC Filtering. Allow packets with the MAC addresses listed below and deny the rest: Select to allow packets with the listed MAC address to pass through the router, and packets with other MAC addresses will be dropped. Deny packets with the MAC addresses listed below and allow the rest: Select to drop packets with the listed MAC address, and packets with other MAC addresses will be allowed to pass through the router.
Direction	Select All when you want to apply the policy to traffic both from LAN to LAN and from LAN to WAN. Select LAN -> WAN when you want to apply the policy only to traffic from LAN to WAN.

3. Click Add MAC Filtering to add MAC addresses or groups to the list.



Name	Specify the name for the entry.
Policy	Choose MAC Group and specify the MAC groups of devices, then the MAC filtering policy will be applied to traffic with the MAC groups. Choose MAC Address and specify the MAC addresses of devices, then the MAC filtering policy will be applied to traffic with the MAC addresses.

4. 4. 4 Attack Defense

Overview

Attacks initiated by utilizing inherent bugs of communication protocols or improper network deployment have negative impacts on networks. In particular, attacks on a network device can cause the device or network paralysis.

With the Attack Defense feature, the gateway can identify and discard various attack packets in the network, and limit the packet receiving rate. In this way, the gateway can protect itself and the connected network against malicious attacks.

The gateway provides two types of Attack Defense:

- **Flood Defense**

If an attacker sends a large number of fake packets to a target device, the target device is busy with these fake packets and cannot process normal services. Flood Defense detects flood packets in real time and limits the receiving rate of the packets to protect the device.

Flood attacks include TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks.

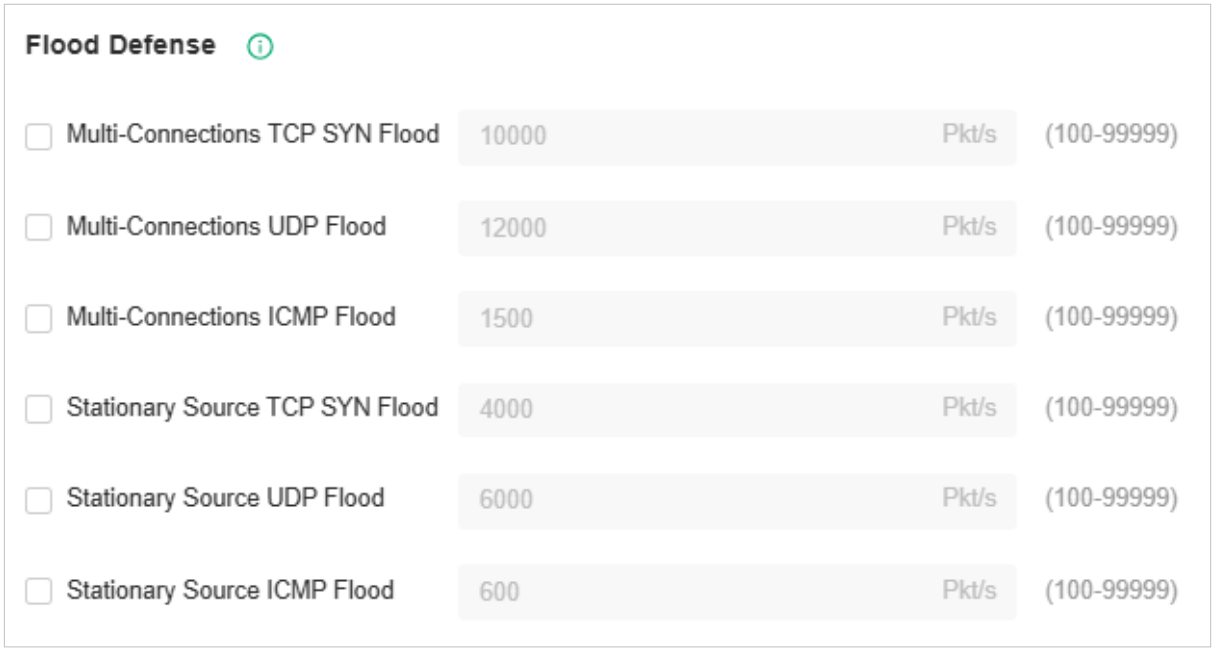
- **Packet Anomaly Defense**

Anomalous packets are packets that do not conform to standards or contain errors that make them unsuitable for processing. Packet Anomaly Defense discards the illegal packets directly.

Configuration

- **Configuring Flood Defense**

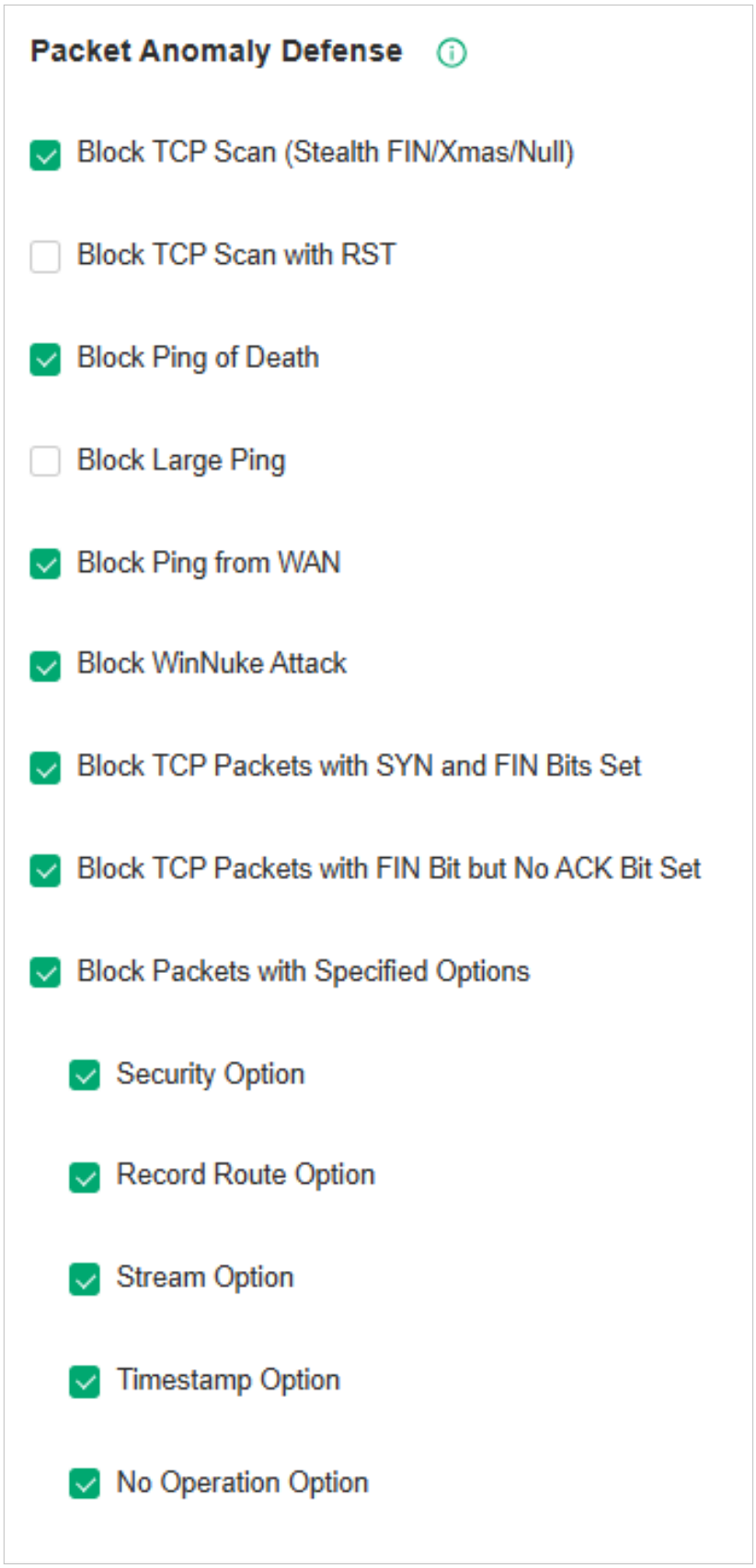
  Launch the controller and access a site. Go to Settings > Network Security > Attack Defense. In the Flood Defense, click the checkbox and set the corresponding limit of the rate at which specific packets are received.



Multi-Connections TCP SYN Flood	A TCP SYN flood attack occurs when the attacker sends the target system with a succession of SYN (synchronize) requests. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the system with SYN messages. No legitimate connections can then be made. With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from all the clients to the specified rate.
Multi-Connections UDP Flood	A UDP flood attack occurs when the attacker sends a large number of UDP packets to a target host in a short time, the target host is busy with these UDP packets and cannot process normal services. With this feature enabled, the gateway limits the rate of receiving UDP packets from all the clients to the specified rate.
Multi-Connections ICMP Flood	If an attacker sends many ICMP Echo messages to the target device, the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected. With this feature enabled, the system limits the rate of receiving ICMP packets from all the clients to the specified rate.
Stationary Source TCP SYN Flood	A TCP SYN flood attack occurs when the attacker sends the target system with a succession of SYN (synchronize) requests. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the system with SYN messages. No legitimate connections can then be made. With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from a single client to the specified rate.
Stationary Source UDP Flood	A UDP flood attack occurs when the attacker sends a large number of UDP packets to a target host in a short time, the target host is busy with these UDP packets and cannot process normal services. With this feature enabled, the gateway limits the rate of receiving UDP packets from a single client to the specified rate.
Stationary Source ICMP Flood	If an attacker sends many ICMP Echo messages to the target device, the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected. With this feature enabled, the system limits the rate of receiving ICMP packets from a single clients to the specified rate.

- **Configuring Packet Anomaly Defense**

  Launch the controller and access a site. Go to Settings > Network Security > Attack Defense. In the Packet Anomaly Defense, click the checkbox and set the corresponding limit of the rate at which specific packets are received.



Block Fragment Traffic	With this option enabled, the fragmented packets without the first part of the packet will be discarded.

Block TCP Scan (Stealth FIN/Xmas/Null)	With this option enabled, the gateway will block the anomalous packets in the following attack scenarios: Stealth FIN Scan: The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal. Xmas Scan: The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1. Null Scan: The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.
Block TCP Scan with RST	With this option enabled, the gateway will respond to RST messages. It is disabled by default.
Block Ping of Death	With this option enabled, the gateway will block Ping of Death attack. Ping of Death attack means that the attacker sends abnormal ping packets which are smaller than 64 bytes or larger than 65535 bytes to cause system crash on the target computer.
Block Large Ping	With this option enabled, the router will block the ping packets which are larger than the specified value (1024 packets by default) to protect the system from Large Ping attack.
Block Ping from WAN	With this option enabled, the router will block the ICMP request from WAN.
Block WinNuke Attack	With this option enabled, the router will block WinNuke attacks. WinNuke attack refers to a remote DoS (denial-of-service) attack that affects some Windows operating systems, such as the Windows 95. The attacker sends a string of OOB (Out of Band) data to the target computer on TCP port 137, 138 or 139, causing system crash or Blue Screen of Death.
Block TCP Packets with SYN and FIN Bits Set	With this option enabled, the router will filter the TCP packets with both SYN Bit and FIN Bit set.
Block TCP Packets with FIN Bit but No ACK Bit Set	With this option enabled, the router will filter the TCP packets with FIN Bit set but without ACK Bit set.
Block Packets with Specified Options	With this option enabled, the router will filter the packets with specified IP options including Security Option, Loose Source Route Option, Strict Source Route Option, Record Route Option, Stream Option, Timestamp Option, and No Operation Option. You can choose the options according to your needs.

4. 4. 5 Firewall

Overview

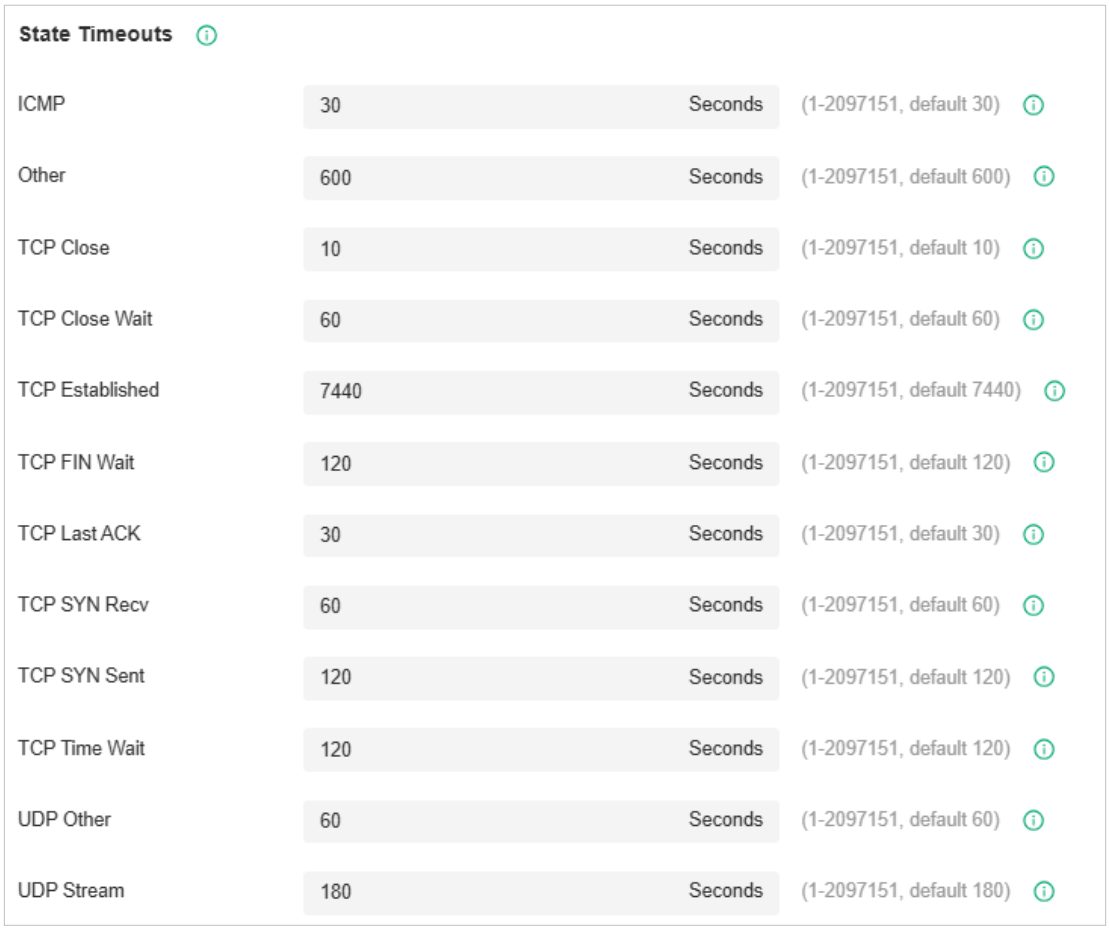
Firewall is used to enhance the network security. In State Timeouts, you can specify a number of timeouts for sessions including TCP, UDP, and ICMP connection. The packets will be forwarded within the specified timeout. When there is no response after the specified time, the session or status will be closed. State timeout will help close inactive sessions and thus avoid network malfunction. In

Firewall Options, you can further configure the gateway to prevent attacks like SYN flood attacks and broadcast ping.

Configuration

- **Configuring State Timeouts**

  Launch the controller and access a site. Go to Settings > Network Security > Firewall. In the Sate Timeouts, set the time limit for the different sessions.

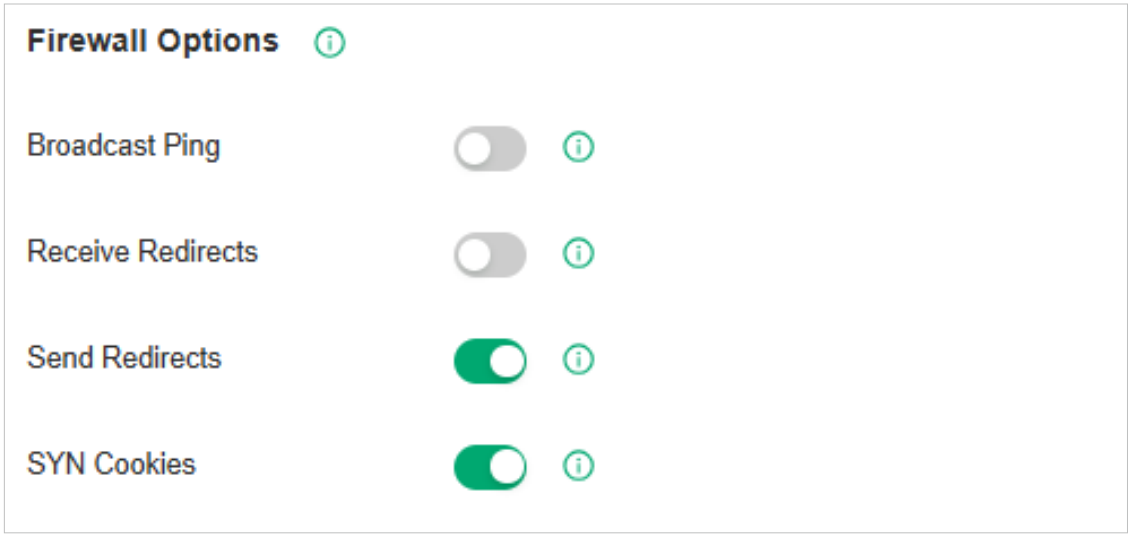


ICMP	The ICMP session will be closed if there is no response after the set time.
Other	The sessions for protocols excluding TCP, UDP, and ICMP will be closed if there is no response after the set time.
TCP Close	The TCP Close status will be closed if there is no response after the set time.
TCP Close Wait	The TCP Close Wait status will be closed if there is no response after the set time.
TCP Established	The TCP Established status will be closed if there is no response after the set time.
TCP FIN Wait	The TCP FIN Wait status will be closed if there is no response after the set time.
TCP Last ACK	The TCP Last ACK status will be closed if there is no response after the set time.

TCP SYN Recv	The TCP SYN (Synchronize) Recv status will be closed if there is no response after the set time.
TCP SYN Sent	The TCP SYN (Synchronize) Sent status will be closed if there is no response after the set time.
TCP Time Wait	The TCP Time Wait status will be closed if there is no response after the set time.
UDP Other	The UDP connections with traffic in only one direction will be stopped if there is no response after the set time.
UDP Stream	The UDP connections with bidirectional traffic will be stopped if there is no response after the set time.

- **Configuring Firewall Options**

  Launch the controller and access a site. Go to Settings > Network Security > Firewall. In the Sate Timeouts, set the time limit for the different sessions.



Broadcast Ping	With it enabled, the gateway will reply to broadcast pings.
Receive Redirects	With it enabled, the gateway will accept ICMP redirects.
Send Redirects	With it enabled, the gateway will send ICMP redirects.
SYN Cookies	With it enabled, the SYN cookies will be used to resist SYN flood attacks that want to open ports on the gateway.

4. 4. 6 IP-MAC Binding

Overview

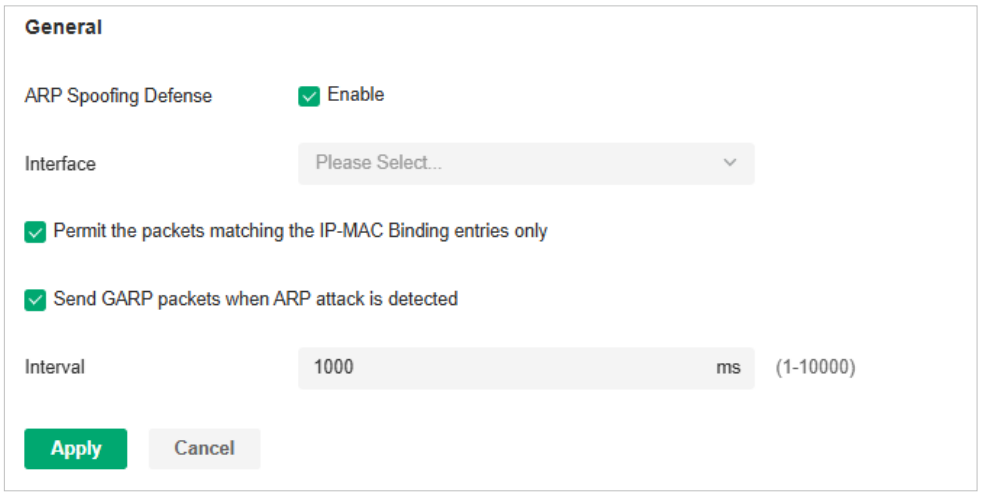
ARP (Address Resolution Protocol) is used to map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations. However, if attackers send ARP spoofing packets with false IP address-to-MAC address mapping entries, the device will update the ARP table

based on the false ARP packets and record wrong mapping entries, which results in a breakdown of normal communication.

Anti ARP Spoofing can protect the network from ARP spoofing attacks. It works based on the IP-MAC Binding. These entries record the correct one-to-one relationships between IP addresses and MAC addresses. When receiving an ARP packet, the router checks whether it matches any of the IP-MAC Binding entries. If not, the router will ignore the ARP packets. In this way, the router maintains the correct ARP table.

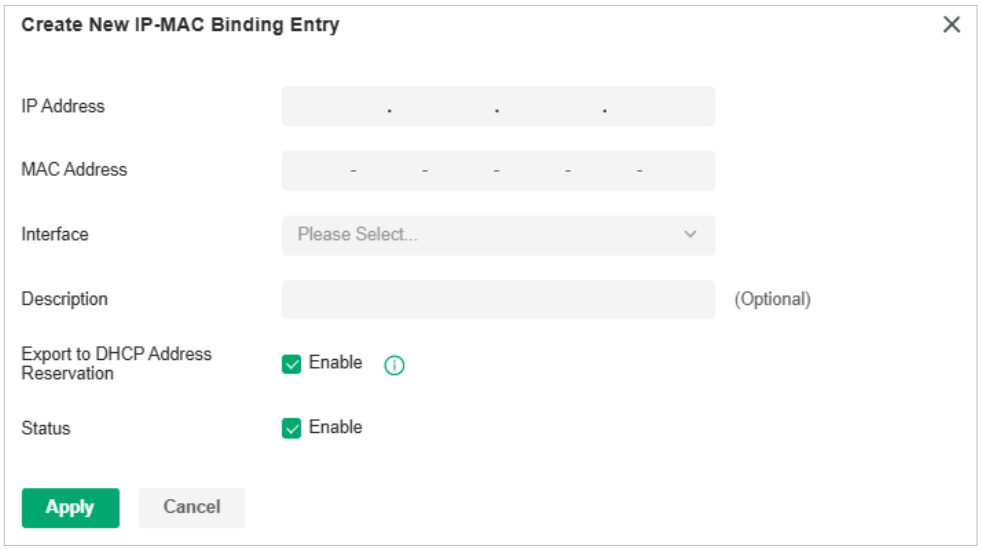
Configuration

1. Launch the controller and access a site. Go to Settings > Network Security > IP-MAC Binding.
2. Enable ARP Spoofing Defense and configure general settings. Click Apply.



ARP Spoofing Defense	Check the box to globally enable ARP Spoofing Defense.
Interface	Select the interface on which the entries will take effect.
Permit the packets matching the IP-MAC Binding entries only	With this option enabled, when receiving a packet, the router will check whether the IP address, MAC address and receiving interface match any of the IP-MAC Binding entries. Only the matched packets will be forwarded. This feature can be enabled only when ARP Spoofing Defense is enabled.
Send GARP packets when ARP attack is detected	With this option enabled, the router will send GARP packets to the hosts if it detects ARP spoofing packets on the network. The GARP packets will inform the hosts of the correct ARP information, which is used to replace the wrong ARP information in the hosts. This feature can be enabled only when ARP Spoofing Defense is enabled.
Interval	Specify the time interval for sending GARP packets. The valid values are from 1 to 10000.

3. Click Create New IP-MAC Binding Entry and add an IP-MAC binding entry. Click Apply.



IP Address	Specify the IP address to be bound.
MAC Address	Specify the MAC address to be bound.
Interface	Select the interface on which the entries will take effect.
Description	Enter a description for identification.
Status	Enable the entry. Only when the status is enabled will the entry take effect.

4. 4. 7 IDS/IPS

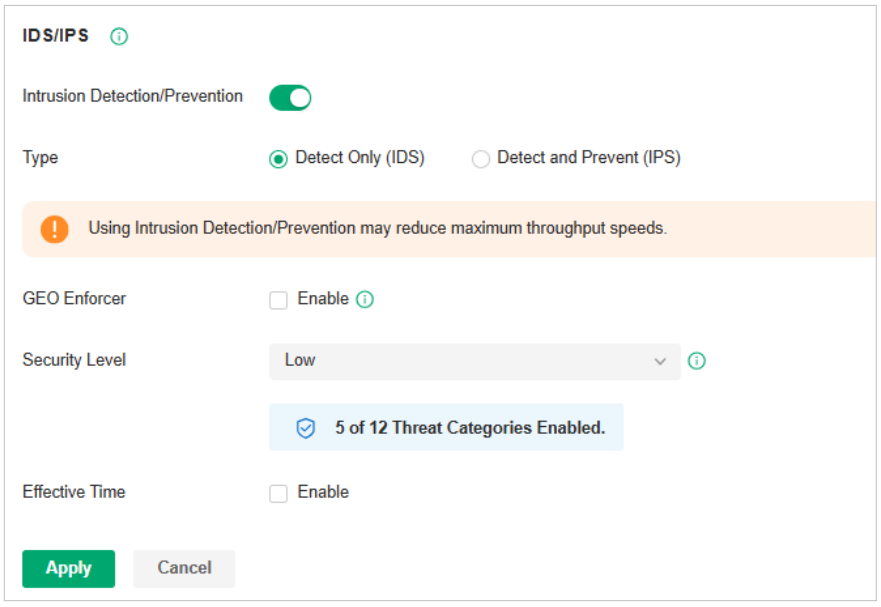
Overview

IDS/IPS is a security mechanism that detects intrusions based on attack characteristics. It can detect malware, Trojan horses, worms, ActiveX and other attacks to protect the network security of users.

Note: Using Intrusion Detection/Prevention may reduce maximum throughput speeds.

Configure IDS/IPS

1. Launch the controller and access a site. Go to Settings > Network Security > IDS/IPS.
2. Enable Intrusion Detection/Prevention and configure the parameters.



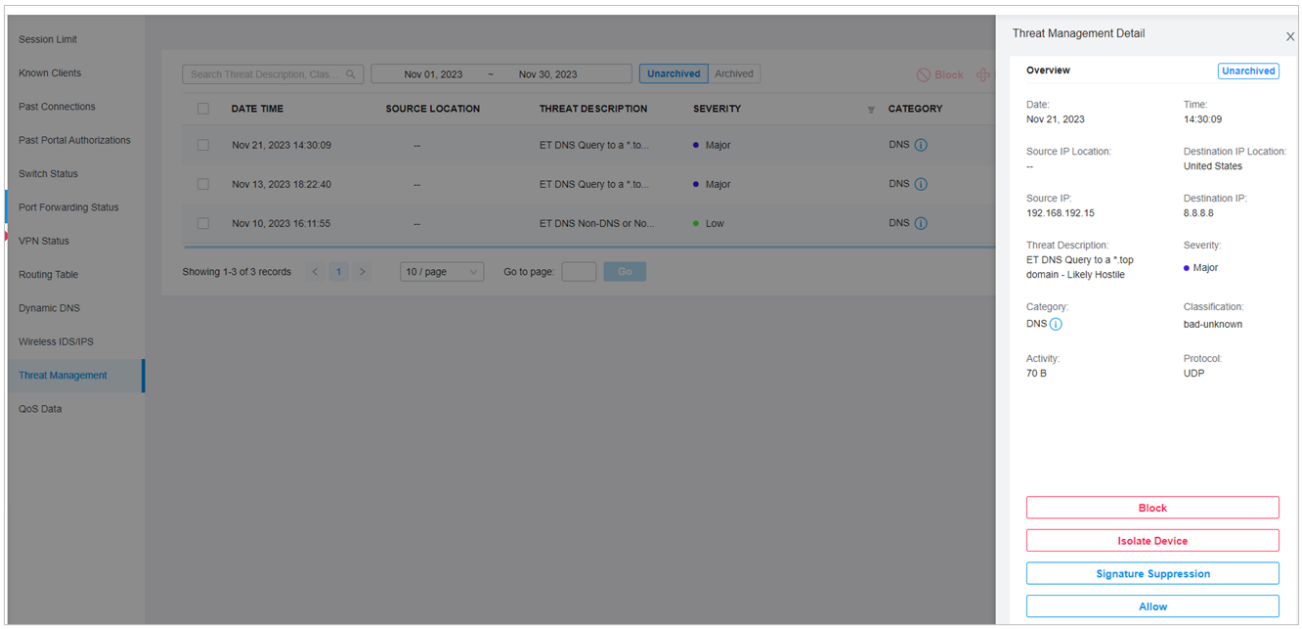
Type	Specify the working mode. In IDS mode, the system will only report the threat log. In IPS mode, the system will block the corresponding connection for 300s after a threat is detected.
GEO Enforcer	Enable geographic location identification of threat logs.
Security Level	Choose the protection level. A higher protection level means more threat types are detected, while a lower protection level only detects some important threats. You can also customize the protection level.
Effective Time	Specify the effective time period of the IDS/IPS module.

3. Apply the settings.

   When the system discovers a threat, the corresponding threat log will be displayed on the Insights > Threat Management page.

Manage Threats in a Site

1. Launch the controller and access a site. Go to Insights > Threat Management.
2. Click a threat that the system discovered, then you can choose a specified response strategy for the corresponding attack IP: Block, Isolate Device, Signature Suppression, or Allow.



Block	Drop traffic to/from the external IP address and the specific internal IP address. If you block an entry, it will be added to the Block List at Settings > Network Security > IDS/IPS.
Isolate Device	Drop traffic to/from the external IP address and any internal IP address.
Signature Suppression	Mute the alerting on certain signatures. This will also disable blocking on traffic matching the designated suppression rule. If you suppress the signature of an entry, it will be added to the Signature Suppression list at Settings > Network Security > IDS/IPS.
Allow	Trust the IP address so that the traffic, depending on the direction selected, will not get blocked to or from the identified IP address. If you allow an entry, it will be added to the Allow List at Settings > Network Security > IDS/IPS.

3. You can further check and edit processed entries at Settings > Network Security > IDS/IPS.

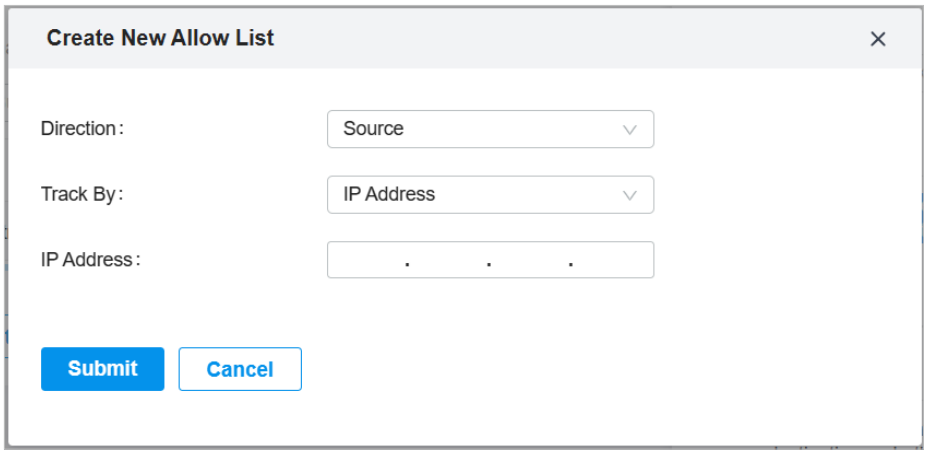
- **Block List**

  The Block List page displays all block entries added through the Threat Management page. You can choose to block all traffic of the source IP in the threat log, or block all traffic between the source IP and the destination IP in the threat log.

- **Allow List**

  On the Allow List page, you can add, view, and edit the exemption entries of IDS/IPS detection, so that the specified objects will no longer trigger threat logs.

  Click Create New Allow List and configure the parameters.



Direction	Specify the location of the object (target) exempt from triggering the threat: source, destination, or both directions.
Track By	Specify the type of object (target) exempt from triggering the threat: IP address, Network, or Subnet.
IP Address/Network/ Subnet	Specify the value of the object.

- **Signature Suppression**

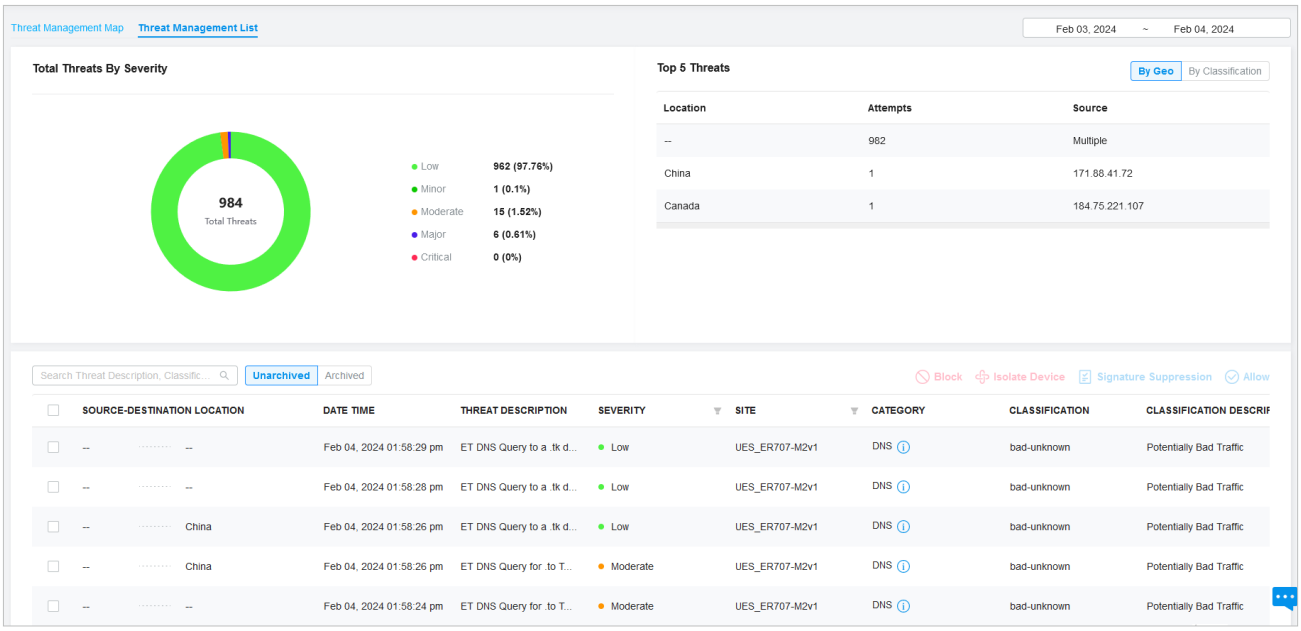
  The Signature Suppression page displays all the signature suppression entries added through the Threat Management page, and the objects with signature suppressed will no longer trigger specific threat logs.

Manage Threats Globally

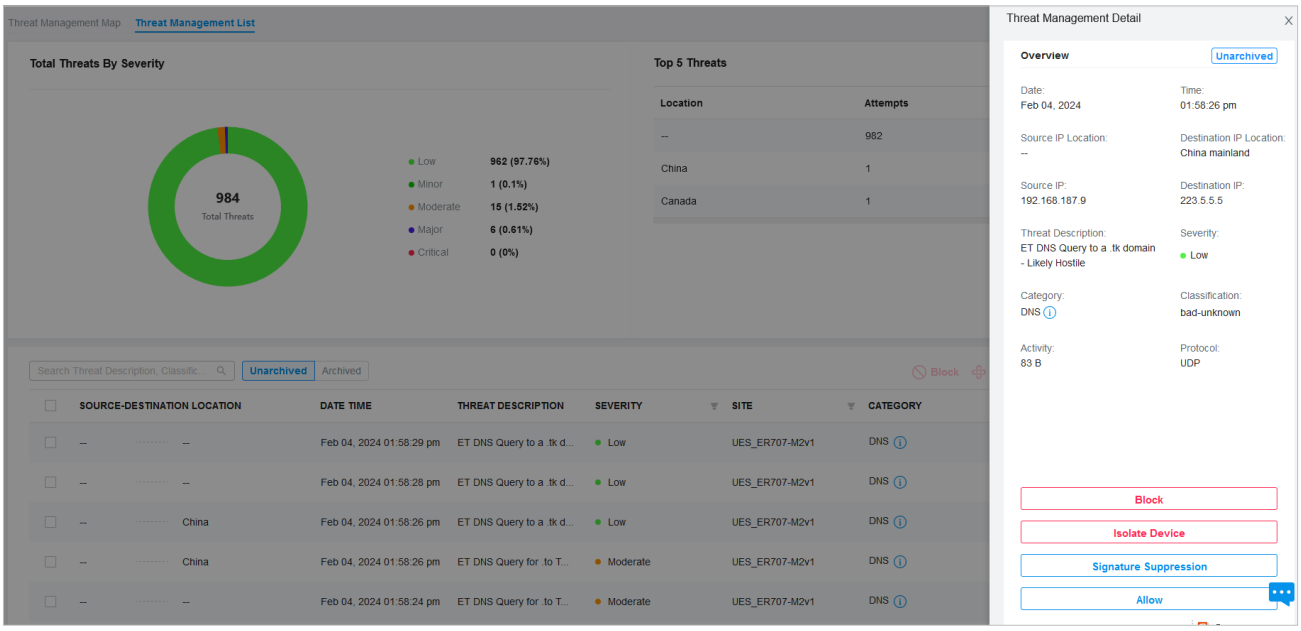
In Global view, go to Security.

- **Threat Management List**

In the Threat Management List, you can check top threats by severity, locations of top threats, and unarchived and archived threats.



In the unarchived threat list, click an entry, then you can choose a specified response strategy for the corresponding attack IP: Block, Isolate Device, Signature Suppression, or Allow.



Block	Drop traffic to/from the external IP address and the specific internal IP address. If you block an entry, it will be added to the Block List at Settings > Network Security > IDS/IPS.
Isolate Device	Drop traffic to/from the external IP address and any internal IP address.

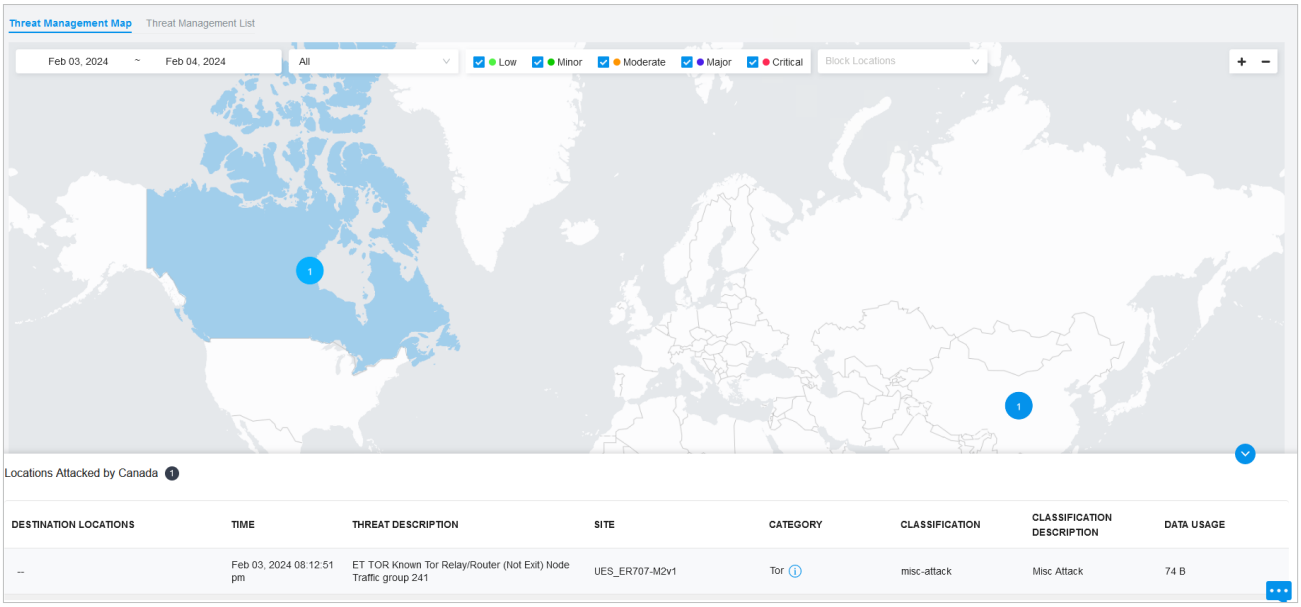
Signature Suppression	Mute the alerting on certain signatures. This will also disable blocking on traffic matching the designated suppression rule. If you suppress the signature of an entry, it will be added to the Signature Suppression list at Settings > Network Security > IDS/IPS.
Allow	Trust the IP address so that the traffic, depending on the direction selected, will not get blocked to or from the identified IP address. If you allow an entry, it will be added to the Allow List at Settings > Network Security > IDS/IPS.

- **Threat Management Map**

In the Threat Management Map, you can view the threat sources and numbers of attacks that the system has discovered. You can click a number in the map to view attack details.

You can right-click a location to block its attack events and manage the Block Locations list.

If excessive attacks have been detected, you can choose specific severity levels to display.



4. 4. 8 Application Control

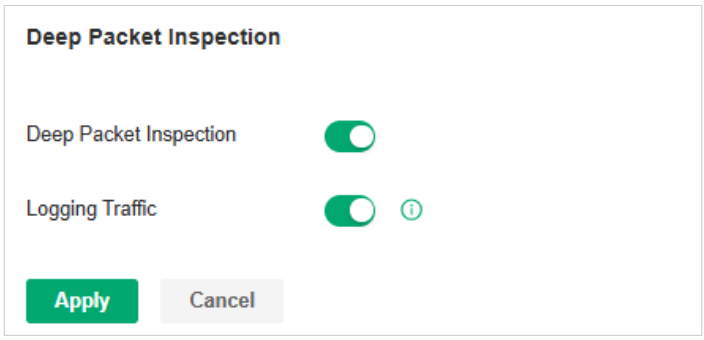
Overview

DPI (Deep Packet Inspection) helps you identify, analyze, and control the traffic at the application layer in the network. DPI engine includes the latest application identification signatures to track which applications are using the most bandwidth. You can better manage and distribute network traffic usage through DPI.

Configuration

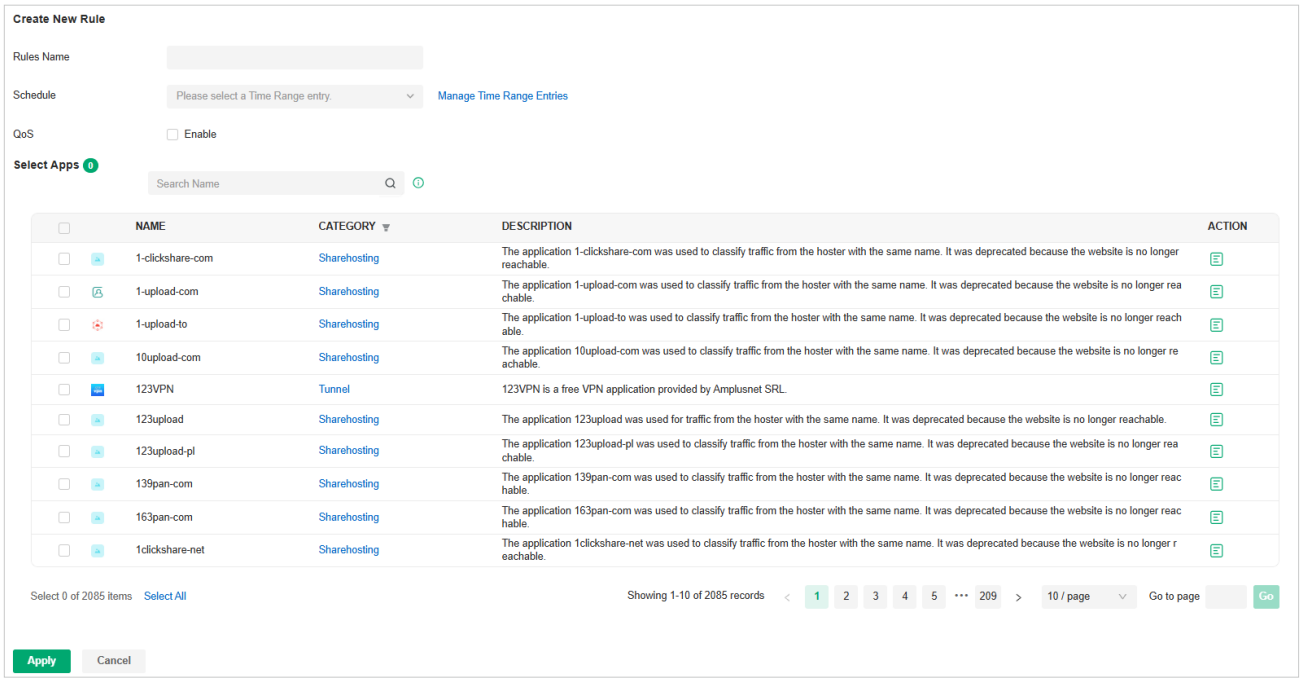
1. Launch the controller and access a site. Go to Settings > Network Security > Application Control.

2. On the Deep Packet Inspection page, enable Deep Packet Inspection and Logging Traffic, then apply the settings.



Deep Packet Inspection	When enabled, the device will send the forwarded traffic to a professional local DPI engine for analysis, so as to judge and identify the type of traffic.
Logging Traffic	When enabled, the device will collect and save the results of traffic analysis. You can check the results on the Statistics > Application Analytics page.

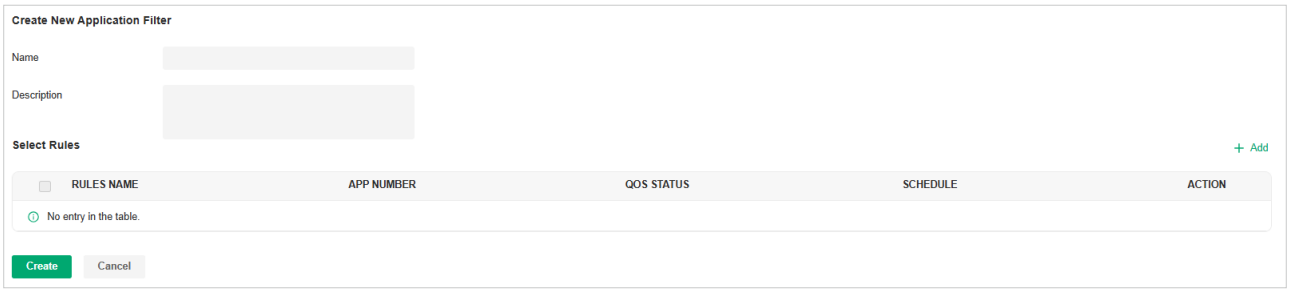
3. Apply the settings.
4. On the Rules Management page, click Create New Rule. You can predefine one or more rules, and APP control strategy that can be referenced, and realize block or QoS actions for specified Apps within a specified time period.



Rule Name	Specify the name of the rule.

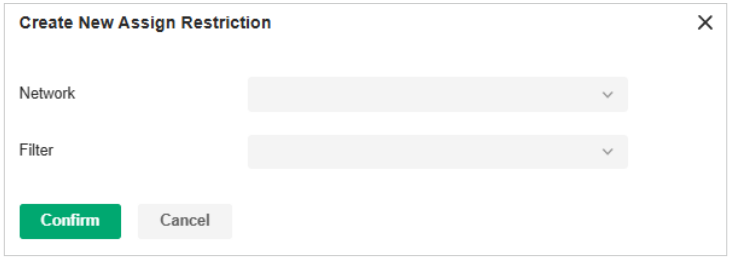
Schedule	Specify the time period when the rule takes effect. You can create new time range according to your needs.
QoS	Enable this option and select QoS Class to configure the QoS strategy if needed. When enabled, the traffic will be limited according to the configuration. When disabled, the App will be blocked.
Select Apps	Select the Apps for the rule.

5. On the Application Filter page, click Create New Application Filter. You can apply the defined rules and divide multiple rules into one filter set for easy management.



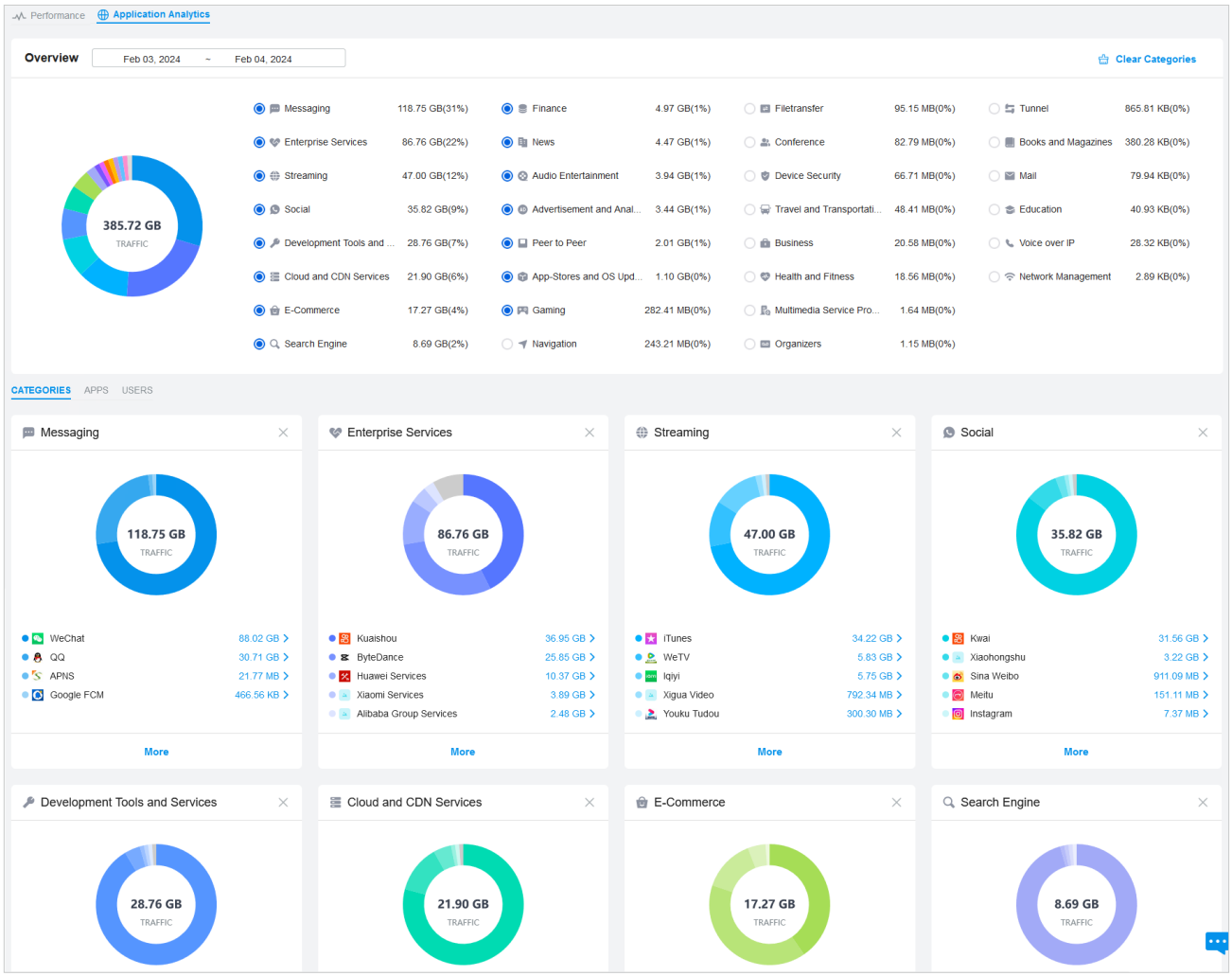
Name	Specify the name of the filter.
Description	Enter a description for identification.
Select Rules	Select the rules for the filter.

6. On the Deep Packet Inspection page, click Create New Assign Restriction. Select a network to apply a pre-defined filter.



Network	Select a network to apply the filter.
Filter	Select a pre-defined filter.

7. Save the settings. You can view the results of traffic analysis on the Statistics > Application Analytics page.



If you want to clear DPI data of a time period, go to the Deep Packet Inspection page, click the Clear Data button and specify the period.

4. 5 Transmission

Transmission helps you control network traffic in multiple ways. You can add policies and rules to control transmission routes and limit the session and bandwidth.

4. 5. 1 Routing

Overview

- **Static Route**

  Network traffic is oriented to a specific destination, and Static Route designates the next hop or interface where to forward the traffic.

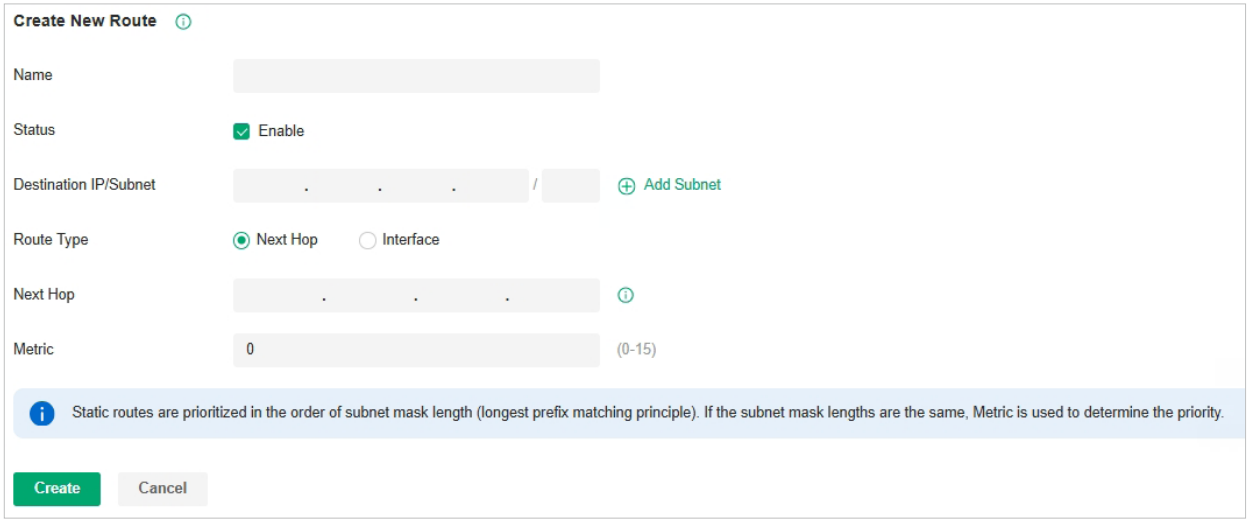
- **Policy Routing**

  Policy Routing designates which WAN port the router uses to forward the traffic based on the source, the destination, and the protocol of the traffic.

Configuration

- **Static Route**

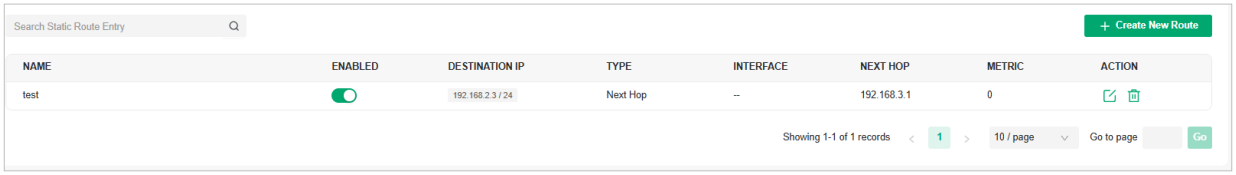
  1. Go to Settings > Transmission > Routing > Static Route. Click Create New Route to load the following page and configure the parameters.



Name	Enter the name to identify the Static Route entry.
Status	Enable or disable the Static Route entry.
Destination IP/Subnet	Destination IP/Subnet identifies the network traffic which the Static Route entry controls. Specify the destination of the network traffic in the format of 192.168.0.1/24. You can click Add Subnet to specify multiple Destination IP/Subnets and click the Delete icon to delete them.

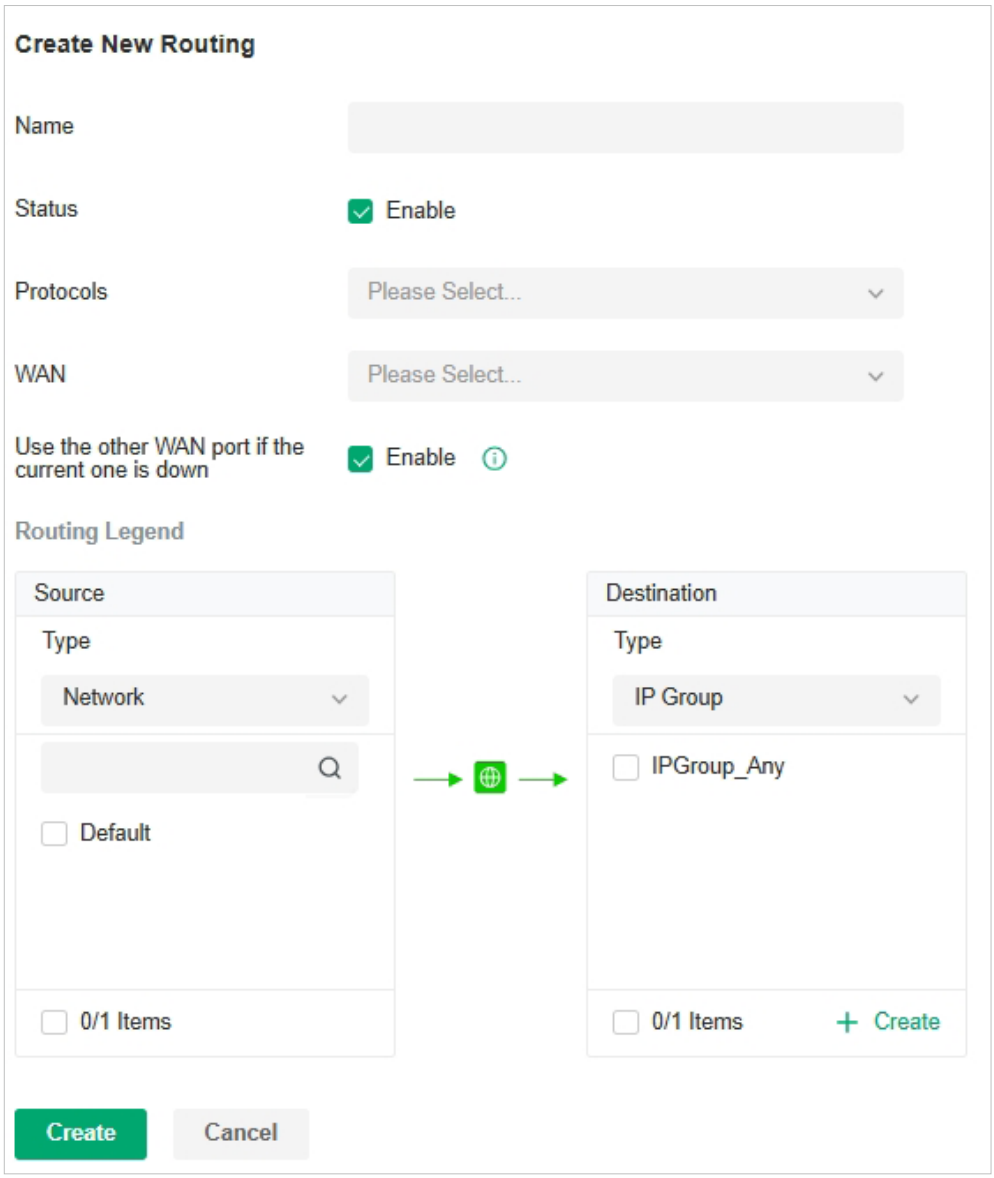
Route Type	Next Hop: With Next Hop selected, your devices forward the corresponding network traffic to a specific IP address. You need to specify the IP address as Next Hop. Interface: With Interface selected, your devices forward the corresponding network traffic through a specific interface. You need to specify the Interface according to your needs.
Metric	Define the priority of the Static Route entry. A smaller value means a higher priority. If multiple entries match the Destination IP/Subnet of the traffic, the entry of higher priority takes precedence. In general, you can simply keep the default value.

2. Click Create. The new Static Route entry is added to the table. You can click the Edit icon to edit the entry. You can click the Delete icon to delete the entry.



Policy Routing

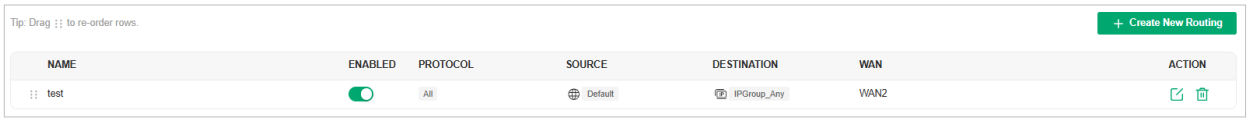
1. Go to Settings > Transmission > Routing > Policy Routing. Click Create New Routing to load the following page and configure the parameters.



Name	Enter the name to identify the Policy Routing entry.
Status	Enable or disable the Policy Routing entry.
Protocols	Select the protocols of the traffic which the Policy Routing entry controls. The Policy Routing entry takes effect only when the traffic matches the criteria of the entry including the protocols.
WAN	Select the WAN port to forward the traffic through. If you want to forward the traffic through the other WAN port when the current WAN is down, enable Use the other WAN port if the current WAN is down.

Routing Legend	The Policy Routing entry takes effect only when the traffic using specified protocols matches the source and destination which are specified in the Routing Legend. Select the type of the traffic source and destination. Network: Select the network interfaces for the traffic source or destination. IP Group: Select the IP Group for the traffic source or destination. You can click + Create to create a new IP Group. IP-Port Group: Select the IP-Port Group for the traffic source or destination. You can click + Create to create a new IP-Port Group. Location Group: Select the Location Group for the traffic destination. You can click + Create to create a new Location Group. Domain Group: Select the Domain Group for the traffic destination. You can click + Create to create a new Domain Group.

2. Click Create. The new Policy Routing entry is added to the table. You can click the Edit icon to edit the entry. You can click the Delete to delete the entry.



4. 5. 2 Switch OSPF

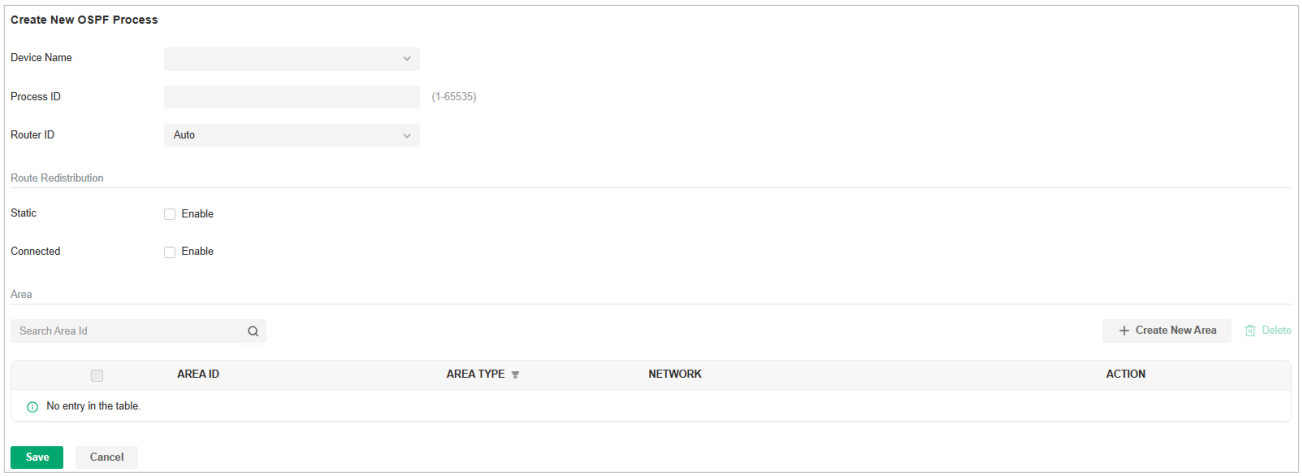
Overview

The OSPF protocol (Open Shortest Path First) is a link-state-based dynamic routing protocol that uses Dijkstra's SPF (shortest path first) algorithm to calculate routes within a single AS (autonomous system). OSPF establishes a link state database by advertising the state of network interfaces between routers, and generates shortest path trees. Other OSPF routers in the area use these shortest paths to construct routes.

- **OSPF Process**

On this page, you can configure the process of the dynamic routing protocol to divide the local router into multiple virtual networks. The configurations only work for the local router.

1. Go to Settings > Transmission > Switch OSPF.
2. In OSPF Process, click Create New OSPF Process.
3. Configure the parameters and apply the settings.

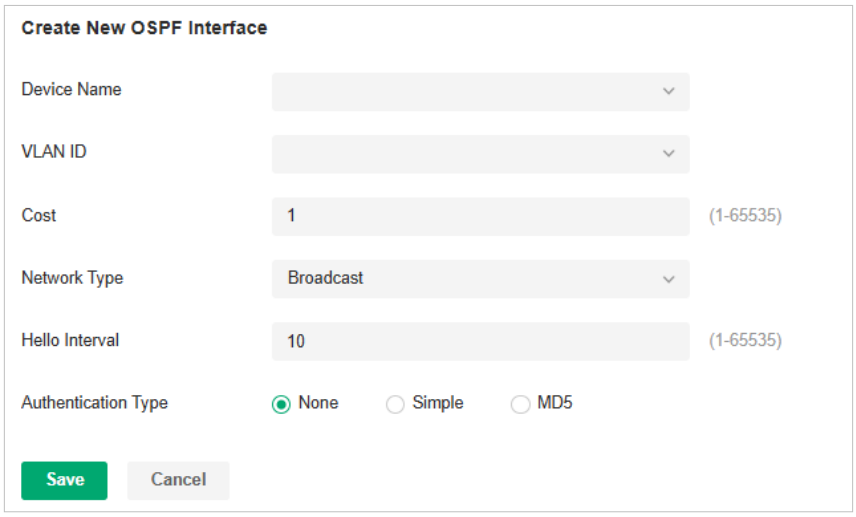


Device Name	Specify the name of the OSPF process.
Process ID	Enter a number between 1 and 65535 to identify the OSPF process locally on the router.
Router ID	Specify the identity of the router. The selection priority order is manually configured interface, loopback interface, then physical interface.
Static	Check the box to enable static route. With this option selected, configure the following parameters: Metric: Specify the path cost when importing external routes. Metric Type: Specify the cost calculation type. Type 1 calculates internal cost and external cost. Type 2 calculates external cost only. The default value is type 2.
Connected	Check the box to enable direct route.
Area	Configure the OSPF areas.

■ OSPF Interface

On this page, you can divide the router into areas and set their OSPF parameters.

1. Go to Settings > Transmission > Switch OSPF.
2. In OSPF Interface, click Create New OSPF Interface.
3. Configure the parameters and apply the settings.



Device Name	Specify the name of the OSPF interface.
VLAN ID	Specify the ID of the VLAN.
Cost	Specify the interface overhead.
Network Type	Specify the network type of the OSPF interface.
Hello Interval	Specify the interval between Hello packets sent on the interface.
Authentication Type	Specify the interface area verification method. None: No authentication. Simple: Simple authentication mode. The key is transmitted with clear texts. With this option selected, specify the Simple Key for authentication. MD5: MD5 authentication mode. The key and key ID are transmitted through MD5 encryption. With this option selected, specify the MD5 Key ID and MD5 Key for authentication.

4. 5. 3 NAT

Overview

- **Port Forwarding**

  You can configure Port Forwarding to allow internet users to access local hosts or use network services which are deployed in the LAN.

  Port Forwarding helps establish network connections between a host on the internet and the other in the LAN by letting the traffic pass through the specific port of the gateway. Without Port Forwarding, hosts in the LAN are typically inaccessible from the internet for the sake of security.

- **ALG**

  ALG ensures that certain application-level protocols function appropriately through your gateway.

- **One-to-One NAT**

  One-to-One NAT will establish a correspondence between a private IP and a public IP, allowing access to the device with the private IP through the corresponding public IP.

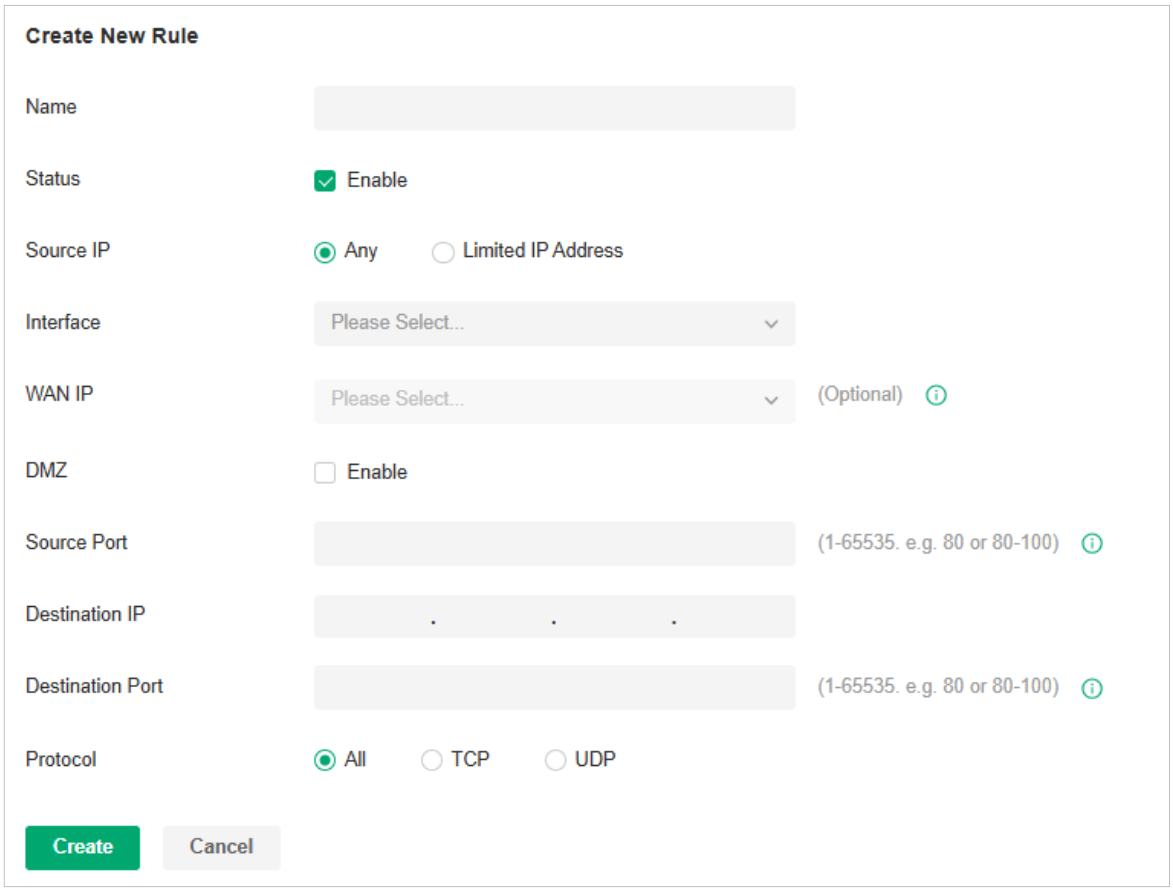
- **Disable NAT**

  Disable NAT allows internal devices to obtain public IP addresses.

Configuration

- **Port Forwarding**

1. Go to Settings > Transmission > NAT > Port Forwarding. Click Create New Rule to load the following page and configure the parameters.



Name	Enter the name to identify the Port Forwarding rule.
Status	Enable or disable the Port Forwarding rule.
Source IP	Any: The rule applies to traffic from any source IP address. Limited IP Address: The rule only applies to traffic from specific IP addresses. With this option selected, specify the IP addresses and subnets according to your needs.

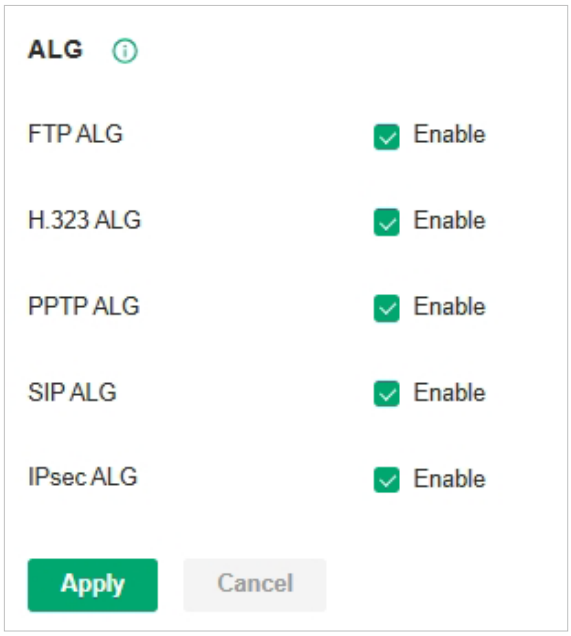
Interface	Select the interface which the rule applies to. Traffic which is received through the interface is forwarded according to the rule.
DMZ	With DMZ enabled, all the traffic is forwarded to the Destination IP in the LAN, port to port. You need to specify the Destination IP. With DMZ disabled, only the traffic which matches the Source Port and the Protocol is forwarded. The traffic is forwarded to the Destination Port of the Destination IP in the LAN. You need to specify the Source Port, Destination IP, Destination Port, and Protocol.
Source Port	The gateway uses the Source Port to receive the traffic from the internet. Only the traffic which matches the Source Port and the Protocol is forwarded.
Destination IP	The traffic is forwarded to the host of the Destination IP in the LAN.
Destination Port	The traffic is forwarded to the Destination Port of the host in the LAN.
Protocol	Network traffic is transmitted using either TCP or UDP protocol. Only the traffic which matches the Source Port and the Protocol is forwarded. If you want both TCP traffic and UDP traffic to be forwarded, select All.

2. Click Create. The new Port Forwarding entry is added to the table. You can click the Edit icon to edit the entry. You can click the Delete icon to delete the entry.



■ ALG

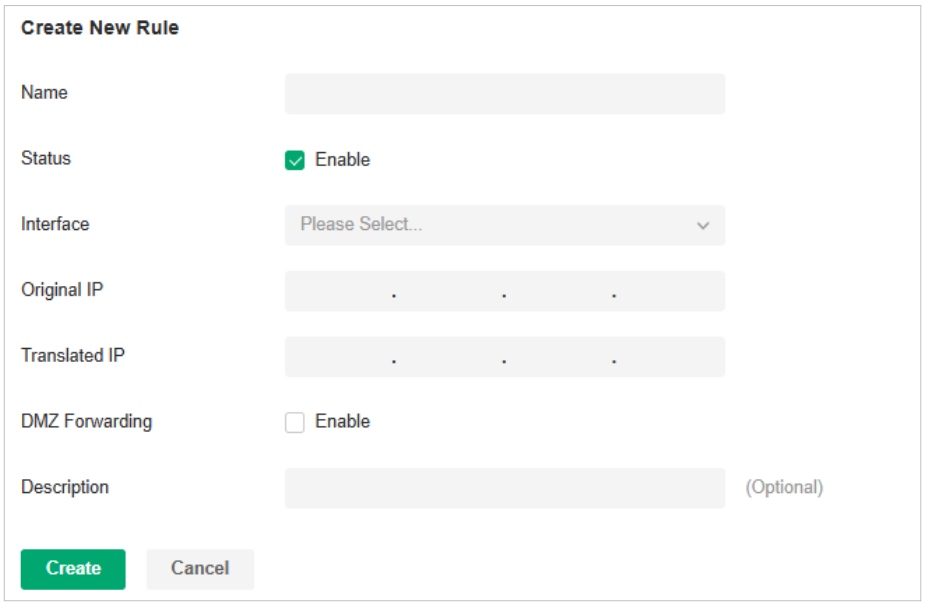
Go to Settings > Transmission > NAT > ALG. Enable or disable certain types of ALG according to your needs and click Apply.



FTP ALG	FTP ALG allows the FTP server and client to transfer data using the FTP protocol in one of the following scenarios: • The FTP server is in the LAN, while the FTP client is on the internet. • The FTP server is on the internet, while the FTP client is in the LAN. • The FTP server and FTP client are in different LANs.
H.323 ALG	H.323 ALG allows the IP phones and multimedia devices to set up connections using the H.323 protocol in one of the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.
PPTP ALG	PPTP ALG allows the PPTP server and client to set up a PPTP VPN in one of the following scenarios: • The PPTP server is in the LAN, while the PPTP client is on the internet. • The PPTP server is on the internet, while the PPTP client is in the LAN. • The PPTP server and PPTP client are in different LANs.
SIP ALG	SIP ALG allows the IP phones and multimedia devices to set up connections using the SIP protocol in one of the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.
IPsec ALG	IPsec ALG allows the IPsec endpoints to set up an IPsec VPN in one of the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.

One-to-One NAT

1. Go to Settings > Transmission > NAT > One-to-One NAT. Click Create New Rule to load the following page and configure the parameters.

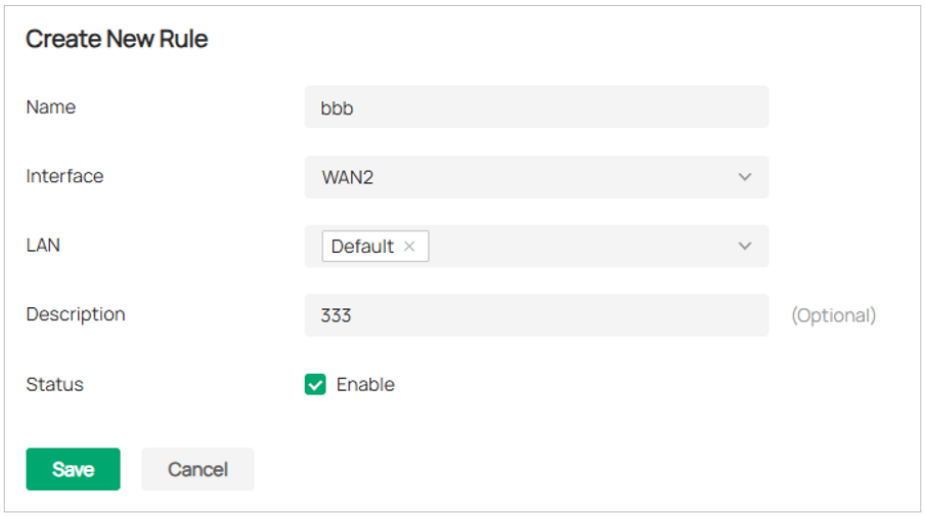


Name	Enter the name to identify the one-to-one NAT rule.
Status	Enable or disable the one-to-one NAT rule.
Interface	Specify the effective interface for the rule only when the connection type is Static IP.
Original IP	Specify the original IP address for the rule, which means the device's private IP. The original IP address cannot be the broadcast address, network segment or interface IP. With One-to-One NAT enabled, the original IP will map to the translated IP.
Translated IP	Specify the translated IP address for the rule, which means the public IP of device. The translated IP address cannot be the broadcast address, network segment or interface IP. With One-to-One NAT enabled, the original IP will map to the translated IP.
DMZ Forwarding	Choose to enable DMZ Forwarding. The packets transmitted to the translated IP address will be forwarded to the host with the original IP address if DMZ Forwarding is enabled.
Description	(Optional) Enter a description for identification.

2. Click Create to add the one-to-one NAT rule.

- **Disable NAT**

1. Go to Settings > Transmission > NAT > Disable NAT. Click Create New Rule to load the following page and configure the parameters.



Name	Enter a name to identify the rule.
Interface	Specify the effective interface for the rule.
LAN	Specify the effective LAN network for the rule.
Description	(Optional) Enter a description for identification.
Status	Enable or disable the rule.

2. Click Create to add the Disable NAT rule.

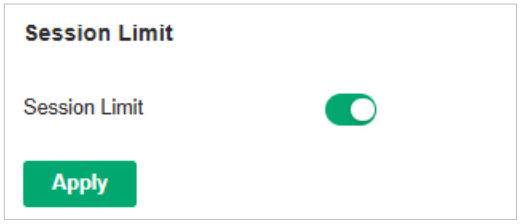
4. 5. 4 Session Limit

Overview

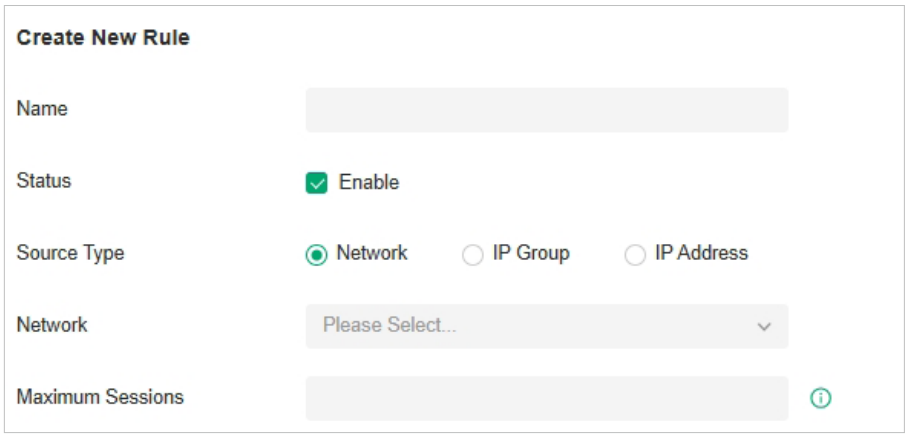
Session Limit optimizes network performance by limiting the maximum sessions of specific sources.

Configuration

1. Go to Settings > Transmission > Session Limit. In Session Limit, enable Session Limit globally and click Apply.



2. In Session Limit Rule List, click Create New Rule to load the following page and configure the parameters.



Name	Enter the name to identify the Session Limit rule.
Status	Enable or disable the Session Limit rule.
Source Type	Network: Limit the maximum sessions of specific LAN networks. With this option selected, select the networks, which you can customize in Wired Networks > LAN Networks. For detailed configuration of networks, refer to 4. 2. 2 Configure LAN Networks. IP Group: Limit the maximum sessions of specific IP Groups. With this option selected, select the IP Groups, which you can customize in Profiles > Groups. For detailed configuration of IP groups, refer to 4. 7 Create Profiles.
Maximum Sessions	Enter the maximum sessions of the specific sources.

3. Click Save. The new Session Limit rule is added to the list. You can click the Edit icon to edit the rule. You can click the Delete icon to delete the rule.



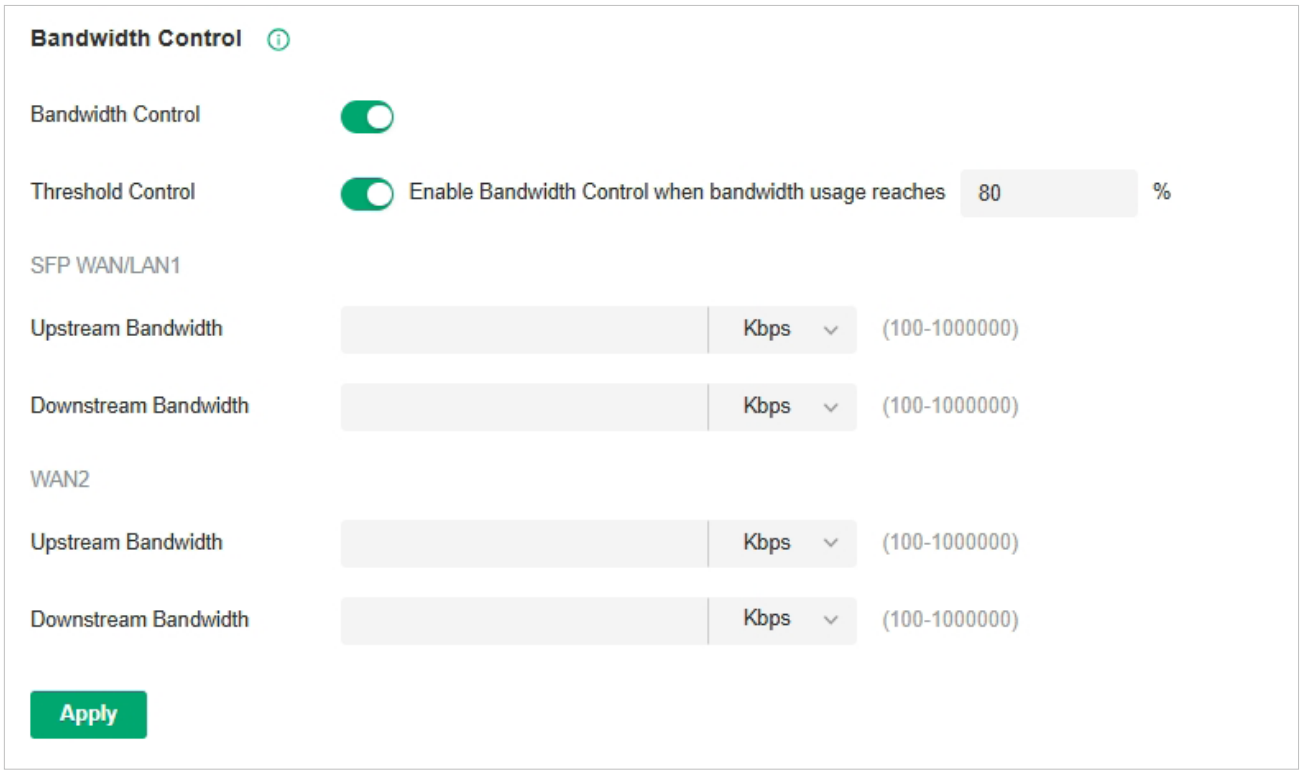
4. 5. 5 Bandwidth Control

Overview

Bandwidth Control optimizes network performance by limiting the bandwidth of specific sources.

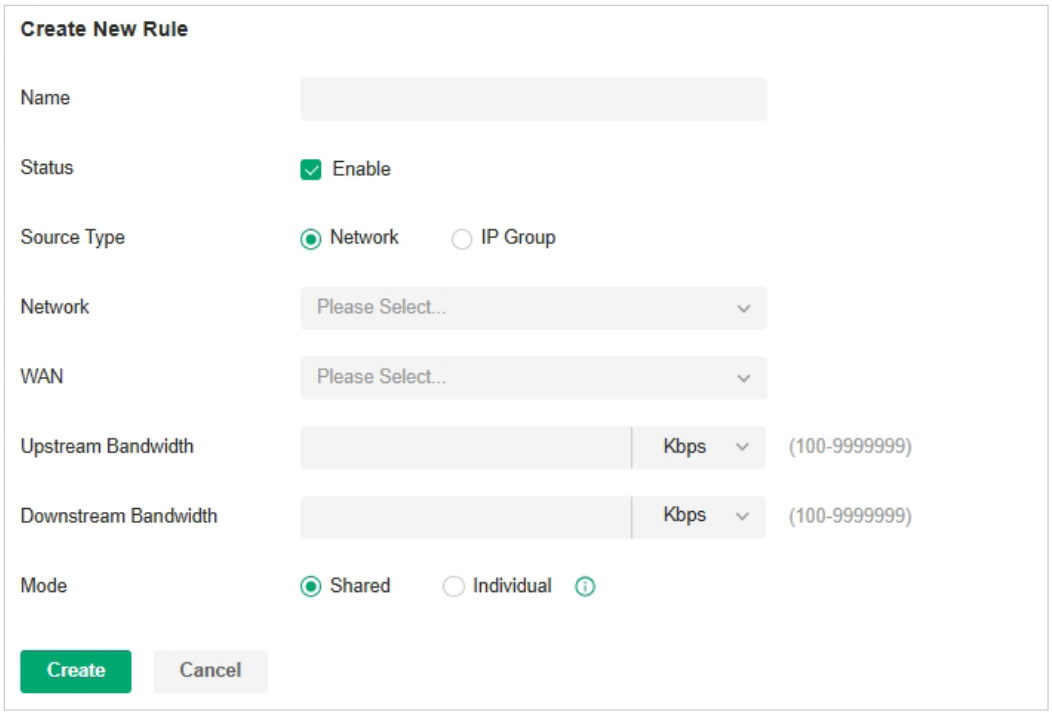
Configuration

1. Go to Settings > Transmission > Bandwidth Control. In Bandwidth Control, enable Bandwidth Control globally and configure the parameters. Then click Apply.



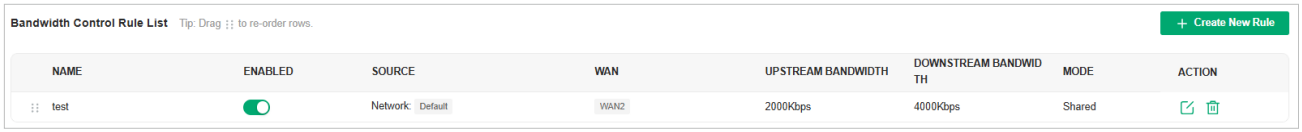
Threshold Control	With Threshold Control enabled, Bandwidth Control takes effect only when total bandwidth usage reaches the specified percentage. You need to specify the total Upstream Bandwidth and Downstream Bandwidth of the WAN ports. It's recommended to use the Test Speed tool to decide the actual Upstream Bandwidth and Downstream Bandwidth.

2. In Bandwidth Control Rule List, click Create New Rule to load the following page and configure the parameters.



Name	Enter the name to identify the Bandwidth Control rule.
Status	Enable or disable the Bandwidth Control rule.
Source Type	Network: Limit the maximum bandwidth of specific LAN networks. With this option selected, select the networks, which you can customize in Wired Networks > LAN Networks. For detailed configuration of networks, refer to 4. 2. 2 Configure LAN Networks. IP Group: Limit the maximum bandwidth of specific IP Groups. With this option selected, select the IP Groups, which you can customize in Profiles > Groups. For detailed configuration of IP groups, refer to 4. 7 Create Profiles.
WAN	Select the WAN port which the rule applies to.
Upstream Bandwidth	Specify the limit of Upstream Bandwidth, which the specific local hosts use to transmit traffic to the internet through the gateway.
Downstream Bandwidth	Specify the limit of Downstream Bandwidth, which the specific local hosts use to receive traffic from the internet through the gateway.
Mode	Specify the bandwidth control mode for the specific local hosts. Shared: The total bandwidth for all the local hosts is equal to the specified values. Individual: The bandwidth for each local host is equal to the specified values.

3. Click Create. The new Bandwidth Control rule is added to the list. You can click the Edit icon to edit the rule. You can click the Delete icon to delete the rule.

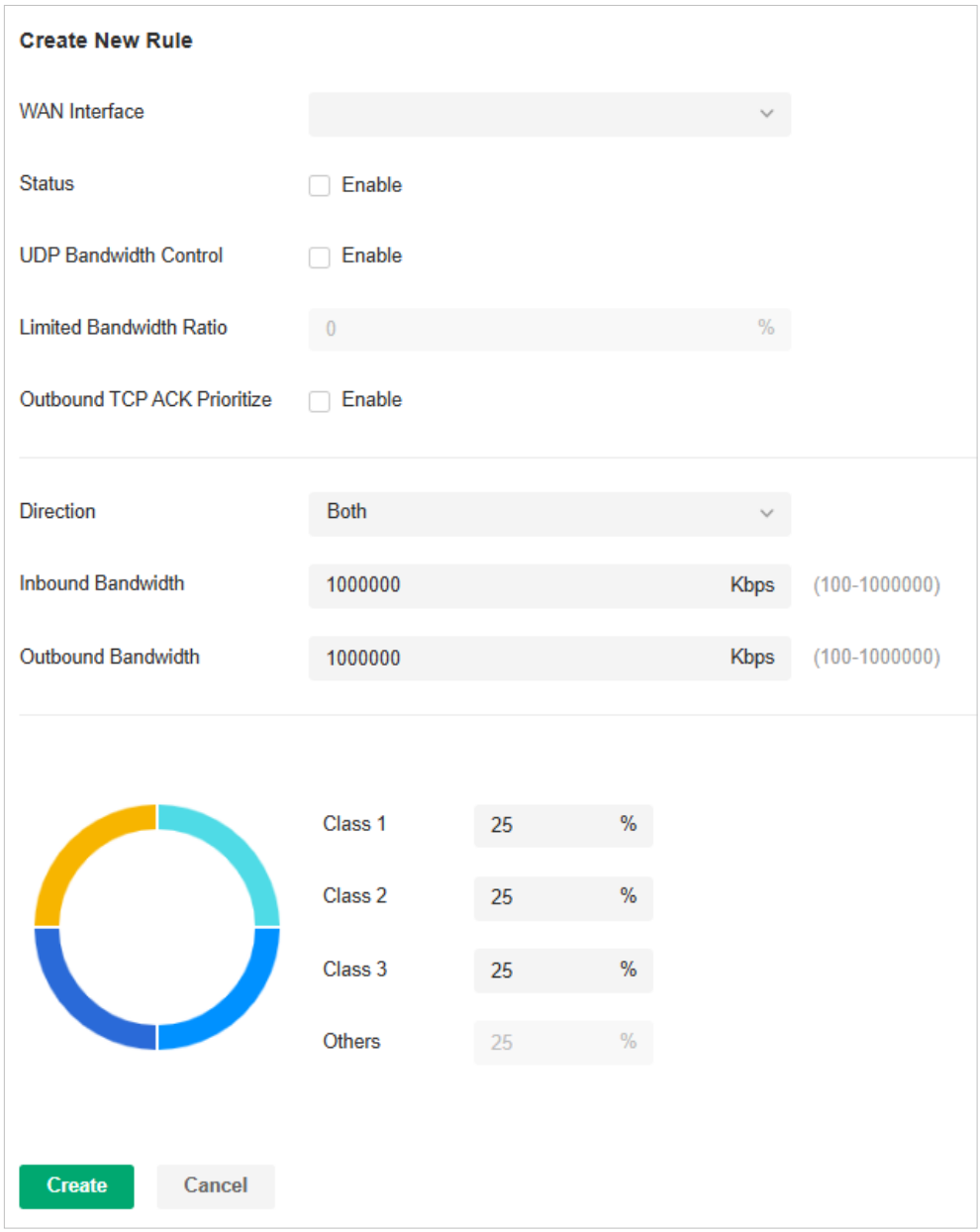


4. 5. 6 Gateway QoS

■ **Bandwidth Control**

This page allows you to configure rules to limit various data flows. In this way, you can optimize the network performance by reasonably utilizing the bandwidth.

1. Launch the controller and access a site. Go to Settings > Transmission > Gateway QoS.
2. Click Create New Rule.



3. Configure the parameters and click Apply.

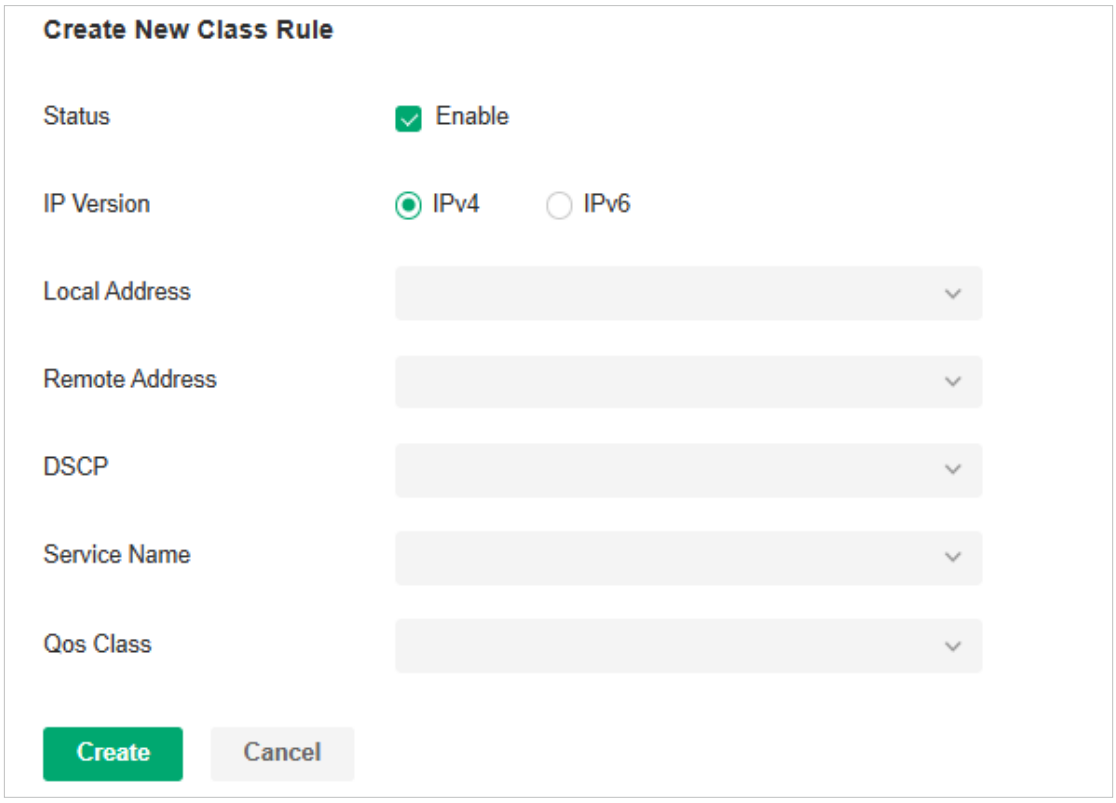
WAN Interface	Select the WAN port. You can configure the QoS rule for a WAN port only when the port is enabled.
Status	Enable or disable QoS for the current entry.
UDP Bandwidth Control	Check the box to enable UDP bandwidth control.
Limited Bandwidth Ratio	When UDP Bandwidth Control is enabled, specify the bandwidth ratio of UDP at each level of class1/2/3/other.
Outbound TCP ACK Prioritize	Check the box to prioritize outbound TCP ACK packets. This function ensures that traffic is not slowed down by remote hosts waiting for ACK packets before sending further traffic.

Direction	Specify the direction of the controlled traffic. “out” means control sending packets. “in” means receiving packets. “both” means both are controlled.
Inbound/Outbound Bandwidth	Enter the maximum threshold of the inbound/outbound bandwidth.
Class1/Class2/Class3/ Others	Specify the proportion of the maximum bandwidth that Class1, Class2, Class3 and Others can occupy to limit the bandwidth usage of specific classification traffic.

■ Class Rule

This page allows you to add or delete class rules. Rules will be matched from top to bottom according to the rule sequence number. When the traffic matches a rule, it will be assigned to the corresponding class and will not continue to match down.

1. Launch the controller and access a site. Go to Settings > Transmission > Gateway QoS > Class Rule.
2. Click Create New Class Rule.



3. Configure the parameters and click Apply.

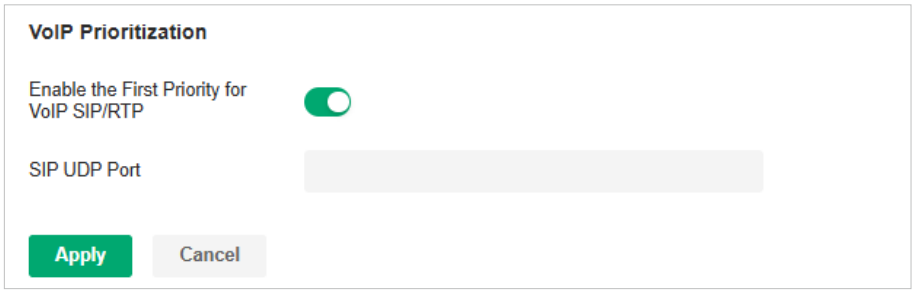
Status	Check the box to enable the rule.
IP Version	Specify the protocol version: IPv4 or IPv6.
Local Address	Match the source IP address of the traffic. For IPv4 protocol, you can use the IP Group object configured in the Profiles > Groups module. For the IPv6 protocol, you can use the IPv6 Group object configured in the Profiles > Groups module.

Remote Address	Match the destination IP address of the traffic. For IPv4 protocol, you can use the IP Group object configured in the Profiles > Groups module. For the IPv6 protocol, you can use the IPv6 Group object configured in the Profiles > Groups module.
DSCP	Match the DSCP value of the traffic: Any, IP procedure, AF, or EF.
Service Name	Match the port number of the traffic. Select the service type object defined in the Preference > Service Type module.
QoS Class	Select the category of traffic that meets the rule.

VoIP Prioritization

This page allows you to configure VoIP prioritization.

1. Launch the controller and access a site. Go to Settings > Transmission > Gateway QoS > VoIP Prioritization.
2. Enable the first priority for VoIP SIP/RTP and enter the SIP UDP port. Then apply the settings.

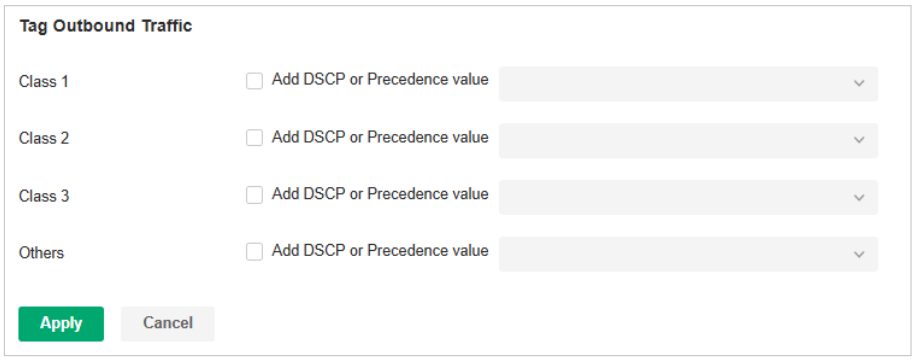


Enable the First Priority for VoIP SIP/RTP	Check the box to enable prioritize VoIP traffic.
SIP UDP Port	Enter the UDP port ID of the VoIP traffic.

Tag Outbound Traffic

This page allows you to add a DSCP or Precedence value for traffic in different classes.

1. Launch the controller and access a site. Go to Settings > Transmission > Gateway QoS > Tag Outbound Traffic.
2. Check the box for your desired class and select the DSCP or Precedence value.



Class 1/2/3/Others	Check the box and select the DSCP (Any, IP procedure, AF, or EF) or Precedence value for traffic.

4. 5. 7 Switch QoS

Overview

- **QoS Basic Settings**

QoS (Quality of Service) function is used to optimize network performance. Typically, networks treat all traffic equally on FIFO (First In First Out) delivery basis. When congestion occurs, the switch will drop the later packets no matter what kind of traffic they are. With QoS configured, the switch forwards traffic according to the priority of the packets. Critical traffic like VoIP and video conference can be preferentially treated.

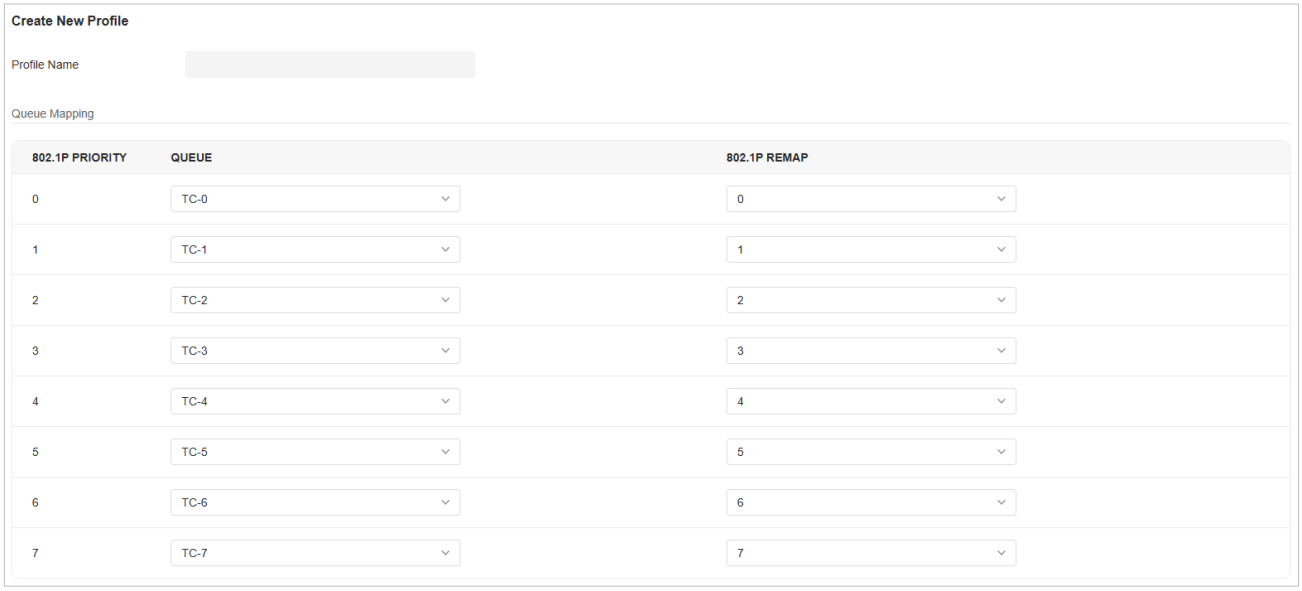
- **Queue Mapping & Scheduler Profile**

Queue Mapping function is used to classify the packets based on the value of 802.1p priority, then map them to different queues. IEEE 802.1p standard defines three bits in 802.1Q tag as PRI filed. The PRI values are called 802.1p priority and used to represent the priority of the layer 2 packets. This function requires packets with VLAN tags.

Scheduler Config function is used to set the scheduler rule for corresponding queue.

Configuration

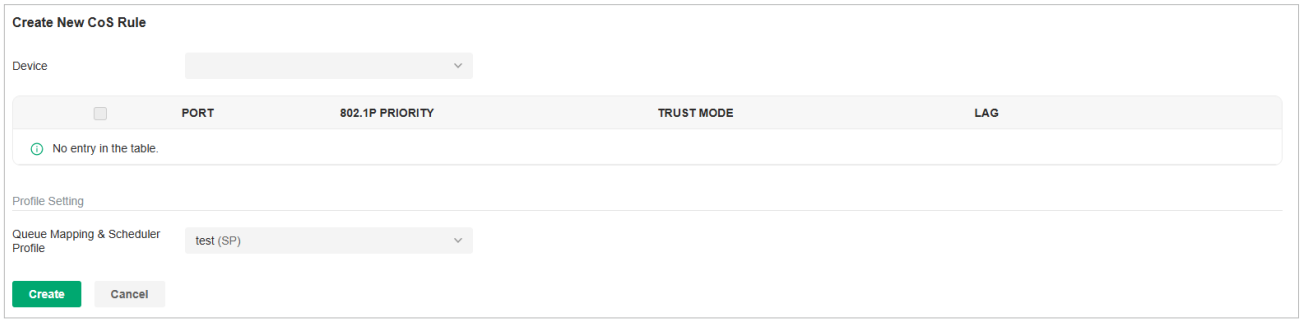
1. Go to Settings > Transmission > Switch QoS.
2. In Queue Mapping & Scheduler Profile, the system provides a default profile. You can also click Create New Profile to create a profile according to site needs.



Queue Mapping

Profile Name	Enter a name to identify the Queue Mapping & Scheduler Profile entry.
802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
802.1p Remap	802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the 802.1p priority of the packets, it will modify the value of packets 802.1p priority according to the map.Here you can view and configure 802.1p Remap.
Scheduler Config	
Queue TC-id	Displays the ID number of priority Queue.
Scheduler Type	Select the type of scheduling used for corresponding queue. When the network congestion occurs, the port will determine the forwarding sequence of the packets according to the type. Strict: In this mode, the switch will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. Weighted: In this mode, the switch will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight. **Note:** If the two scheduler types are both applied to a port, the queues in Strict mode will take precedence.
Queue Weight	Specify the queue weight for the desired queue. This value can be set only in the Weighted mode.

3. In QoS Basic Settings, click Create New Rule. Select a switch, configure the parameters and apply the settings.



Device	Select a device to config the CoS Rule.
Port	Select one or more ports to configure.
802.1p Priority	Specify the port-to-802.1p priority mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p-to-queue mappings.

Trust Mode	Select the Trust mode for the desired port. The switch will process the ingress packets according to the trusted priority mode. Untrusted: In this mode, the packets will be processed according to the port priority configuration. Trust 802.1p: In this mode, the packets will be processed according to the 802.1p priority configuration. Trust DSCP: In this mode, the packets will be processed according to the DSCP priority configuration.
LAG	Displays the LAG that the port belongs to.
Queue Mapping & Scheduler Profile	Select the Queue Mapping & Scheduler Profile to be bound.

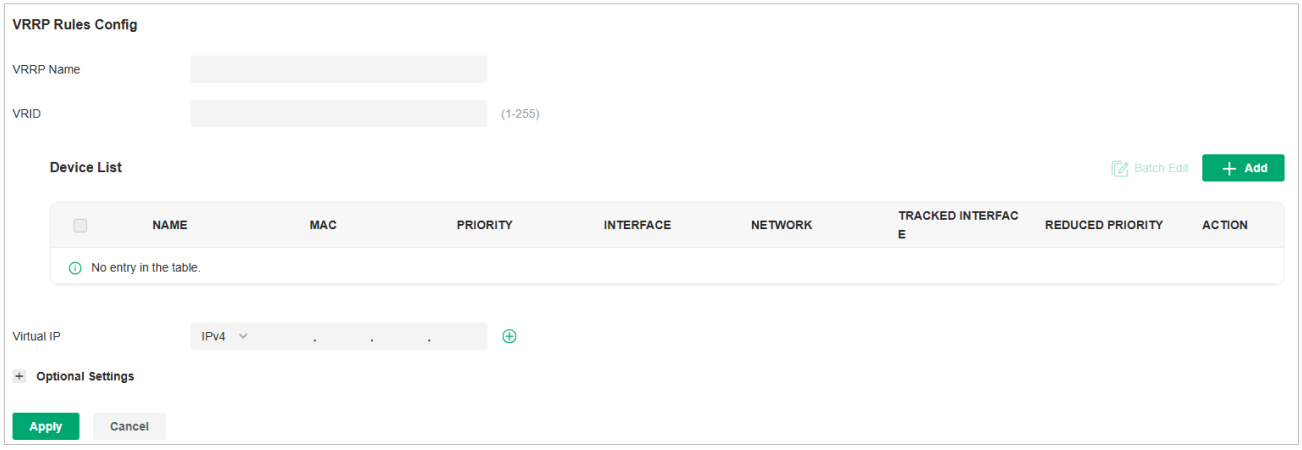
4. 5. 8 VRRP

Overview

VRRP or Virtual Routing Redundancy Protocol is a function on the switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts.

Configuration

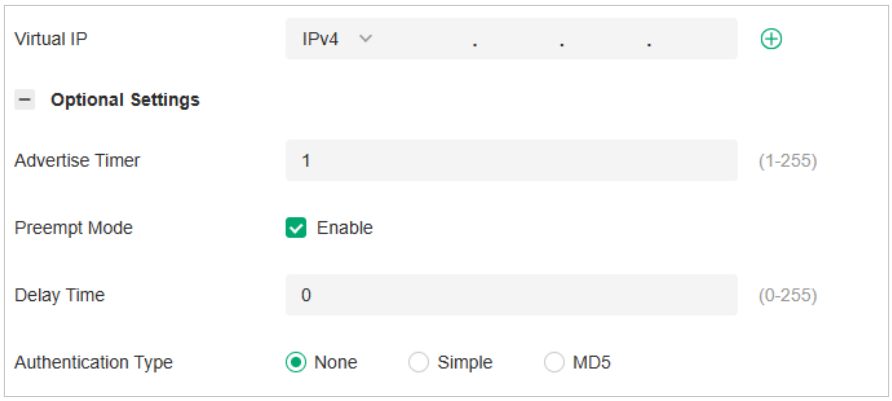
1. Go to Settings > Transmission > VRRP.
2. Click Create VRRP Rule. Set the VRRP Name and VRID.



VRRP Name	Enter a name to identify the rule.
VRID	Enter the VRID to create a new VRRP. The VRID ranges from 1 to 255.

Device List	Click Add to select a switch and configure device VRRP. The switch you add will display in the Device List. Device Name: Name of the device. MAC: MAC address of the device. Priority: Priority associated with the VRRP. It ranges from 1 to 254. Interface: Interface ID associated with the VRRP. Network: Intersection of device network (IP/mask). Tracked Interface: Interface to be tracked. Reduced Priority: Priority to reduce if the associated interface is down.
Virtual IP	Add virtual IP addresses associated with the VRRP. Up to 16 virtual IP addresses can be added for every VRRP.

3. Expand and configure Optional Settings if needed.



Advertise Timer	Enter the advertise timer associated with the VRRP. It ranges from 1 to 255.
Preempt Mode	Select Enable or disable the preempt Mode from the pull-down list. If you select Enable, a backup router will preempt the master router if it has a priority greater than the master virtual router's priority. The Preempt Mode is enabled by default.
Delay Time	Enter the delay time associated with the VRRP. It ranges from 0 to 255.
Authentication	Select the type of Authentication for the Virtual Router from the pull-down list. The default is None. None: No authentication will be performed. Simple: Authentication will be performed using a text password. If you select this mode, enter the Key. MD5: Authentication of MD5 will be performed using a text password. If you select this mode, enter the Key.

4. Apply the settings.

4. 6 Configure VPN

VPN (Virtual Private Network) provides a means for secure communication between remote computers across a public wide area network (WAN), such as the internet. The gateways supports various types of VPN.

4. 6. 1 VPN

Overview

VPN (Virtual Private Network) gives remote LANs or users secure access to LAN resources over a public network such as the internet. Virtual indicates the VPN connection is based on the logical end-to-end connection instead of the physical end-to-end connection. Private indicates users can establish the VPN connection according to their requirements and only specific users are allowed to use the VPN connection.

The core of VPN connection is to realize tunnel communication, which fulfills the task of data encapsulation, data transmission and data decompression via the tunneling protocol. The gateway supports common tunneling protocols that a VPN uses to keep the data secure:

- **IPsec**

IPsec (IP Security) can provide security services such as data confidentiality, data integrity and data authentication at the IP layer. IPsec uses IKE (Internet Key Exchange) to handle negotiation of protocols and algorithms based on the user-specified policy, and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more paths between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

- **PPTP**

PPTP (Point-to-Point Tunneling Protocol) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP uses the username and password to validate users.

- **L2TP**

L2TP (Layer 2 Tunneling Protocol) provides a way for a dialup user to make a virtual Point-to-Point Protocol (PPP) connection to an L2TP network server (LNS), which can be a security gateway. L2TP sends PPP frames through a tunnel between an L2TP access concentrator (LAC) and the LNS. Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. L2TP uses the username and password to validate users.

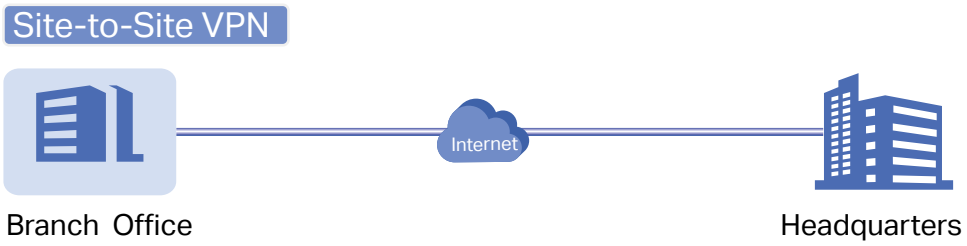
- **OpenVPN**

OpenVPN uses OpenSSL for encryption of UDP and TCP for traffic transmission. OpenVPN uses a client-server connection to provide secure communications between a server and a remote client over the internet. One of the most important steps in setting up OpenVPN is obtaining a certificate which is used for authentication. The SDN controller supports generating the certificate which can be downloaded as a file on your computer. With the certificate imported, the remote clients are checked out by the certificate and granted access to the LAN resources.

There are many variations of virtual private networks, with the majority based on two main models:

- **Site-to-Site VPN**

  A Site-to-Site VPN creates a connection between two networks at different geographic locations. Typically, headquarters set up Site-to-Site VPN with the subsidiary to provide the branch office with access to the headquarters' network.



  The gateway supports two types of Site-to-Site VPNs:

  - Auto IPsec

    The controller automatically creates an IPsec VPN tunnel between two sites on the same controller. The VPN connection is bidirectional. That is, creating an Auto IPsec VPN from site A to site B also provides connectivity from site B to site A, and nothing is needed to be configured on site B.

  - Manual IPsec

    You create an IPsec VPN tunnel between two peer routers over internet manually, from a local router to a remote router that supports IPsec. The gateway on this site is the local peer router.

- **Client-to-Site VPN**

  A Client-to-Site VPN creates a connection to the LAN from a remote host. It is useful for teleworkers and business travelers to access their central LAN from a remote location without compromising privacy and security.

  The first step to build a Client-to-Site VPN connection is to determine the role of the gateways and which VPN tunneling protocol to use:

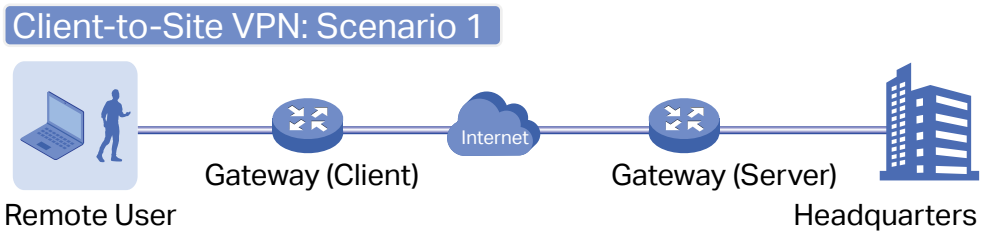
  - VPN Server

    The gateway on the central LAN works as a VPN server to provide a remote host with access to the local network. The gateway which functions as a VPN server can use L2TP, PPTP, IPsec, or OpenVPN as the tunneling protocol.

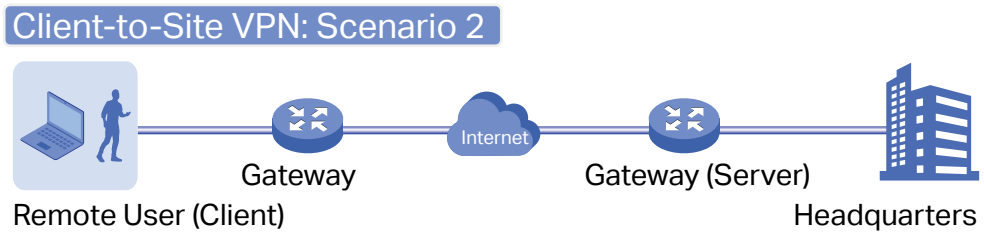
  - VPN Client

    Either the remote user's gateway or the remote user's laptop or PC works as the VPN client.

    When the remote user's gateway works as the VPN client, the gateway helps create VPN tunnels between its connected hosts and the VPN server. The gateway which functions as a VPN client can use L2TP, PPTP, or OpenVPN as the tunneling protocol.



When the remote user's laptop or PC works as the VPN client, the laptop or PC uses a VPN client software program to create VPN tunnels between itself and the VPN server. The VPN client software program can use L2TP, PPTP, IPsec, or OpenVPN as the tunneling protocol.

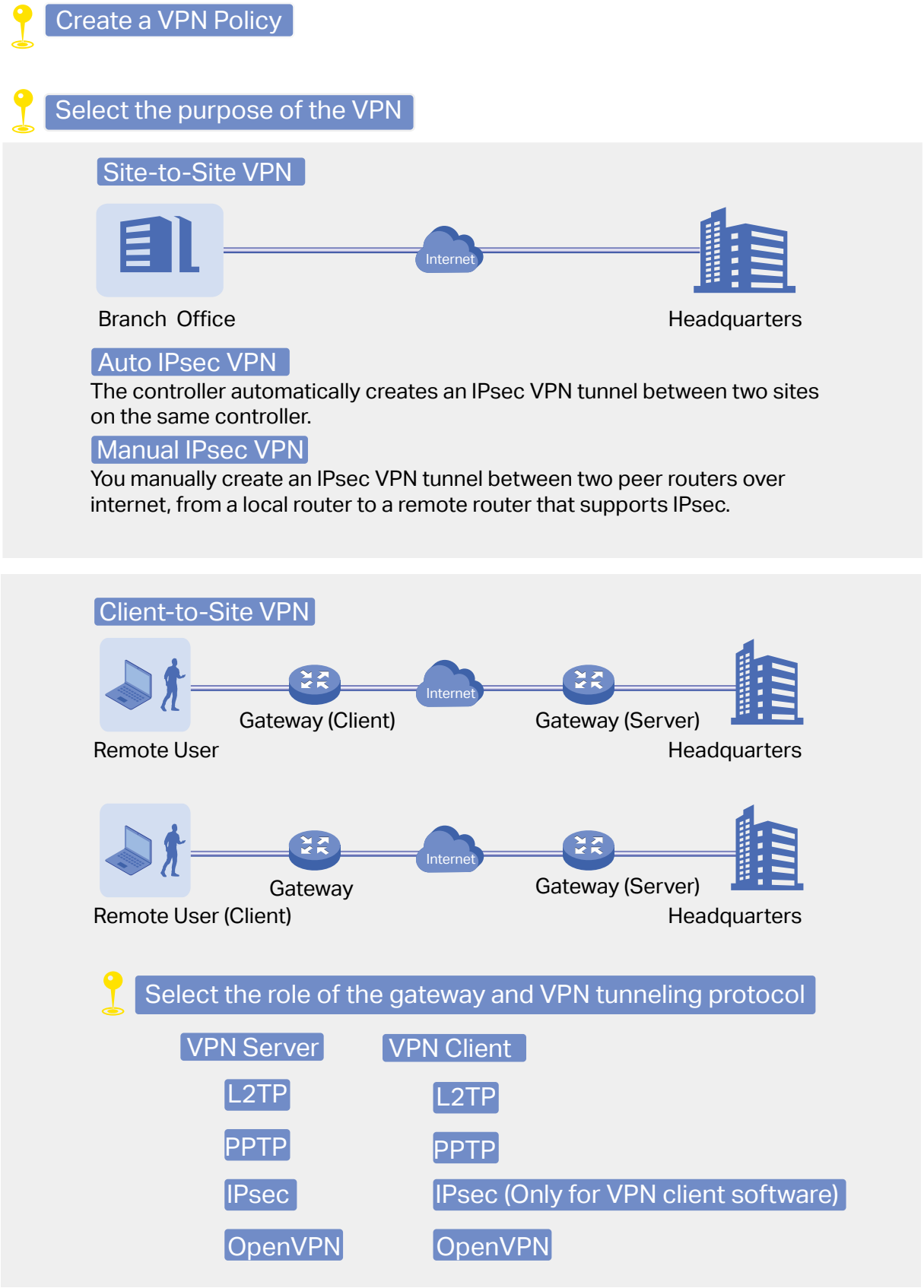


Note:

In scenario 1, you need to configure VPN client and VPN server separately on the gateways, while remote hosts can access the local networks without running VPN client software.

In scenario 2, you need to configure VPN server on the gateway, and then configure the VPN client software program on the remote user's laptop or PC, while the remote user's gateway doesn't need any VPN configuration.

Here is the infographic to provide a quick overview of VPN solutions.



Configuration

To complete the VPN configuration, follow these steps:

1) Create a new VPN policy and select the purpose of the VPN according to your needs. Select Site-to-Site if you want the network connected to another. Select Client-to-Site if you want some hosts connected to the network.

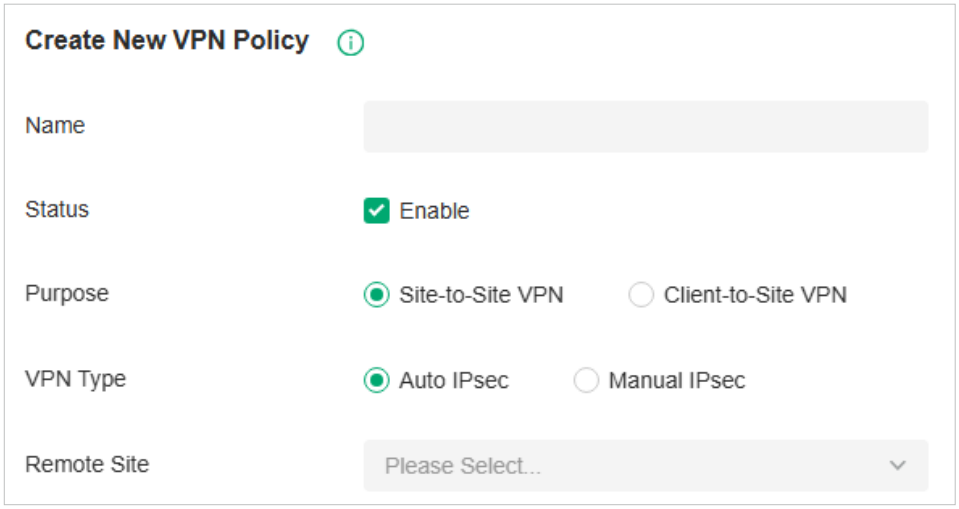
2) Select the VPN tunneling protocol and configure the VPN policy based on the protocol.

■ Configuring Site-to-Site VPN

The gateway supports two types of Site-to-Site VPNs: Auto IPsec and Manual IPsec.

- Configuring Auto IPsec VPN

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.

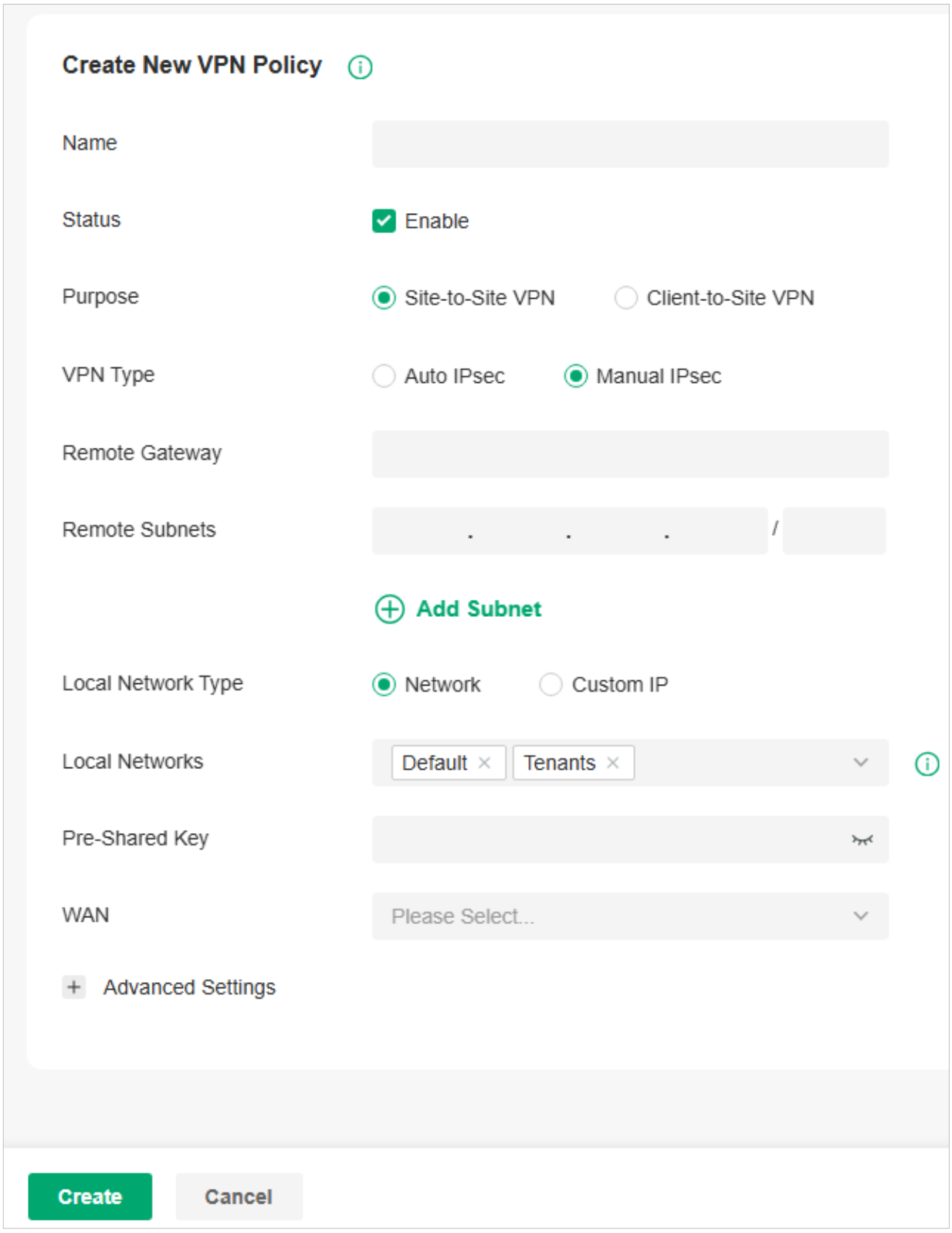


2. Enter a name to identify the VPN policy and select the purpose as Site-to-Site VPN. Refer to the following table to configure the required parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Site-to-Site VPN.
VPN Type	Select the VPN type as Auto IPsec. With Auto IPsec, the controller automatically creates an IPsec VPN tunnel between two sites on the same controller. The VPN connection is bidirectional. That is, creating an Auto IPsec VPN from site A to site B also provides connectivity from site B to site A, and nothing is needed to be configured on site B.
Remote Site	Select the site on the other end of the Auto IPsec VPN tunnel. Make sure that the selected remote site has an Omada managed gateway within the same controller.

- Configuring Manual IPsec VPN

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.

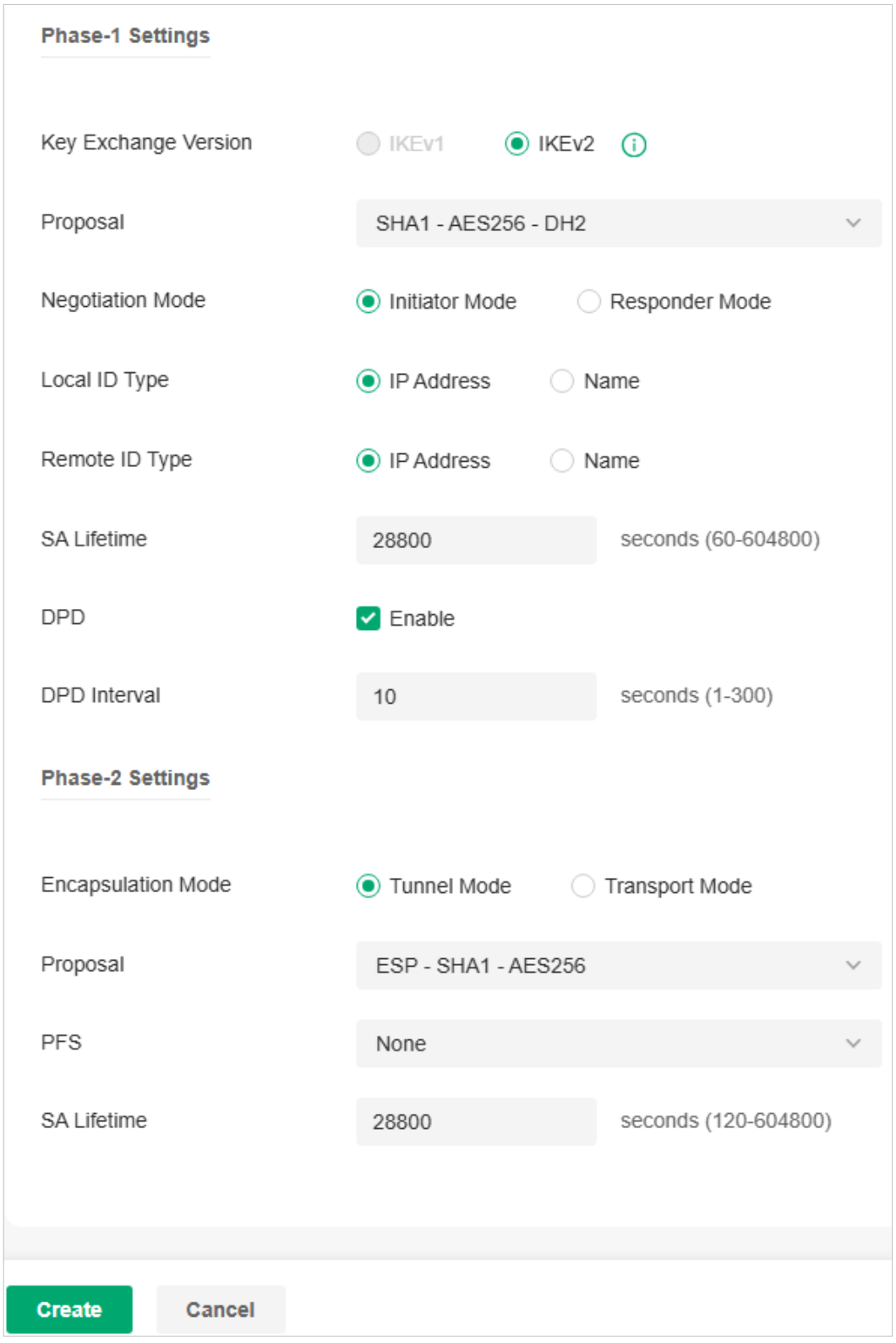


2. Enter a name to identify the VPN policy and select the purpose as Site-to-Site VPN. Refer to the following table to configure the basic parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.

Purpose	Select the purpose for the VPN as Site-to-Site VPN.
VPN Type	Select the VPN type as Manual IPsec.
Remote Gateway	Enter an IP address or a domain name as the gateway on the remote peer of the VPN tunnel.
Remote Subnets	Enter the IP address range of LAN on the remote peer of the VPN tunnel. Remote subnets should not be in the same network segment as the local LAN.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
Pre-Shared Key	Enter the pre-shared key(PSK). Both peer gateways must use the same pre-shared secret key for authentication. A pre-shared key is a string of characters that is used as an authentication key. Both peer gateways create a hash value based on the same pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party. The pre-shared keys should be long and random for security. Short or predictable pre-shared keys can be easily broken in brute-force attacks. To maintain a high level of security, administrators are recommended to update the pre-shared key periodically.
WAN	Select the WAN port on which the IPsec VPN tunnel is established.

3. Click **Advanced Settings** to load the following page.



Advanced settings include Phase-1 settings and Phase-2 settings. Phase-1 is used to set up a secure encrypted channel which the two peers can negotiate Phase-2, and then establish the IKE Security Associations (IKE SA). Phase-2 is used to negotiate about a set of parameters that define what traffic can go through the VPN, and how to encrypt and authenticate the traffic, then establish the IPsec Security Associations (IPsec SA).

Refer to the following table to complete the configurations according to your actual needs and click **Create**.

For Phase-1 Settings:

Phase-1 Settings	The IKE version you select determines the available Phase-1 settings and defines the negotiation process . Both VPN gateways must be configured to use the same IKE version and Phase-1 settings.
Internet Key Exchange Version	Select the version of Internet Key Exchange (IKE) protocol which is used to set up security associations for IPsec. Both IKEv1 and IKEv2 are supported with gateways, but IKEv1 is available only when the VPN policy is applied to a single Remote Subnet and a single Local Network. Note that both peer gateways must be configured to use the same IKE version.
Proposal	Specify the proposal for IKE negotiation phase-1. An IKE proposal lists the encryption algorithm, authentication algorithm and Diffie-Hellman (DH) groups to be negotiated with the remote IPsec peer. Authentication algorithms verify the data integrity and authenticity of a message. Encryption algorithms protect the data from being read by a third-party. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Note that both peer gateways must be configured to use the same Proposal.
Exchange Mode	Specify the IKE Exchange Mode when IKEv1 is selected. Main Mode: This mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. Aggressive Mode: This mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
Negotiation Mode	Specify the IKE Negotiation Mode as Initiator Mode or Responder Mode. Initiator Mode: This mode means that the local device initiates a connection to the peer. Responder Mode: This mode means that the local device waits for the connection request initiated by the peer.
Local ID Type	Specify the type of Local ID which indicates the authentication identifier sent to the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Local ID field to use the name as the ID for authentication. Note that the type and value of Local ID should be the same as Remote ID given for the remote peer of the VPN tunnel.

Local ID	When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
Remote ID Type	Specify the type of Remote ID which indicates the authentication identifier received from the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Remote ID field to use the name as the ID for authentication. Note that the type and value of Remote ID should be the same as Local ID given for the remote peer of the VPN tunnel.
Remote ID	When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.
DPD	Check the box to enable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.
DPD Interval	Specify the interval between sending DPD requests with DPD enabled. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.

For Phase-2 Settings:

Phase-2 Settings	The purpose of Phase 2 negotiations is to establish the Phase-2 SA (also called the IPsec SA). The IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic.
Encapsulation Mode	Specify the Encapsulation Mode as Tunnel Mode or Transport Mode. When both ends of the tunnel are hosts, either mode can be chosen. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, Tunnel Mode is recommended to ensure safety.
Proposal	Specify the proposal for IKE negotiation phase-2. An IPsec proposal lists the encryption algorithm, authentication algorithm and protocol to be negotiated with the remote IPsec peer. Note that both peer gateways must be configured to use the same Proposal.
PFS	Select the DH group to enable PFS (Perfect Forward Security) for IKE mode, then the key generated in phase-2 will be irrelevant with the key in phase-1, which enhance the network security. With None selected, it means PFS is disabled and the key in phase-2 will be generated based on the key in phase-1.
SA Lifetime	Specify IPsec SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related IPsec SA will be deleted.

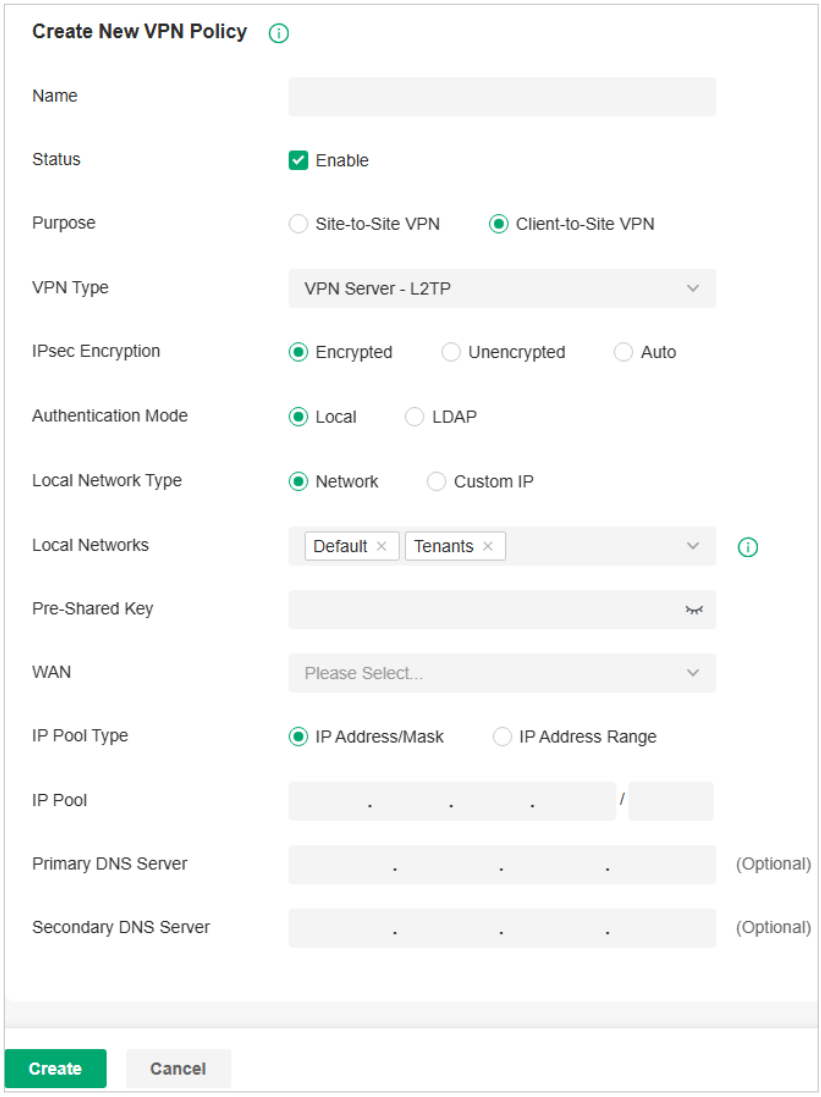
Configuring Client-to-Site VPN

The gateway supports seven types of client-to-Site VPNs depending on the role of your gateway and the protocol that you used:

Configuring the gateway as a VPN server using L2TP
Configuring the gateway as a VPN server using PPTP
Configuring the gateway as a VPN server using IPsec
Configuring the gateway as a VPN server using OpenVPN
Configuring the gateway as a VPN client using L2TP
Configuring the gateway as a VPN client using PPTP
Configuring the gateway as a VPN client using OpenVPN

- Configuring the gateway as a VPN server using L2TP

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.



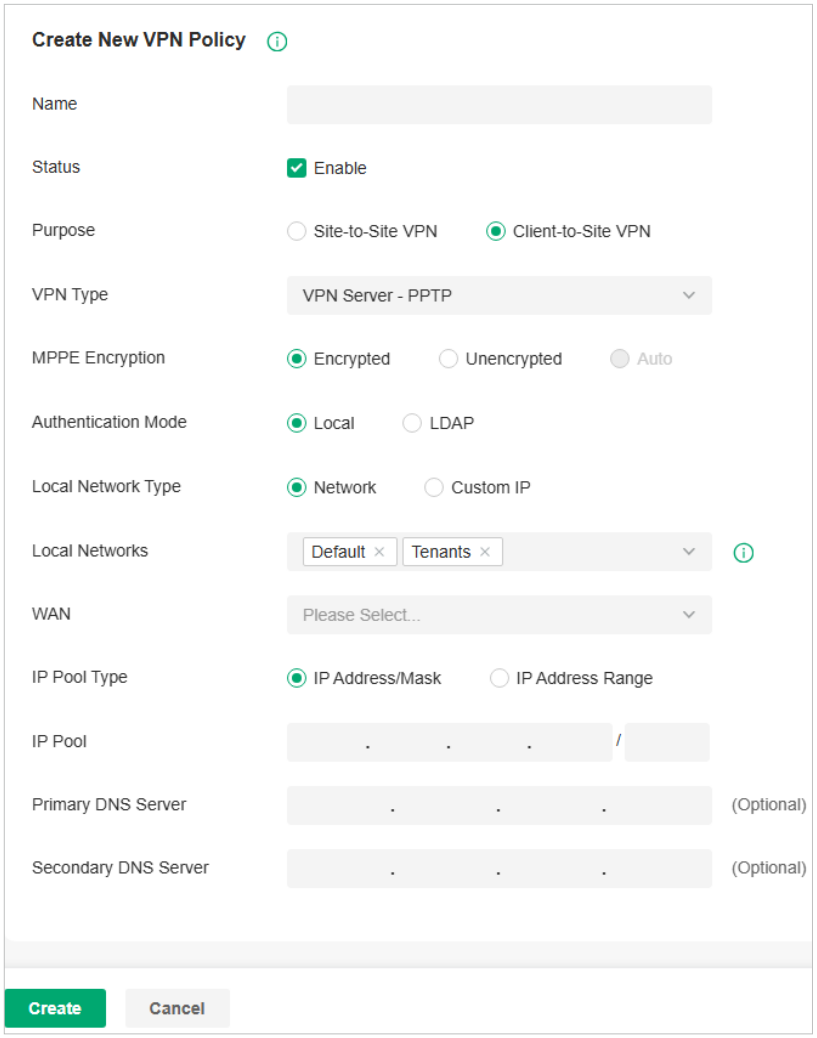
2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - L2TP.
IPsec Encryption	Specify whether to enable the encryption for the tunnel. Encrypted: Select Encrypted to encrypt the L2TP tunnel by IPsec (L2TP over IPsec). With Encrypted selected, enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication. Unencrypted: With Unencrypted selected, the L2TP tunnel will not be encrypted by IPsec. Auto: With Auto selected, the L2TP server will determine whether to encrypt the tunnel according to the client 's encryption settings. And enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication.
Authentication Mode	Select the authentication mode: Local or LDAP.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
Pre-shared Key	Enter the pre-shared secret key when IPsec Encryption is selected as Encrypted and Auto. Both peer routers must use the same pre-shared secret key for authentication.
WAN	Select the WAN port on which the L2TP VPN tunnel is established. Each WAN port supports only one L2TP VPN tunnel when the gateway works as a L2TP server.
IP Pool Type	Specify the format of the IP pool.
IP Pool	If you selected IP Address/Mask type, enter the IP address and subnet mask to decide the range of the VPN IP pool. If you select IP Address Range type, enter the start and end IP addresses of the VPN IP pool.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. Add the VPN users account to validate remote hosts. To create VPN users, refer to 4. 6. 2 VPN User.

- Configuring the gateway as a VPN server using PPTP

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.



2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click **Create**.

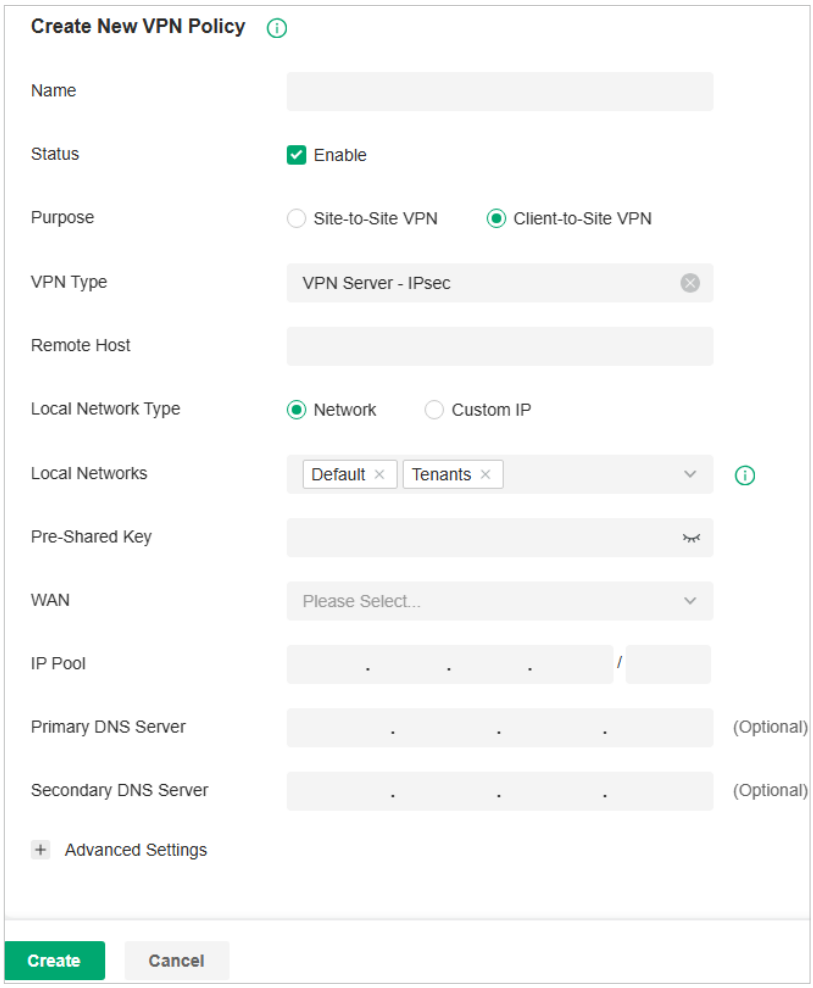
Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - PPTP.
MPPE Encryption	Specify whether to enable MPPE (Microsoft Point-to-Point Encryption) for the tunnel. Encrypted: With Encrypted selected, the PPTP tunnel will be encrypted by MPPE. Unencrypted: With Unencrypted selected, the PPTP tunnel will be not encrypted by MPPE.

Authentication Mode	Select the authentication mode: Local or LDAP.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
WAN	Select the WAN port on which the PPTP VPN tunnel is established. Each WAN port supports only one PPTP VPN tunnel when the gateway works as a PPTP server.
IP Pool Type	Specify the format of the IP pool.
IP Pool	If you selected IP Address/Mask type, enter the IP address and subnet mask to decide the range of the VPN IP pool. If you select IP Address Range type, enter the start and end IP addresses of the VPN IP pool.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. Add the VPN users account to validate remote hosts. To create VPN users, refer to 4. 6. 2 VPN User.

- Configuring the gateway as a VPN server using IPsec

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.

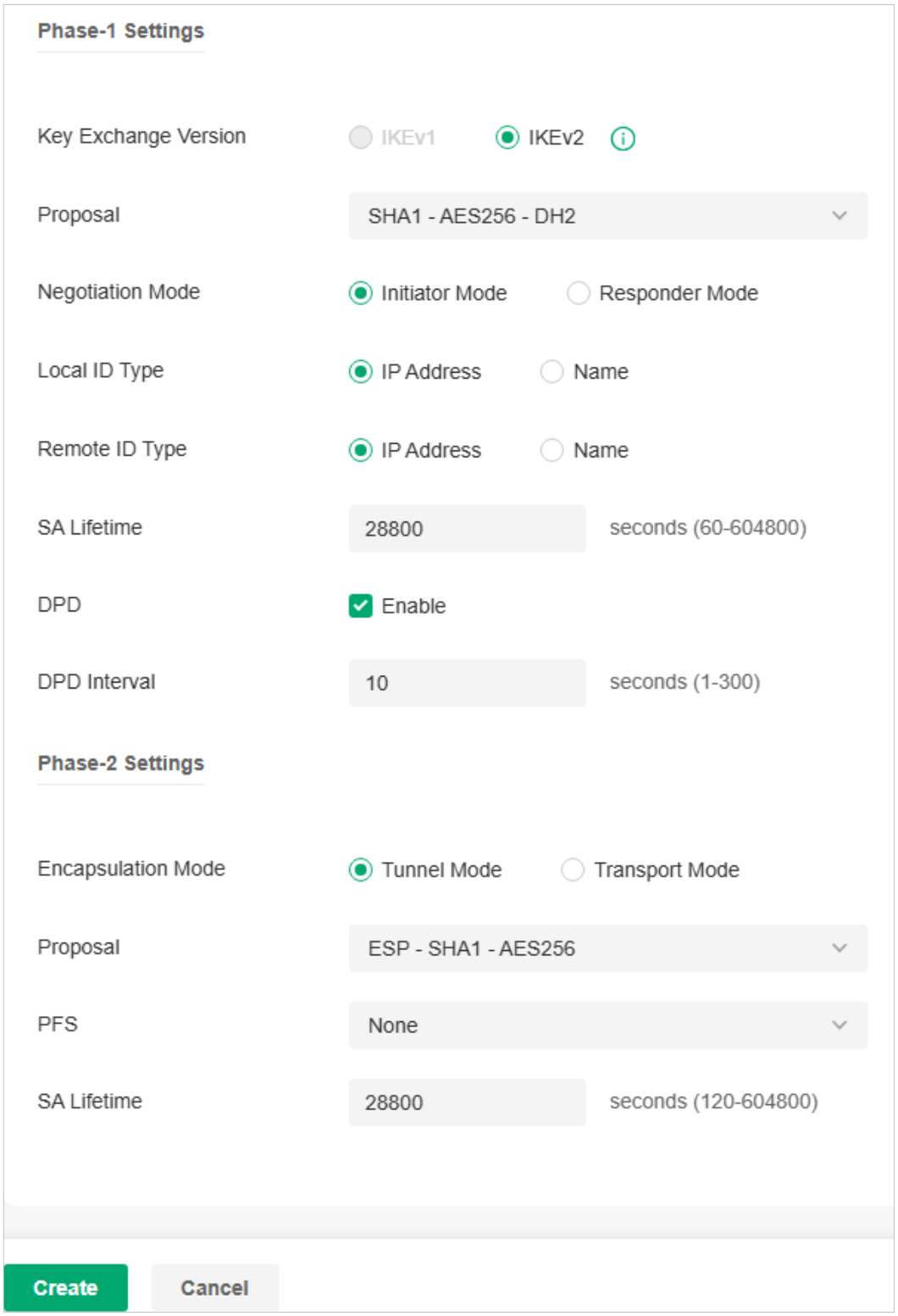


2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the basic parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - IPsec.
Remote Host	Enter an IP address or a domain name of the host on the remote peer of the VPN tunnel. 0.0.0.0 represents any IP address.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.

Pre-Shared Key	Enter the pre-shared key(PSK). Both peer gateways must use the same pre-shared secret key for authentication. A pre-shared key is a string of characters that is used as an authentication key. Both VPN peers create a hash value based on the same pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party. The pre-shared keys should be long and random for security. Short or predictable pre-shared keys can be easily broken in brute-force attacks. To maintain a high level of security, administrators are recommended to update the pre-shared key periodically.
WAN	Select the WAN port on which the IPsec VPN tunnel is established.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. Click Advanced Settings to load the following page.



Advanced settings include Phase-1 settings and Phase-2 settings. Phase-1 is used to set up a secure encrypted channel which the two peers can negotiate Phase-2, and then establish the IKE Security Associations (IKE SA). Phase-2 is used to negotiate about a set of parameters that define what traffic can go through the VPN, and how to encrypt and authenticate the traffic, then establish the IPsec Security Associations (IPsec SA).

Refer to the following table to complete the configurations according to your actual needs and click **Create**.

For Phase-1 Settings:

Phase-1 Settings	The IKE version you select determines the available Phase-1 settings and defines the negotiation process . Both VPN gateways must be configured to use the same IKE version and Phase-1 settings.
Internet Key Exchange Version	Select the version of Internet Key Exchange (IKE) protocol which is used to set up security associations for IPsec. Both IKEv1 and IKEv2 are supported with gateways, but IKEv1 is available only when the VPN policy is applied to a single Remote Subnet and a single Local Network. Note that both VPN peers must be configured to use the same IKE version.
Proposal	Specify the proposal for IKE negotiation phase-1. An IKE proposal lists the encryption algorithm, authentication algorithm and Diffie-Hellman (DH) groups to be negotiated with the remote IPsec peer. Authentication algorithms verify the data integrity and authenticity of a message. Encryption algorithms protect the data from being read by a third-party. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Note that both VPN peers must be configured to use the same Proposal.
Exchange Mode	Specify the IKE Exchange Mode when IKEv1 is selected. Main Mode: This mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. Aggressive Mode: This mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
Negotiation Mode	Specify the IKE Negotiation Mode as Initiator Mode or Responder Mode. Initiator Mode: This mode means that the local device initiates a connection to the peer. Responder Mode: This mode means that the local device waits for the connection request initiated by the peer.
Local ID Type	Specify the type of Local ID which indicates the authentication identifier sent to the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Local ID field to use the name as the ID for authentication. Note that the type and value of Local ID should be the same as Remote ID given for the remote peer of the VPN tunnel.
Local ID	When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).

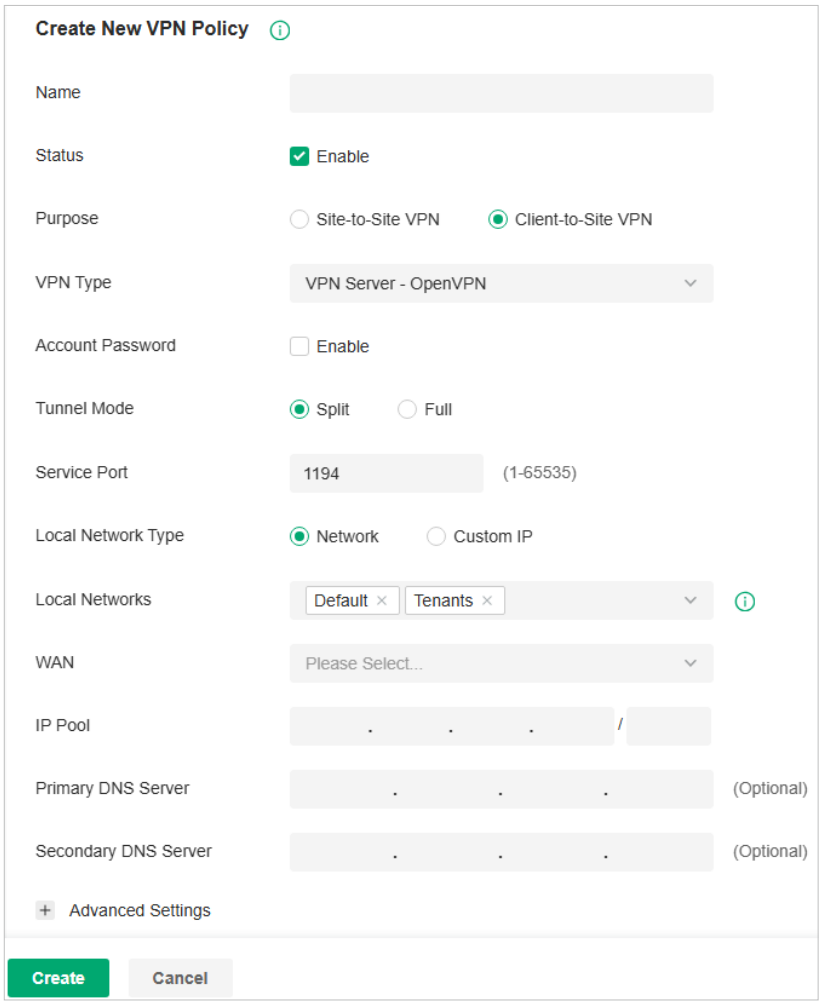
Remote ID Type	Specify the type of Remote ID which indicates the authentication identifier received from the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Remote ID field to use the name as the ID for authentication. Note that the type and value of Remote ID should be the same as Local ID given for the remote peer of the VPN tunnel.
Remote ID	When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.
DPD	Check the box to enable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.
DPD Interval	Specify the interval between sending DPD requests with DPD enabled. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.

For Phase-2 Settings:

Phase-2 Settings	The purpose of Phase 2 negotiations is to establish the Phase-2 SA (also called the IPsec SA). The IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic.
Encapsulation Mode	Specify the Encapsulation Mode as Tunnel Mode or Transport Mode. When both ends of the tunnel are hosts, either mode can be chosen. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, Tunnel Mode is recommended to ensure safety.
Proposal	Specify the proposal for IKE negotiation phase-2. An IPsec proposal lists the encryption algorithm, authentication algorithm and protocol to be negotiated with the remote IPsec peer. Note that both peer gateways must be configured to use the same Proposal.
PFS	Select the DH group to enable PFS (Perfect Forward Security) for IKE mode, then the key generated in phase-2 will be irrelevant with the key in phase-1, which enhance the network security. With None selected, it means PFS is disabled and the key in phase-2 will be generated based on the key in phase-1.
SA Lifetime	Specify IPsec SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related IPsec SA will be deleted.

- Configuring the gateway as a VPN server using OpenVPN

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.

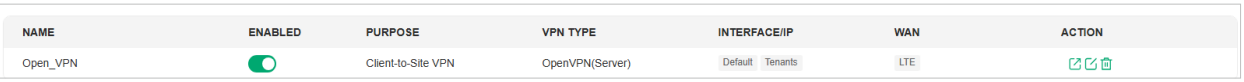


2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - OpenVPN.
Account Password	Specify whether VPN clients need to enter a user account to access the VPN tunnel. When enabled, you need to create accounts on the VPN User page.
Tunnel Mode	Select the tunnel mode: Split or Full. Full tunneling uses the VPN for all your traffic, whereas split tunneling sends part of your traffic through a VPN and part of it through the open network. Full tunneling is more secure than split tunneling.
Protocol	Select the communication protocol for the gateway which works as an OpenVPN Server. Two communication protocols are available: TCP and UDP.
Service Port	Enter a VPN service port to which a VPN device connects.

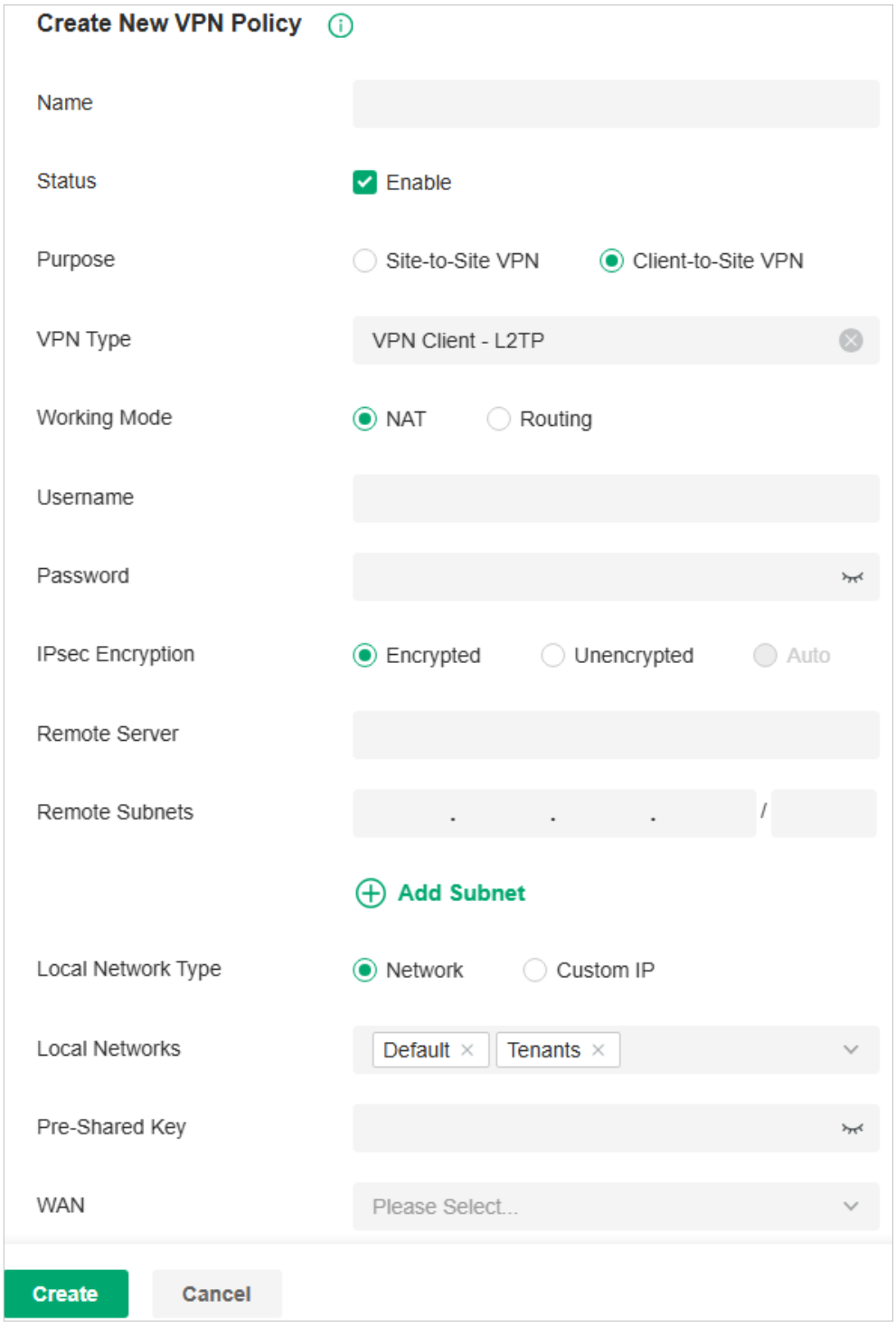
Authentication Mode	Select the authentication mode: Local or LDAP. LDAP is used for SSO (single sign-on), which enables users to use the same password in multiple services.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
WAN	Select the WAN port on which the VPN tunnel is established. Each WAN port supports only one OpenVPN tunnel when the gateway works as a OpenVPN server.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. After clicking **Create** to save the VPN policy, go to VPN Policy List and click the export icon in the Action column to export the OpenVPN file that ends in .ovpn which is to be used by the remote client. The exported OpenVPN file contains the certificate and configuration information.



- Configuring the gateway as a VPN client using L2TP

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.



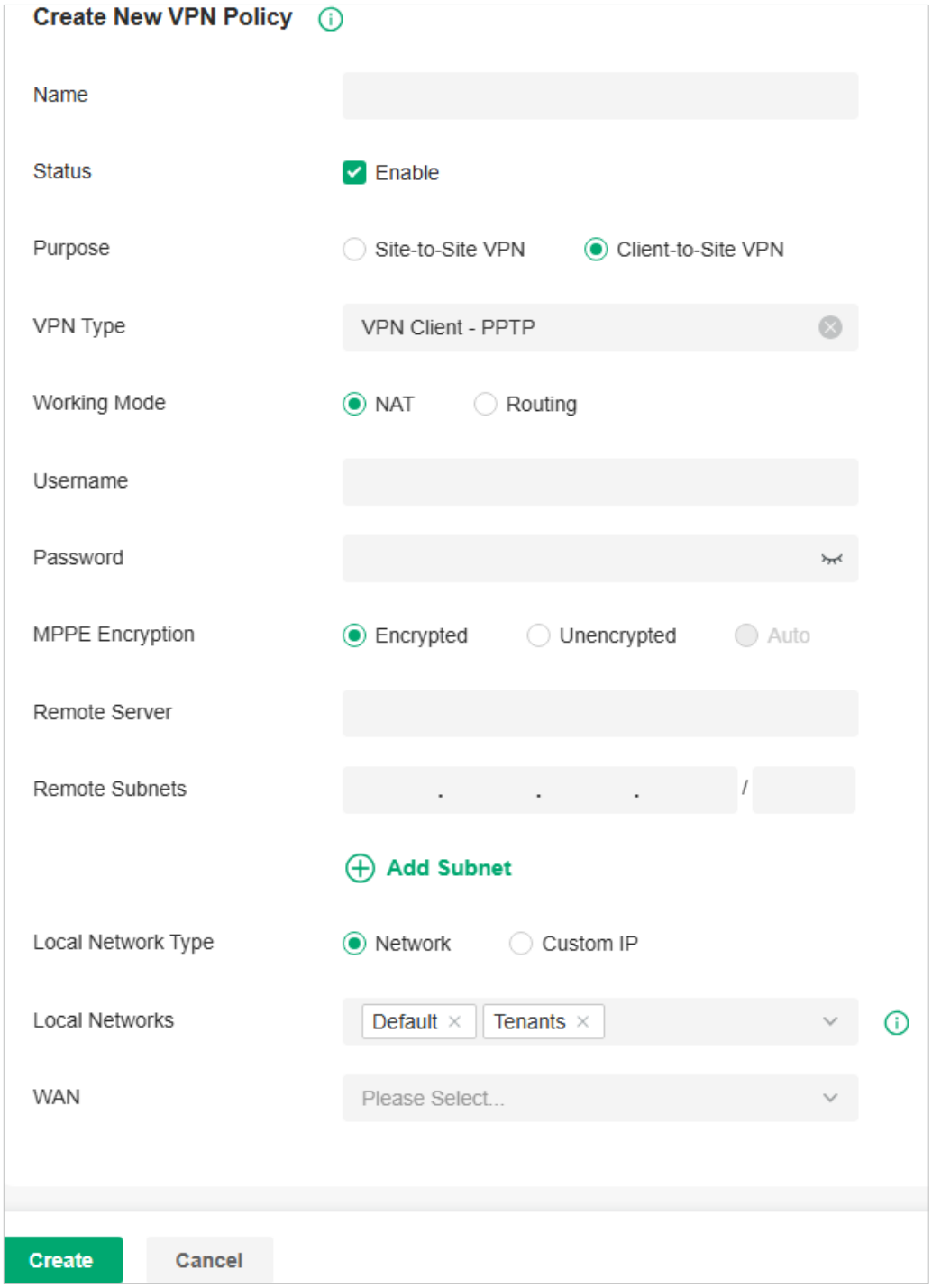
2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Client - L2TP.

Working Mode	Specify the Working Mode as NAT or Routing. NAT: With NAT (Network Address Translation) mode selected, the L2TP client uses the assigned IP address as its source addresses of original IP header when forwarding L2TP packets. Routing: With Routing selected, the L2TP client uses its own IP address as its source addresses of original IP header when forwarding L2TP packets.
Username	Enter the username used for the VPN tunnel. This username should be the same as that of the L2TP server.
Password	Enter the password of user. This password should be the same as that of the L2TP server.
IPsec Encryption	Specify whether to enable the encryption for the tunnel. Encrypted: Select Encrypted to encrypt the L2TP tunnel by IPsec (L2TP over IPsec). With Encrypted selected, enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication. Unencrypted: With Unencrypted selected, the L2TP tunnel will be not encrypted by IPsec.
Remote Server	Enter the IP address or domain name of the L2TP server.
Remote Subnets	Enter the IP address and subnet mask to specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
Pre-shared Key	Enter the pre-shared secret key when the L2TP tunnel is encrypted by IPsec. Both peer gateways must use the same pre-shared secret key for authentication.
WAN	Select the WAN port on which the VPN tunnel is established.

- Configuring the gateway as a VPN client using PPTP

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.



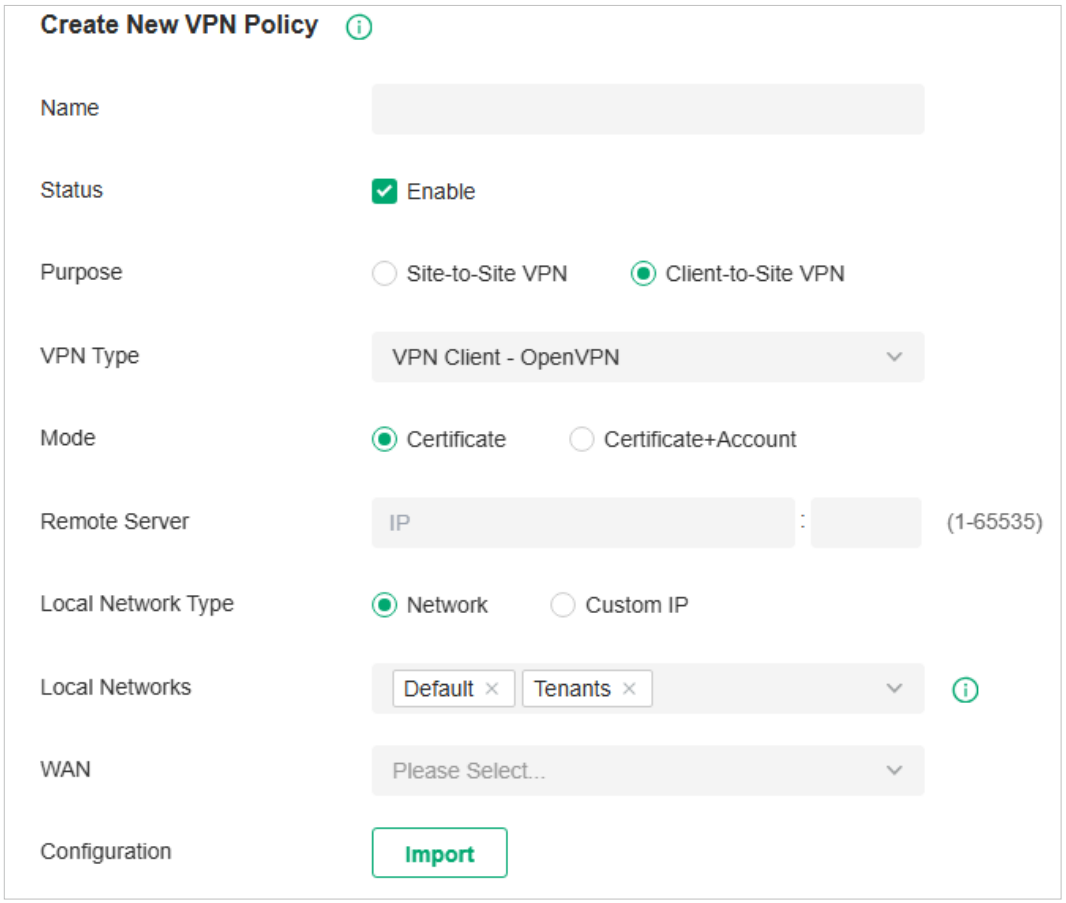
2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Client - PPTP.

Working Mode	Specify the Working Mode as NAT or Routing. NAT: With NAT (Network Address Translation) mode selected, the PPTP client uses the assigned IP address as its source addresses of original IP header when forwarding PPTP packets. Routing: With Routing selected, the PPTP client uses its own IP address as its source addresses of original IP header when forwarding PPTP packets.
Username	Enter the username used for the VPN tunnel. This username should be the same as that of the PPTP server.
Password	Enter the password of user. This password should be the same as that of the PPTP server.
MPPE Encryption	Specify whether to enable the encryption for the tunnel. Encrypted: Select Encrypted to encrypt the PPTP tunnel by MPPE. Unencrypted: With Unencrypted selected, the PPTP tunnel will be not encrypted by MPPE.
Remote Server	Enter the IP address or domain name of the PPTP server.
Remote Subnets	Enter the IP address and subnet mask to specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
WAN	Select the WAN port on which the VPN tunnel is established.

- Configuring the gateway as a VPN client using OpenVPN

1. Launch the controller and access a site. Go to **Settings** > **VPN**. Click **Create New VPN Policy** to load the following page.



2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click **Create**.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Client - OpenVPN.
Mode	Select the access mode according to VPN requirements. Certificate: Select this option if the VPN tunnel only requires the certificate. Certificate+Account: Select this option if the VPN tunnel requires the certificate and VPN user account. If selected, configure the following parameters: Username: Enter the username for the VPN tunnel. Password: Enter the password for the VPN tunnel.
Remote Server	Enter the IP address or domain name of the OpenVPN server.

Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
WAN	Select the WAN port on which the VPN tunnel is established.
Configuration	Click the import icon to import the OpenVPN file that ends in .ovpn generated by the OpenVPN server. Only one file can be imported. If the certificate file and configuration file are generated singly by the OpenVPN server, combine two files and import the whole file.

4. 6. 2 VPN User

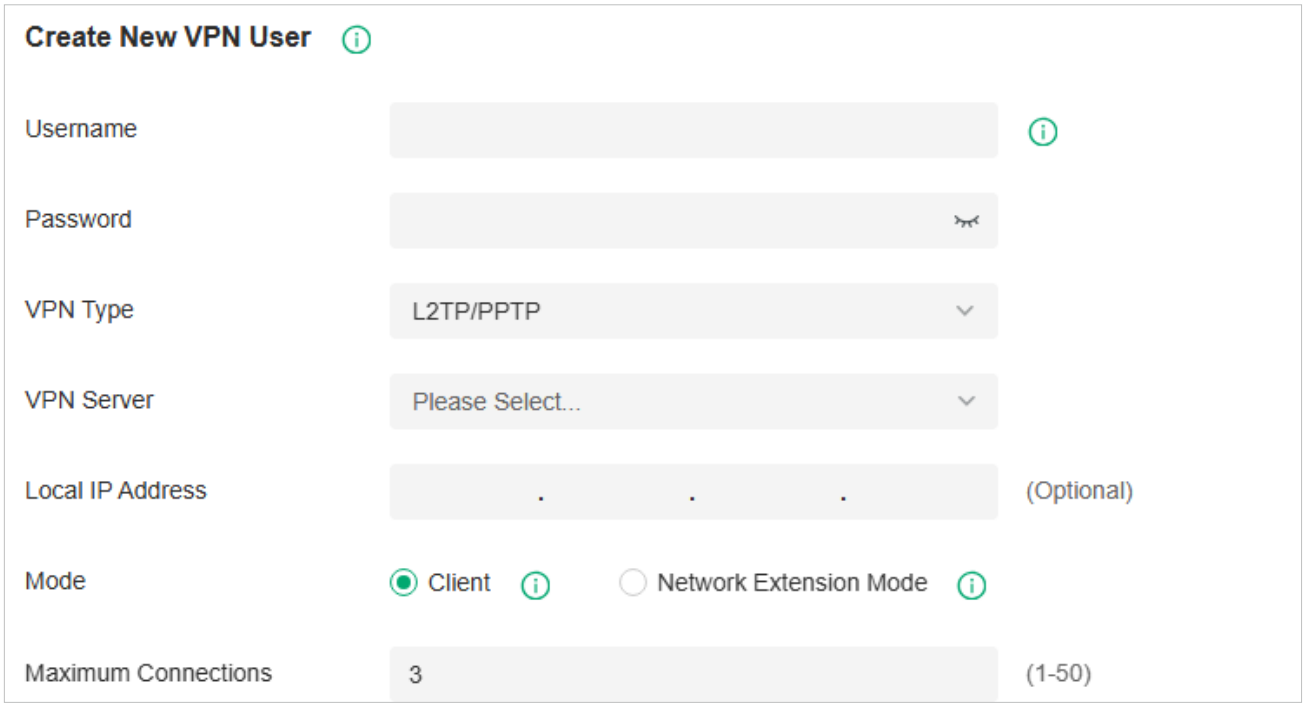
Overview

VPN User is used to configure and record your custom settings for VPN configurations, and it allows you to configure VPN users that can be used for multiple VPN servers. It saves you from setting the VPN users with the same configurations repeatedly when you want to apply the user in different VPN servers.

Configuration

To configure the VPN users, follow these steps:

1. Launch the controller and access a site. Go to **Settings** > **VPN** >**VPN User**. Click **Create New VPN User** to add a new entry of VPN User.



2. Specify the parameters and click **Create**.

Username	Enter the username used for the VPN tunnel. The client use the username for the validation before accessing the network.
Password	Enter the password of user. The client uses the password for the validation before accessing the network.
Protocol	Select the protocol type for the VPN tunnel.

If you selected the L2TP/PPTP protocol, specify the following parameters:

VPN Server	Select the VPN server that the VPN user is applied to.
Local IP Address	(Optional) Specify the local IP address of the VPN tunnel.
Mode	Specify the connection mode for the VPN users. Client: This mode allows the client to request for an IP address and the server supplies the IP addresses from the VPN IP Pool. With this mode selected, set maximum number of concurrent VPN connections with the same account in Maximum Connections. Network Extension Mode: This mode allows only clients from the configured subnet to connect to the server and obtain VPN services. With this mode selected, specify the subnets in Remote Subnets.

If you selected the OpenVPN protocol, specify the following parameter:

VPN Server	Select the VPN server that the VPN user is applied to.

To edit or delete the VPN users, click the icon in the Action column. You can further filter the entries based on the VPN Server.

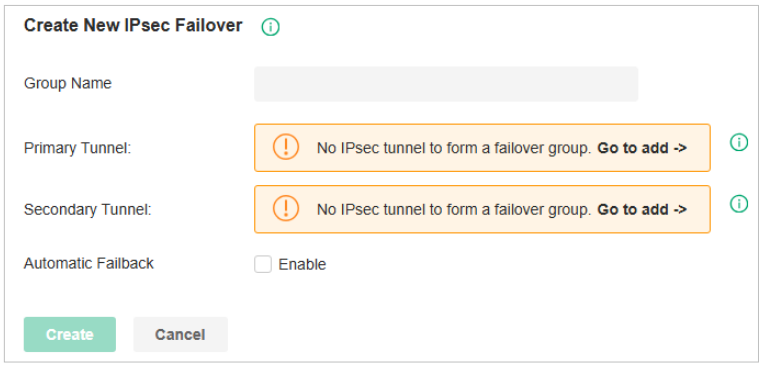
4. 6. 3 IPsec Failover

Overview

IPsec Failover is used to configure the backup group of the IPsec connection. When the primary connection in the group is interrupted, it will try to use the secondary connection to dial up to maintain the stability of the VPN network.

Configuration

1. Launch the controller and access a site. Go to Settings > VPN >IPsec Failover. Click Create New IPsec Failover to add a new entry.



Group Name	Enter a name to identify the IPsec Failover group.
Primary Tunnel	Specify the IPsec primary connection.
Secondary Tunnel	Specify the IPsec secondary connection.
Automatic Failback	Select this function to automatically switch back to the primary connection when it is reachable. When selected, specify the Gateway Failover Timeout time, then the system will query whether the primary connection is reachable within the time, and if yes, it will switch back to the primary connection.

4. 6. 4 SSL VPN

Overview

SSL VPN uses Secure Socket Layer (SSL) to ensure information safety and provides abundant services such as user management, resource management, user lockout, authentication and accounting.

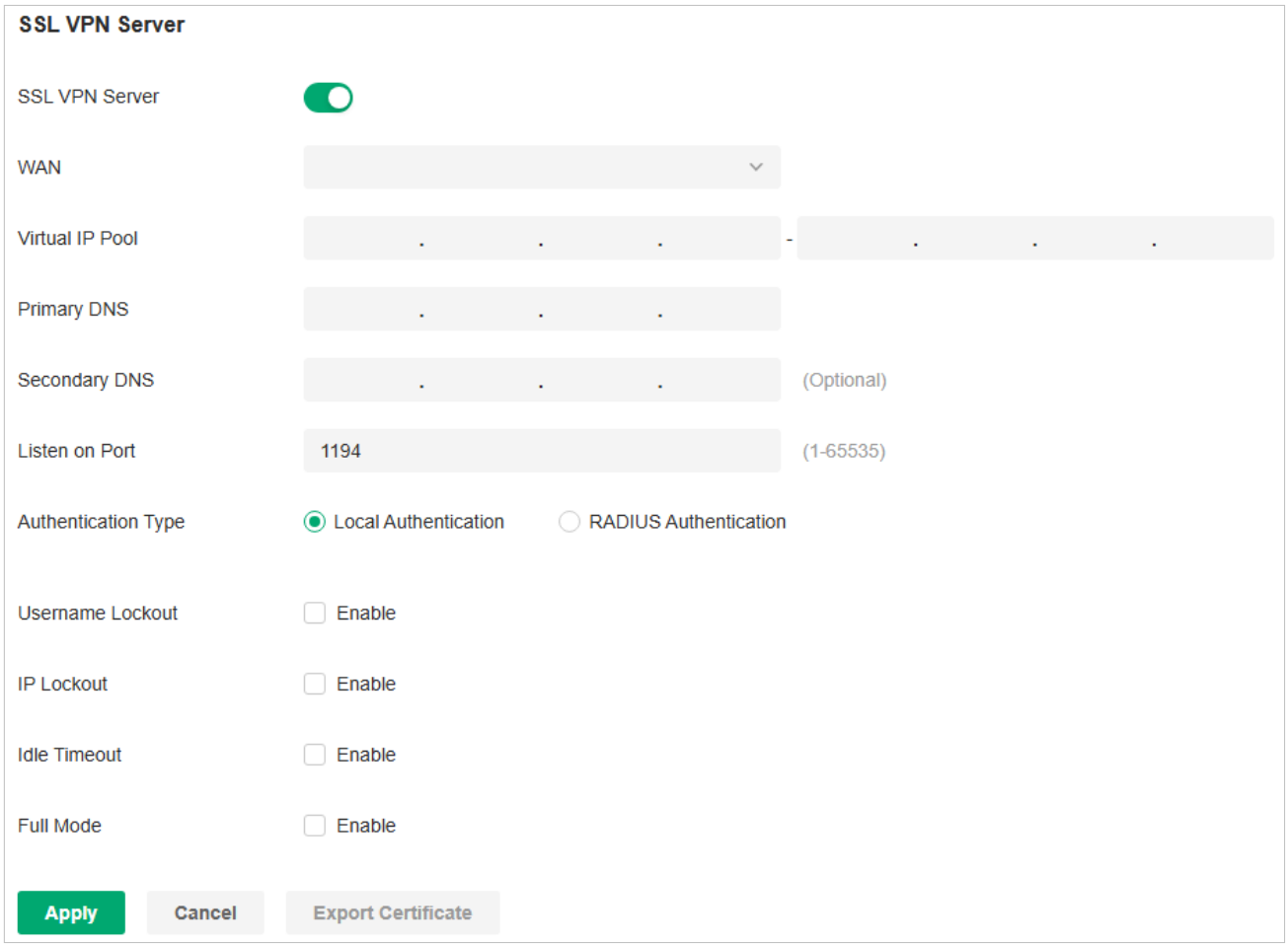
SSL VPN uses username and password for authentication and login. A network administrator can assign different resources to different types of users, and meanwhile associate the users with multiple resources, making it easy to manage and limit the services the users can access through the VPN.

Configuration

- **SSL VPN Server**

  In SSL VPN Server, you can enable the feature and configure the SSL VPN settings.

1. Launch the controller and access a site. Go to Settings > VPN > SSL VPN > SSL VPN Server. Enable SSL VPN Server.

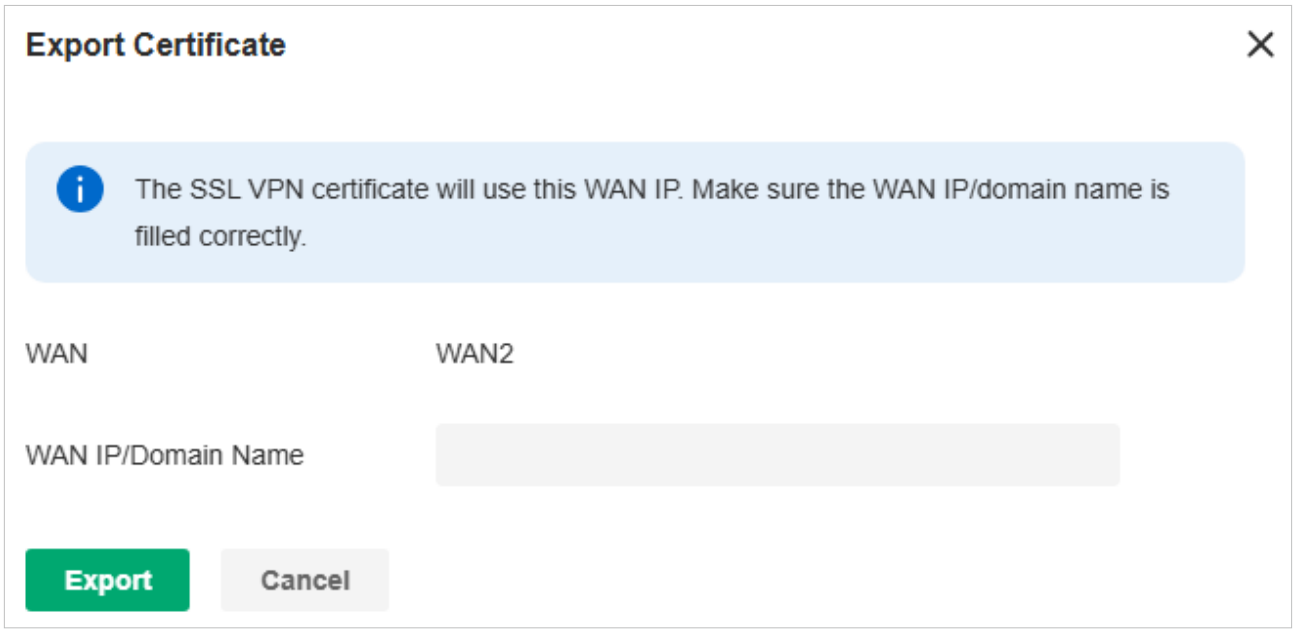


2. Configure the parameters according to your needs. Click Apply.

WAN	Select the port for the SSL VPN server to listen on, and the VPN tunnel will take effect on the port.
Virtual IP Pool	Set a virtual IP Pool, and the SSL VPN server will assign an IP address to a connected client within the pool.
Primary/Secondary DNS	Specify the IP address of the DNS server. The clients will be informed of the DNS server, and it can help the clients resolve the domain name.
Listen on Port	Specify the port for the SSL VPN server to listen on. By default, it is 1194.

Authentication Type	Select the authentication for the clients: Local Authentication or RADIUS Authentication. If you selected RADIUS Authentication, configure the following parameters: RADIUS Server: Select a RADIUS server profile. Authentication Type: Select the authentication protocol for the RADIUS server. Max Requests: Specify the maximum number of requests sent when no response is received. Request Timeout: Specify the maximum interval for request timeout. After timeout, the request will be sent again. NAS IP: Specify the IP address for the router to communicate with the RADIUS server.
Username Lockout	When enabled, you can lock out a username in case of excessive login attempts. Max Login Attempts: Specify the maximum failed login attempts for a username. If the number of attempts reaches this amount, the username will be locked out. Lockout Duration: Specify how long the username will be locked out.
IP Lockout	When enabled, you can lock out an IP address in case of excessive login attempts. Max Login Attempts: Specify the maximum failed login attempts for a login IP. If the number of attempts reaches this amount, the login IP will be locked out. Lockout Duration: Specify how long the login IP will be locked out.
Idle Timeout	When enabled, the VPN tunnel will close automatically if there is no traffic for the specified amount of time.
Full Mode	When enable, all traffic will go through the SSL VPN tunnel. When disabled, only the resource-related traffic will go through the tunnel.

3. Click Export Certificate, enter the WAN IP/Domain Name to access the VPN, then click Export. The VPN configuration file will be exported for clients to access the VPN.

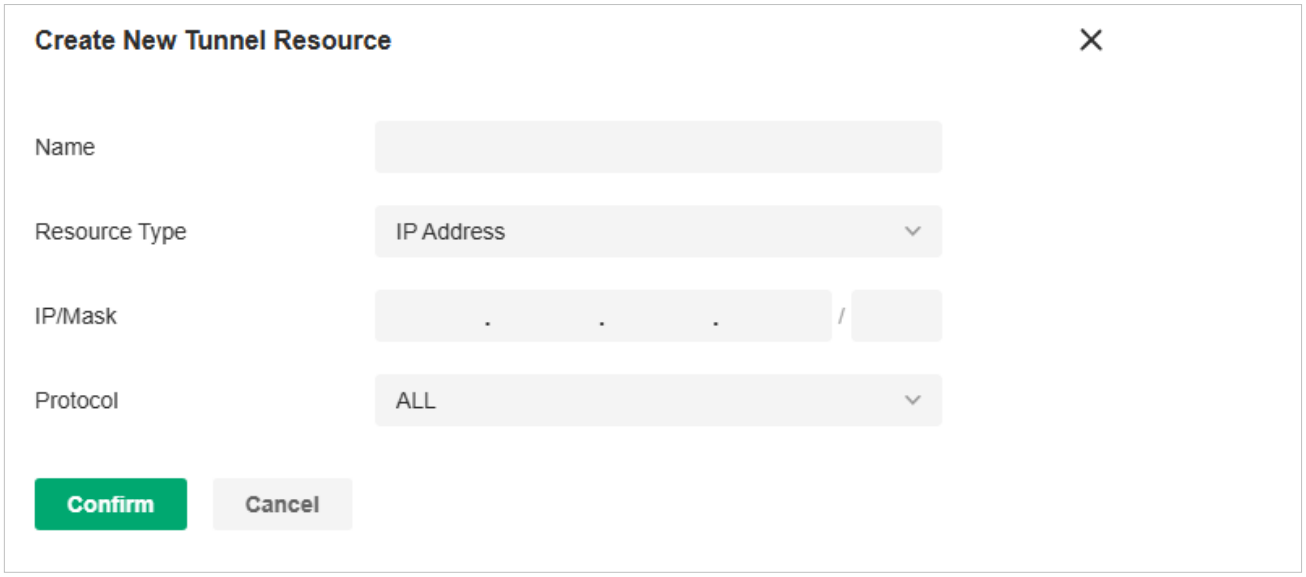


- **Resource Management**

  In Tunnel Resources, you can configure the resources the clients can access through the VPN tunnel, including IP range and domain name.

  In Resource Group, you can add the multiple tunnel resources to a group for better management. By default, two resource groups are provided: Group_ALL (indicates all resources) and Group_LAN (indicates all LAN resources).

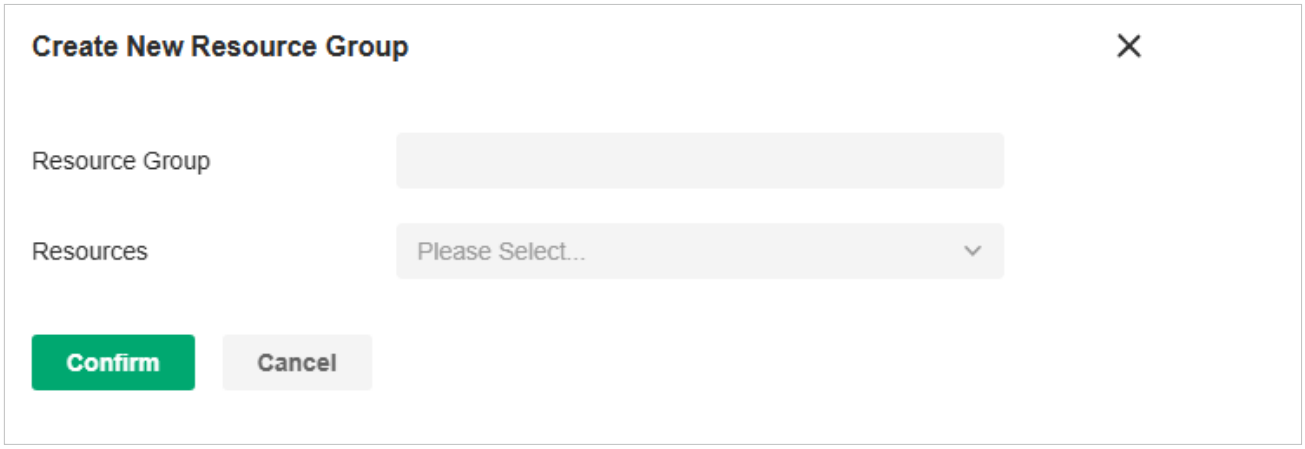
1. Launch the controller and access a site. Go to Settings > VPN > SSL VPN > Resource Management.
2. Click Create New Tunnel Resource to load the following page. Configure the parameters and click Confirm.



Name	Specify a name for the entry.

Resource Type	Select the type for the resources: IP Address or Domain Name. If you selected IP Address, configure the following parameters: IP/Mask: Specify IP range the clients can access. Protocol: Select the protocol type that the client can access in the IP range, and the router will filter illegal packets through firewall rules. By default, the value is ALL, and it means there is no restriction on the client. If you selected Domain Name, specify domain name the clients can access.

3. Click Create New Resource Group to load the following page. Configure the parameters and click Confirm.

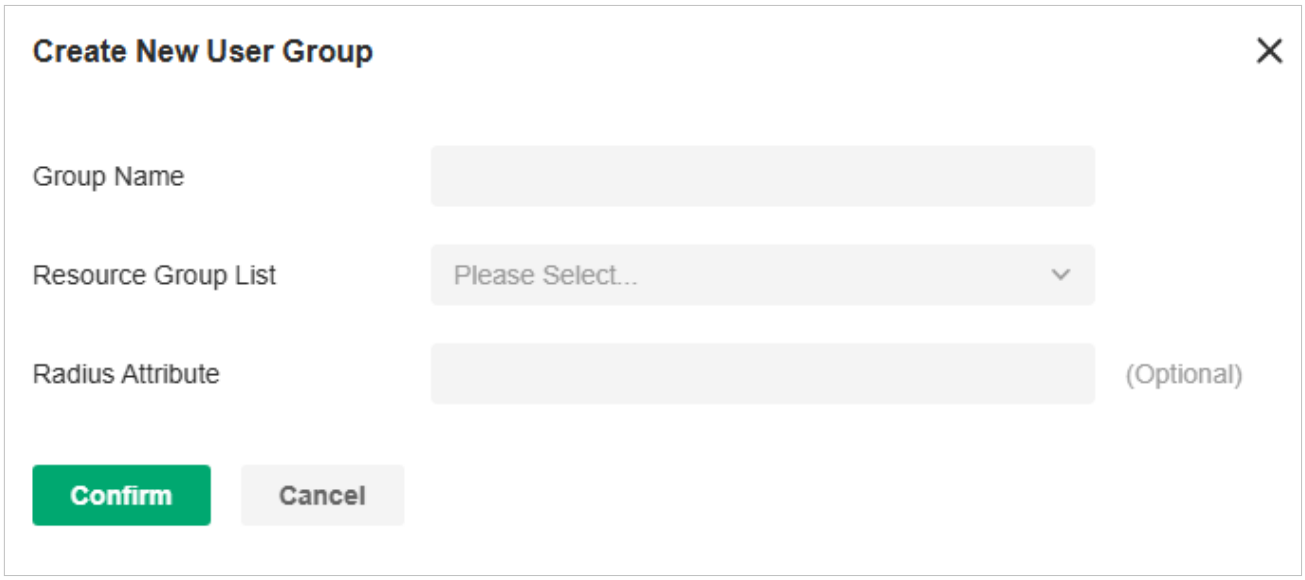


Resource Group	Specify a name for the resource group.
Resources	Select the resources for the group.

- **User Group**

  In User Group, you can add multiple users to a group for better management.

1. Launch the controller and access a site. Go to Settings > VPN > SSL VPN > User Group.
2. Click Create New User Group to load the following page. Configure the parameters and click Confirm.

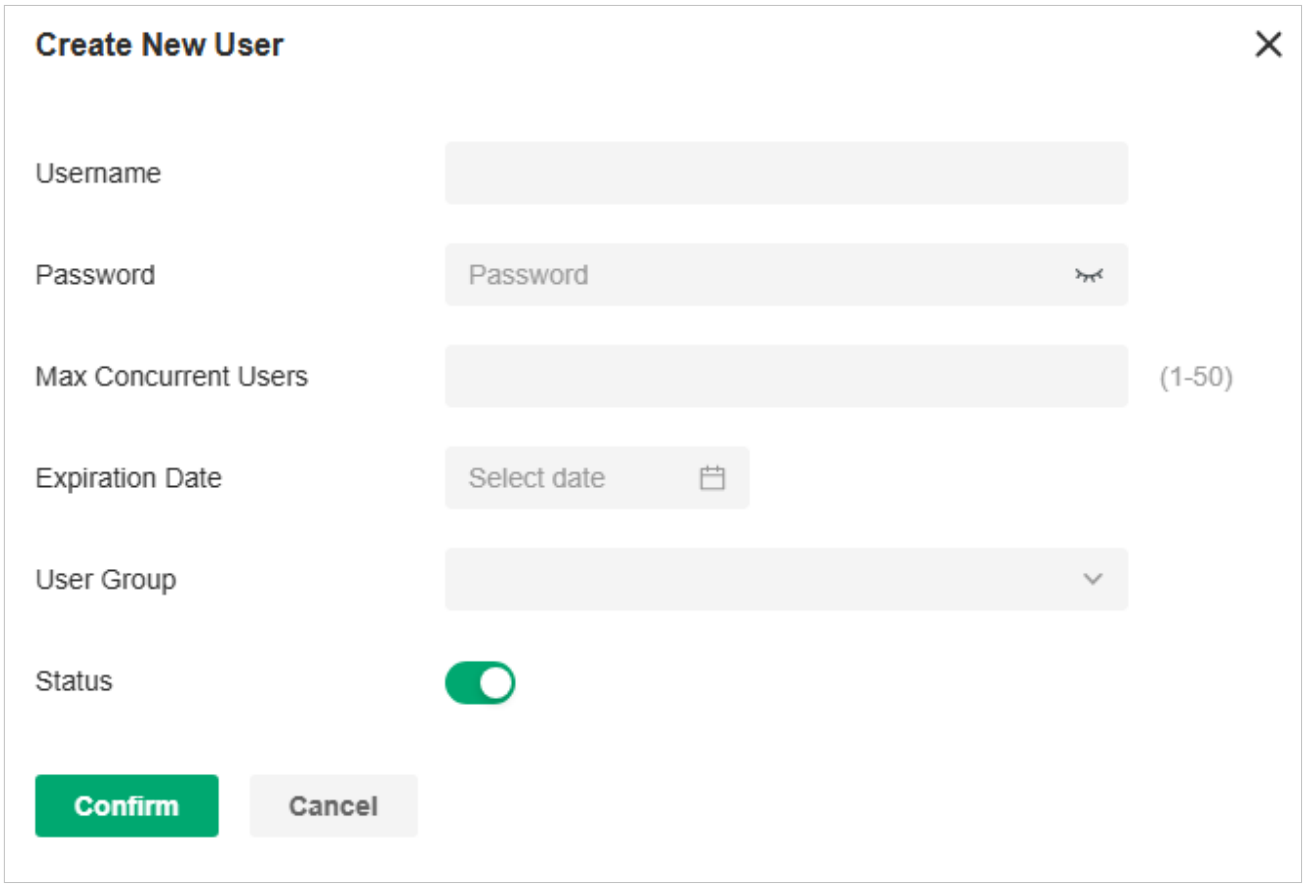


Group Name	Specify a name for the user group.
Resource Group List	Select the resource group for the user group.

- **User List**

  In User List, you can view and configure all user settings of the SSL VPN.

1. Launch the controller and access a site. Go to Settings > VPN > SSL VPN > User List.
2. Click Create New User to load the following page. Configure the parameters and click Confirm.

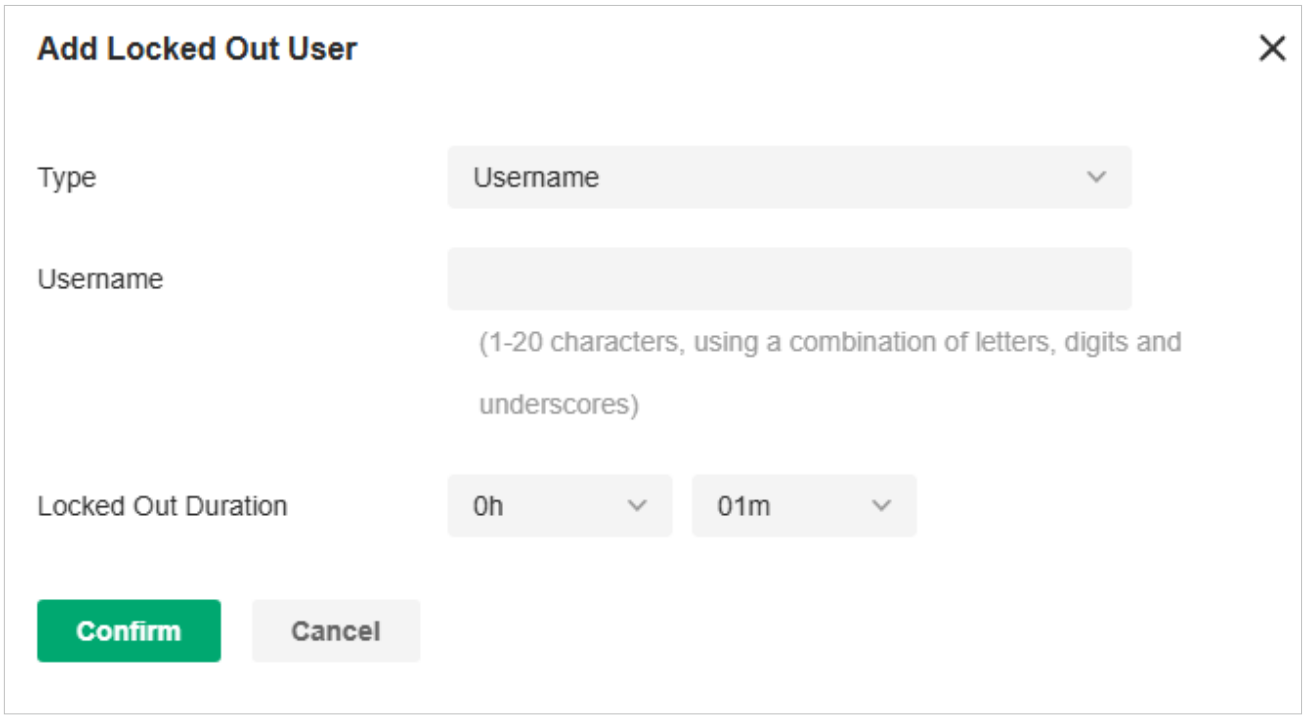


Username	Specify the username a client used for login.
Password	Specify the password a client used for login.
Max Concurrent Users	Specify the maximum number of clients using the username for login concurrently. If the number reaches this amount, new login attempts will be rejected.
Expiration Date	Specify when the user account will expire.
User Group	Select which group the user belongs to. A user can only be added to one user group.
Status	Click the checkbox to enable this entry.

- **Locked Out User**

  In Locked Out User, you can view the currently locked out users, and add, delete or edit an entry.

1. Launch the controller and access a site. Go to Settings > VPN > SSL VPN > Locked Out User.
2. Click Add Locked Out User to load the following page. Configure the parameters and click Confirm.



Type	Specify the locked out type. If you selected Username, specify the username of a locked out user. If you selected IP Address, specify the IP address of a locked out user.
Lockout Duration	Specify how long the entry will be locked out.

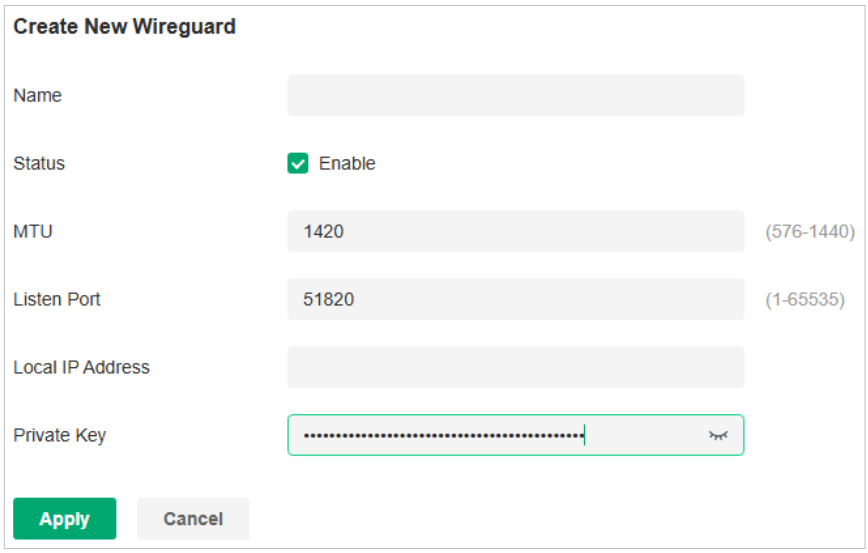
4. 6. 5 WireGuard VPN

Overview

WireGuard VPN is a secure, fast and modern VPN protocol. It is based on the UDP protocol and uses modern encryption algorithms to improve work efficiency.

- **WireGuard**

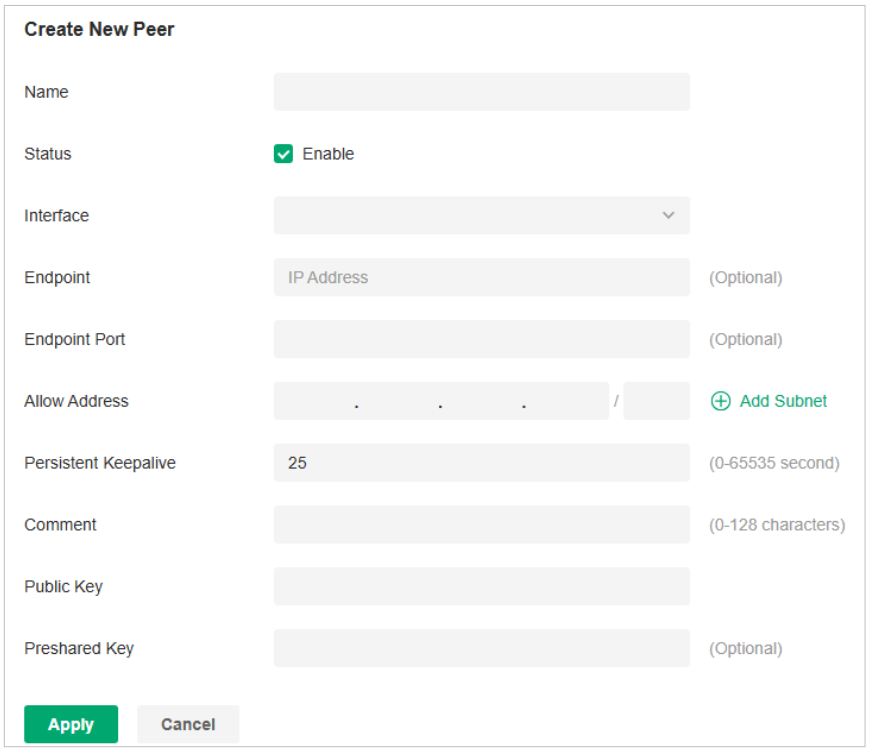
1. Launch the controller and access a site. Go to Settings > VPN > WireGuard.
2. Click Create New WireGuard. Configure the parameters and click Apply.



Name	Specify the name that identifies the WireGuard interface.
Status	Specify whether to enable the WireGuard interface.
MTU	Specify the MTU value of the WireGuard interface. The default value 1420 is recommended.
Listen Port	Specify the port number that the WireGuard interface listens to.
Local IP Address	Specify the IP address of the WireGuard interface.
Private Key	Specify the private key of the WireGuard interface. The value will be automatically generated on the device, and you can also modify it manually.

Peers

1. Launch the controller and access a site. Go to Settings > VPN > WireGuard > Peers.
2. Click Create New Peer. Configure the parameters and click Apply.



Name	Specify the name that identifies the peer.
Status	Specify whether to enable the peer.
Interface	Specify the WireGuard interface to which the peer belongs.
Endpoint	Specify the IP address of the peer. This parameters is required when the Router actively connects to other WireGurad Server.
Endpoint Port	Specify the port number of the peer. This parameters is required when the Router actively connects to other WireGurad Server.
Allowed Address	Specify the address segment that allows traffic to pass through. Generally, it is the same as the WireGuard VPN interface IP configured on the remote device.
Persistent Keepalive	Specify the tunnel keepalive packet interval.
Comment	Enter the description of the peer.
Public Key	Fill in the public key information exported from the remote device.
Preshared Key	Specify an optional shared key.

4. 7 Create Profiles

Profiles section is used to configure and record your custom settings for site configurations. It includes Time Range and Groups profiles. In Time Range section, you can configure time templates for wireless schedule, PoE schedule, etc. In Groups section, you can configure groups based on IP, IP-Port and MAC addresses for ACL, Routing, NAT, etc. After creating the profiles, you can apply them to multiply configurations for different sites, saving you from repeatedly setting up the same information.

4. 7. 1 Time Range

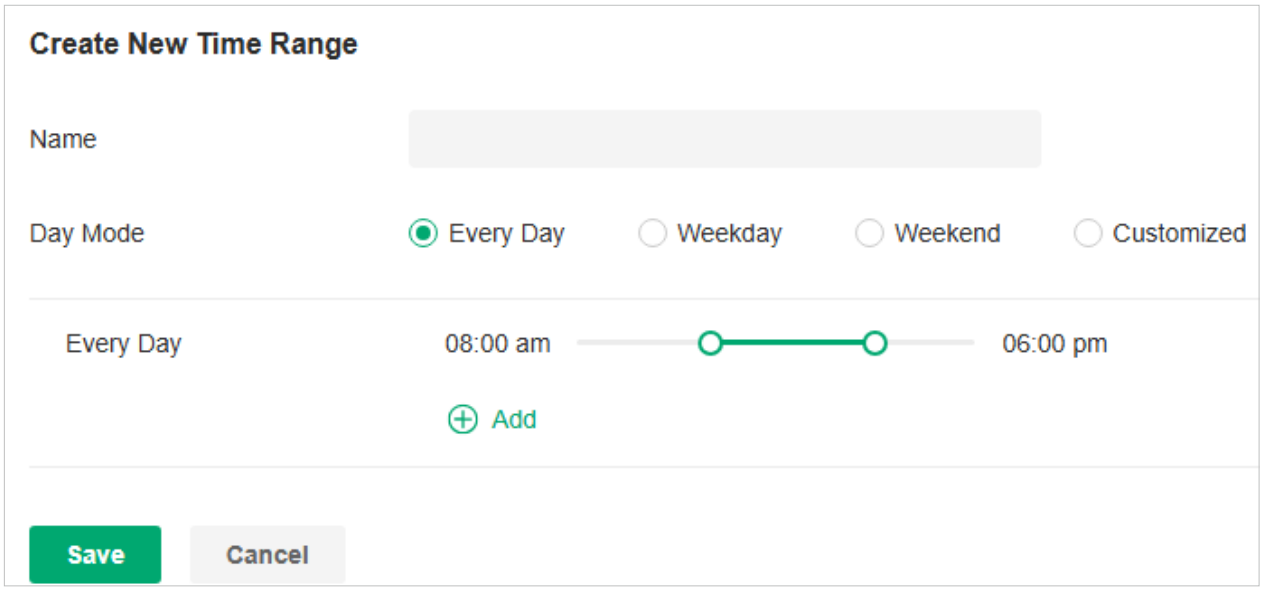
Overview

Time Range section allows you to customize time-related configurations. You can set different time range templates which can be shared and applied to wireless schedule, PoE schedule, etc. in site configuration.

Configuration

To configure the time range profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Basic Profile >Time Range. Click Create New Time Range to add a new time range entry. By default, there is no entry in the list.

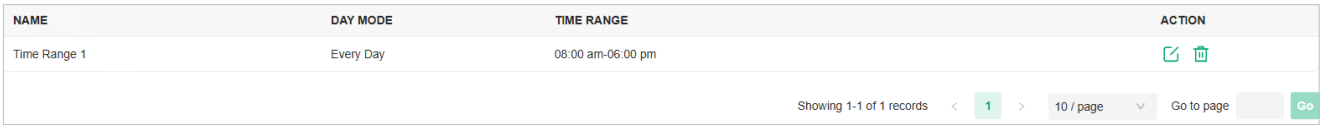


2. Enter a Name for the new entry, select the Day Mode, and specify the time range. Click +Add to add a new time period, click Save to save the entry. After saving the newly added entry, you can apply them to site configuration.

Name	Enter a name for the new entry, and it is a string with 1 to 64 ASCII symbols.

Day Mode	Select Every Day, Weekday, Weekend, or Customized first before specifying the time range for each day. Every Day: You only need to set the time range once, and it will repeat every day. Weekday: You only need to set the time range once, and it will repeat every weekday from Monday to Friday. Weekend: You only need to set the time range once, and it will repeat every Saturday and Sunday. Customized: You are able to set different time range for the chosen day(s) based on your needs. When a day is not chosen, the WiFi is open all day by default.

You can view the name, day mode and time range in the list.



To edit or delete the time range entry, click the icon in the Action column.

4. 7. 2 Groups

Overview

Groups section allows you to customize client groups based on IP, IP-Port, or MAC Address. You can set different rules for the groups profiles which can be shared and applied to ACL, Routing, NAT, etc. in site configuration.

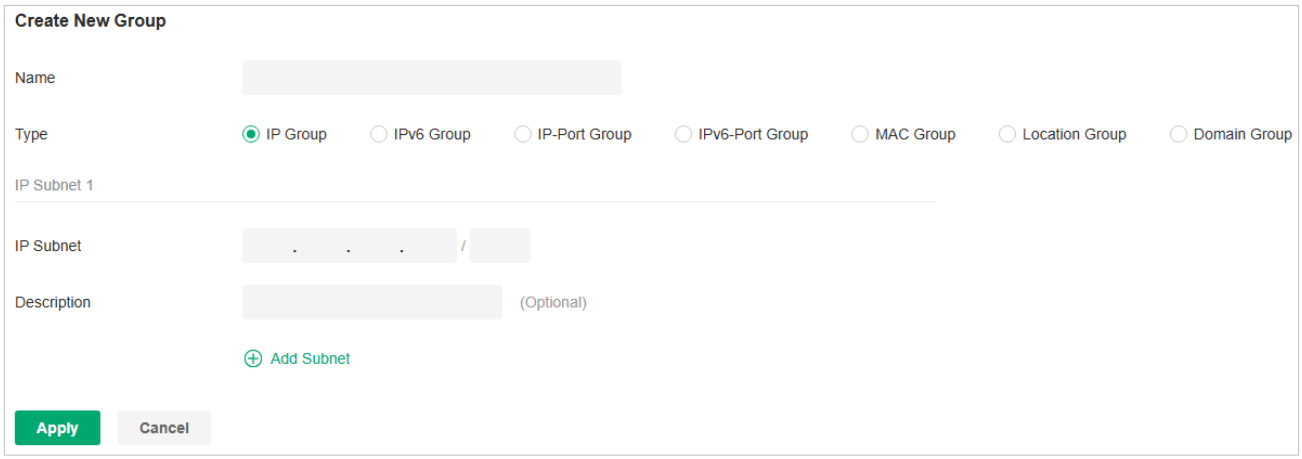
Configuration

To configure the group profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Basic Profile > Groups. Click Create New Group to add a new group profile.



2. Enter a name for the new group profile entry, and select the type for the new entry.



- **To create an IP group profile:**

  Choose the IP Group type and specify IP subnets.

- **To create an IPv6 group profile:**

  Choose the IPv6 Group type and specify IPv6 addresses.

- **To Create an IP-Port group profile:**

  Choose the IP-Port Group type and specify the IP-Port type and ports, while it is optional to specify IP subnets. If you only specify ports without entering any IP subnets, it means the group contains the specified ports for all IP addresses.

- **To create an IPv6-Port group profile:**

  Choose the IPv6-Port Group type and specify the IP-Port type and ports, while it is optional to specify IPv6 addresses. If you only specify ports without entering any IPv6 addresses, it means the group contains the specified ports for all IPv6 addresses.

- **To configure a MAC group profile:**

  Choose the MAC Group type and add MAC addresses in the MAC Addresses List.

- **To configure a location group profile:**

  Choose the Location Group type and select locations. You can enter a description for identification.

- **To configure a domain group profile:**

  Choose the Domian Group type and specify the domain names. You can specify up to 16 domain names for the group. The domain name can be complete, such as www.baidu.com and www.twitter.com; it can also contain wildcards, such as *.google.com, which will match domain names such as www.google.com, pam.google.com and google.com in special cases..

3. Click Apply to save the entry.

   You can view and edit the group list, and export the MAC group if needed. You can apply the customized profiles during site configuration.



4. 7. 3 Rate Limit

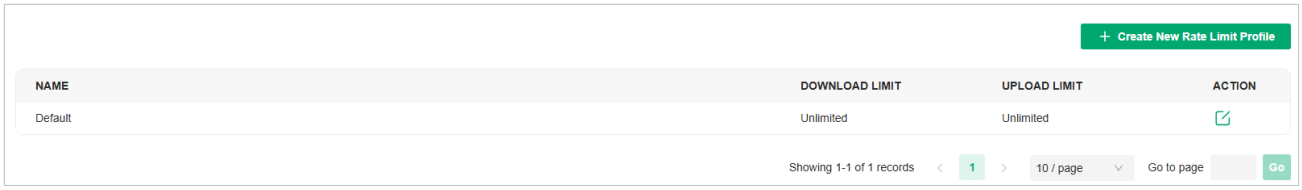
Overview

Rate Limit allows you to customize rate-related configurations. You can set different rate limit templates. They can be bound with wireless network to limit the upload/download rate of clients connected the SSID, and applied to specific types of Portal, such as Local User and Voucher. After creating the profiles, you can apply them to multiple configurations, saving you from repeatedly setting up the same information.

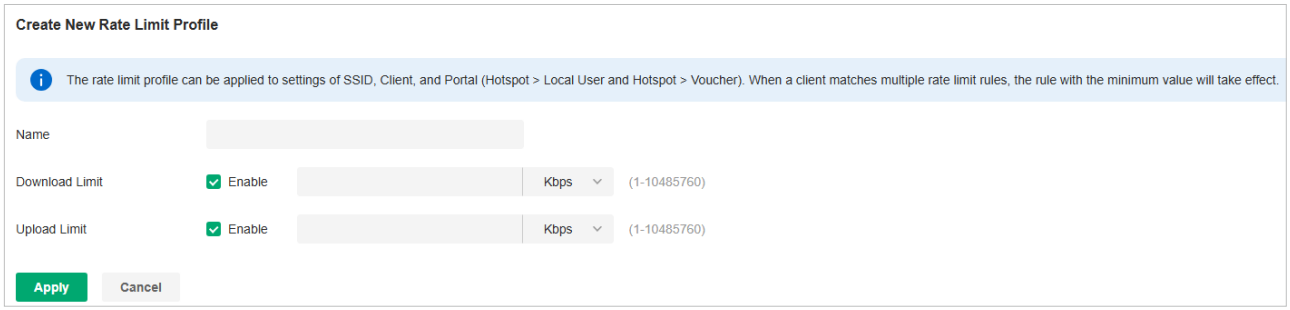
Configuration

To configure the rate limit profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Basic Profile > Rate Limit. By default, there is an entry with no limits, and it can not be deleted. Click Create New Rate Limit Profile to add a new group entry.



2. Enter a name and specify the download/upload rate limit for the new entry. After saving the newly added entry, you can apply them to other configurations such as Portal and Wireless Settings.



Name	Enter a name to identify the created rate limit profile.
Download Limit	Enable the download limit, and specify the rate limit correspondingly in Kbps or Mbps.
Upload Limit	Enable the upload limit, and specify the rate limit correspondingly in Kbps or Mbps.

3. Click Apply to save the entry. After saving the newly added entry, you can apply them to site configuration. To apply the customized rate limit profiles in the related configurations, refer to 4. 8. 1 Portal, and 4. 3. 1 Set Up Basic Wireless Networks.

You can view the name, download limit, and upload limit in the list.

To view, edit or delete the rate limit profile, click the icon in the Action column.

4. 7. 4 PPSK

Overview

PPSK is a security solution for you to manage individual client devices without much complexity. With PPSK, each user is assigned with a unique passphrase for authentication. Also, it allows the binding of a passphrase and the device MAC address(es), and thus only the specified device can be authenticated using the passphrase. In PPSK, you can create a PPSK list and apply it to multiple wireless networks, saving you from repeatedly setting up the same information.

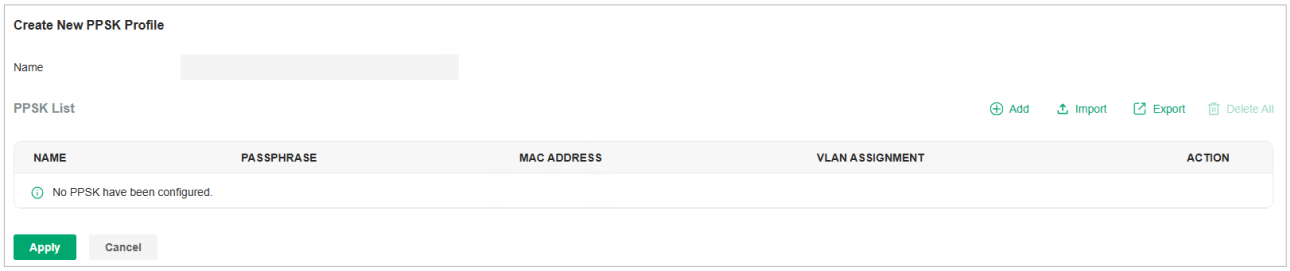
Configuration

To configure the PPSK profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Network Profile > PPSK. Click Create New PPSK Profile to add a new PPSK profile .



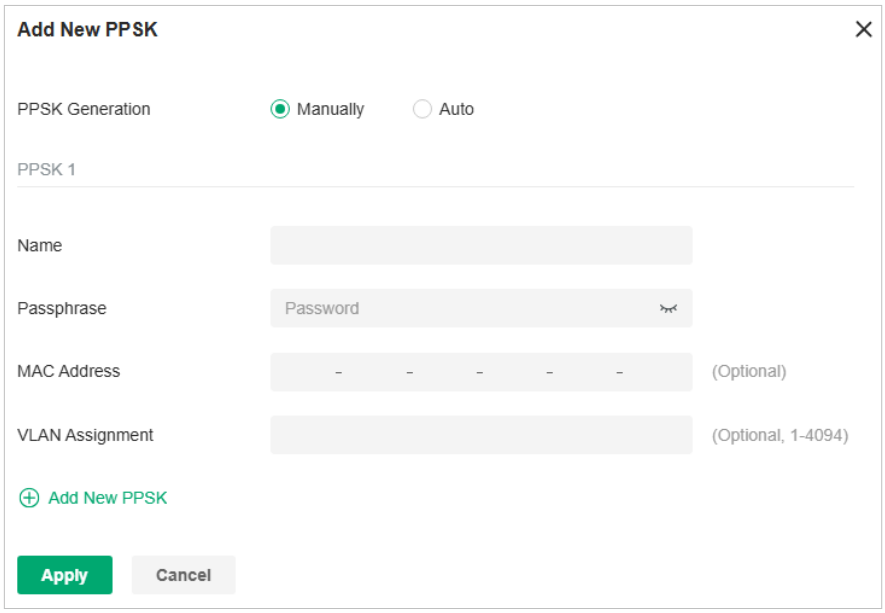
2. Enter a name for the new profile.



3. Add new entries to the PPSK profile.

- **Method 1: Add entries manually**

  Click Add and select Manually for PPSK Generation. Configure the parameters.

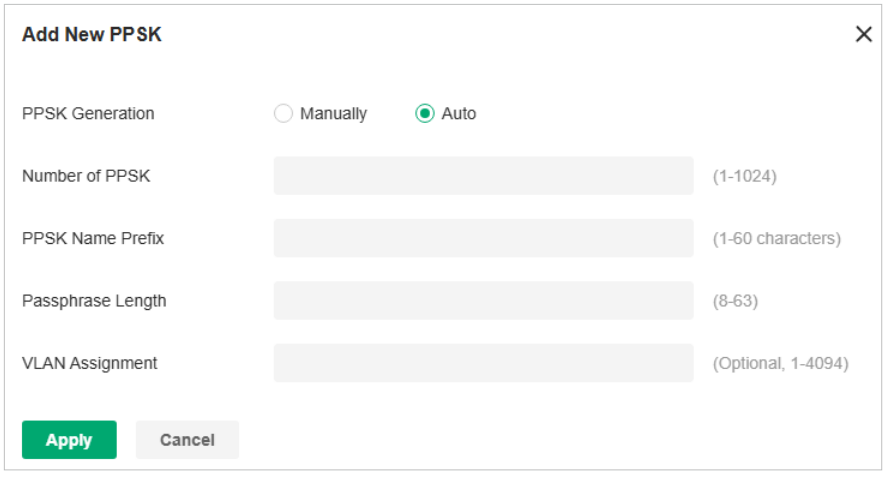


Name	Enter a name to identify the created PPSK.
Passphrase	Enter a passphrase, and the client will use the passphrase for authentication.
MAC Address	(Optional) Enter the MAC address of the device that can use the passphrase for authentication.
VLAN Assignment	(Optional) Enter the VLAN ID, and the client who uses the passphrase for authentication will be assigned to the specified VLAN.

Apply the settings. The new PPSK entry will be created.

- **Method 2: Add entries automatically**

  Click Add and select Auto for PPSK Generation. Configure the parameters and apply the settings.



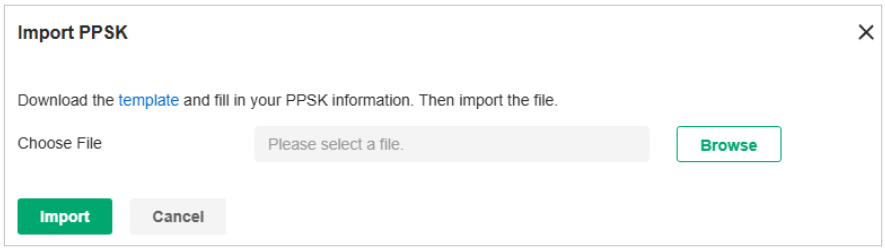
Number of PPSK	Enter the number of PPSK entries to create.
PPSK Name Prefix	Enter the prefix of the names for the created PPSK entries.

Passphrase Length	Enter the passphrase length.
VLAN Assignment	(Optional) Enter the VLAN ID, and the client who uses the passphrase for authentication will be assigned to the specified VLAN.

Apply the settings. New PPSK entries will be created automatically.

- **Method 3: Export and Import entries in batch**

  After creating PPSK entries, you can click Export to save them to a file locally, then access another site and click Import to import them in batches from the file.



4. After saving the newly added profile, you can apply them to wireless networks, refer to 4. 3. 1 Set Up Basic Wireless Networks.

4. 7. 5 Gateway QoS Service

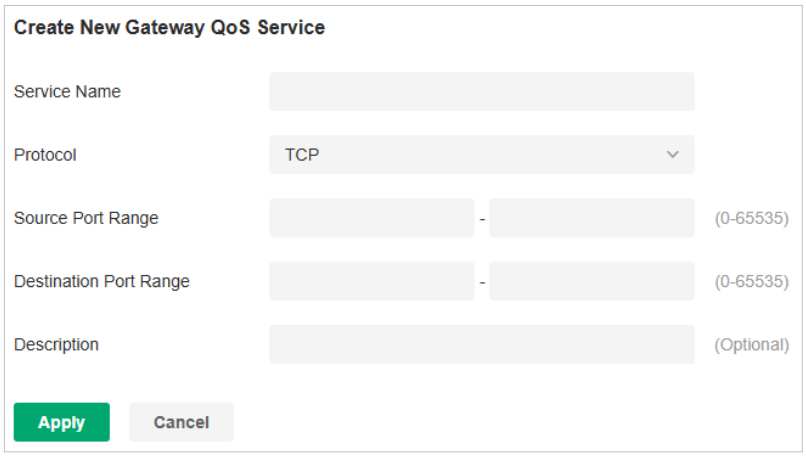
Overview

In Gateway QoS Service, you can define service type entries that will appear as matching conditions for you to choose when configuring the rules of related modules like QoS. The default entries cannot be edited or deleted. You can add other entries if your service type is not in the list.

Configuration

To configure the Gateway QoS Service profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Network Profile > Gateway QoS Service. Click Create New Gateway QoS Service to add a new profile .



2. Configure the parameters.

Service Name	Enter a name to identify the profile.
Protocol	Specify the protocol for the service. The system predefined protocols include TCP, UDP, TCP/UDP and ICMP. For other protocols, select the option Other.
Source Port Range	Specify the source port range for the service. Packets whose source port and destination port are both in the range are considered as the target packets.
Destination Port Range	Specify the destination port range for the service. Packets whose source port and destination port are both in the range are considered as the target packets.
Type	Specify the type of the ICMP packets. 255 means all types are included. ICMP packets with both the type and code fields matched are considered as the target packets.
Code	Specify the code of the ICMP packets. 255 means all codes are included. ICMP packets with both the type and code fields matched are considered as the target packets.
Protocol Number	Specify the protocol number of the packets. Packets matched with the protocol number are considered as the target packets.
Description	Enter a description for identification.

3. Click Apply to save the profile. Now you can select the predefined entry of service type when configuring rules of related modules like QoS.

4. 7. 6 Bonjour Service

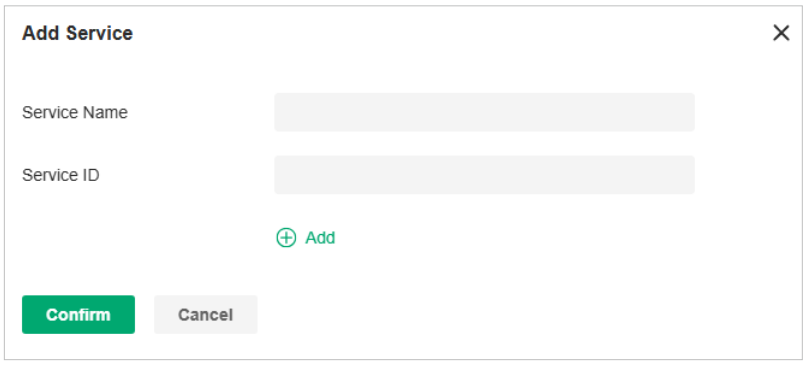
Overview

mDNS (Multicast DNS) Repeater can help forward mDNS request/reply packets between different VLANs. With this function, you can create a forwarding rule to allow the devices in the specified Client VLAN to discover the mDNS service in the specified Service VLAN. You can also specify the services to be forwarded.

Configuration

To configure the Bonjour Service profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Network Profile > Bonjour Service. Click Create New Bonjour Service to add a new profile .



2. Configure the parameters.

Service Name	Enter a name to identify the profile.
Service ID	Specify the domain name corresponding to the mDNS service. It is used to identify and filter mDNS packets.

3. Click Apply to save the profile.

4. 7. 7 RADIUS Profile

Overview

RADIUS (Remote Authentication Dial In User Service) is a client/server protocol that provides for the AAA (Authentication, Authorization, and Accounting) needs of modern IT environments.

In authentication services including 802.1X, Portal and MAC-Based Authentication, Omada devices operate as clients of RADIUS to pass user information to designated RADIUS servers. A RADIUS server maintains a database which stores the identity information of legal users. It authenticates users against the database when the users are requesting to access the network, and provides authorization and accounting services for them.

A RADIUS profile records your custom settings of a RADIUS server. After creating a RADIUS profile, you can apply it to multiple authentication policies like Portal and 802.1X, saving you from repeatedly entering the same information.

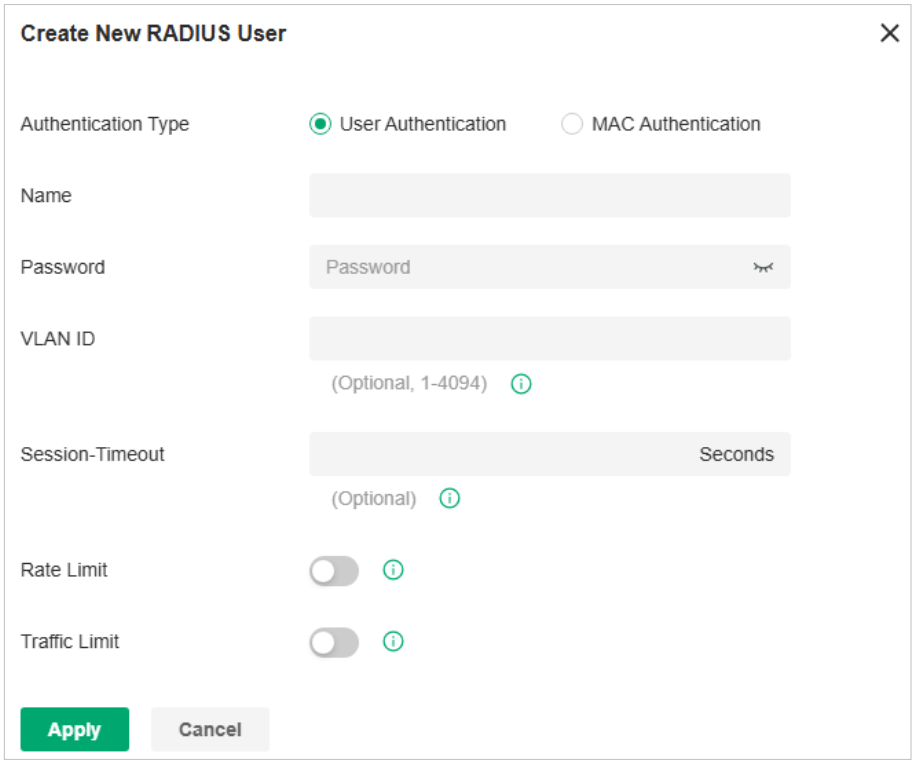
Configuration

- **Configure the Built-in RADIUS Profile (for on-premise controllers only)**

  a. Launch the controller and access a site. Go to Settings > Network Profile > RADIUS Profile.

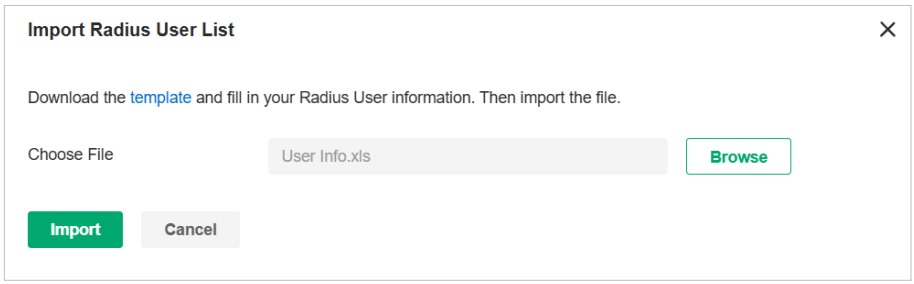
  b. An on-premise controller provides a Built-in RADIUS Profile. Click the edit icon of the profile, then add or import RADIUS users.

To add a new RADIUS user, click Add New RADIUS User and configure the parameters.



Authentication Type	Select the Authentication Type. User Authentication: Select this option and enter the user Name and Password for authentication. MAC Authentication: Select this option and enter the MAC Address for authentication.
VLAN ID	Enter a VLAN ID to assign VLANs to users.
Session-Timeout	Configure the authentication expiration time for users.
Rate Limit	When enabled, you can set limits for Uplink Rate and Downlink Rate of each client to balance bandwidth usage. This function applies to the portal service only.
Traffic Limit	When enabled, you can set limits for Uplink Traffic and Downlink Traffic of each client. This function applies to the portal service only.

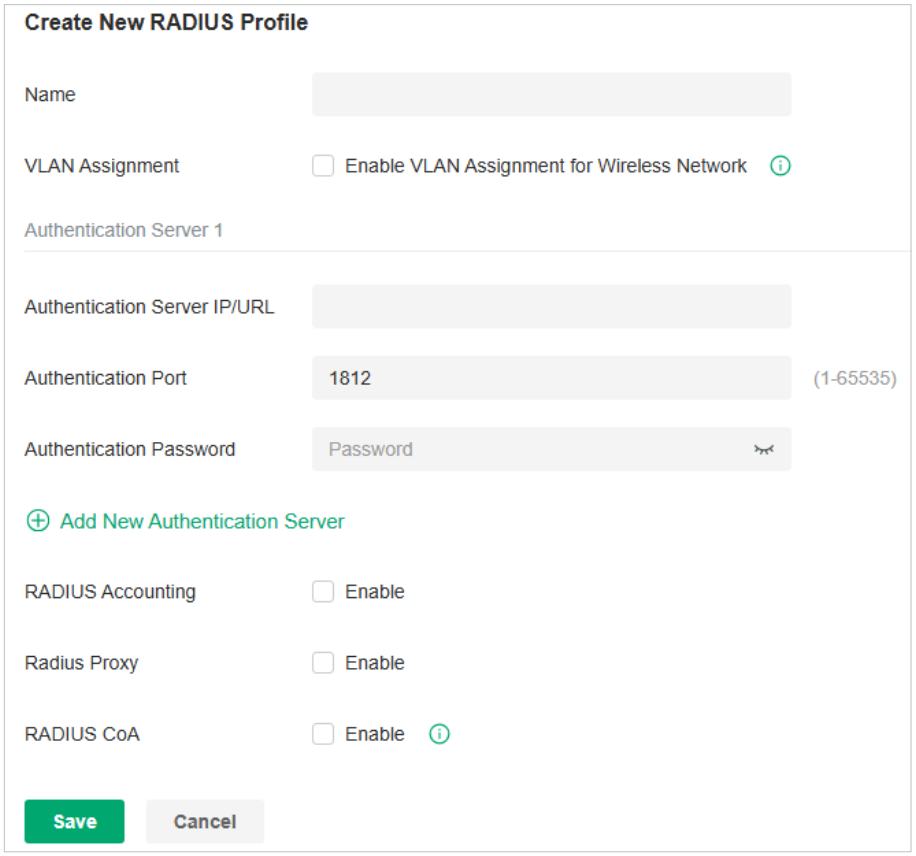
To import RADIUS users in batches, click Import, download the template and fill in your Radius User information. Then import the file.



Create New RADIUS Profile

a. Launch the controller and access a site. Go to Settings > Network Profile > RADIUS Profile.

b. Click Create New RADIUS Profile. Configure the parameters and save the settings.



Name	Enter a name to identify the RADIUS profile.
VLAN Assignment	This feature allows the RADIUS server to place a wireless user into a specific VLAN based on the credentials supplied by the user. To use the feature, you should create the specific VLAN first. And the user-to-VLAN mappings must be already stored in the RADIUS server database. **Note:** 1. VLAN Assignment is not currently supported when a client is authenticated by Portal with External RADIUS Server or RADIUS Hotspot. 2. VLAN Assignment is applicable only when the device supports the feature. To make this feature work properly, it is recommended to upgrade your devices to the latest firmware version.
Authentication Server IP	Enter the IP address of the authentication server.
Authentication Port	Enter the UDP destination port on the authentication server for authentication requests.
Authentication Password	Enter the password that will be used to validate the communication between network devices and the RADIUS authentication server.
RADIUS Accounting	Click the checkbox to enable RADIUS Accounting to meet billing needs. This feature is only available for APs with Portal to account for wireless clients.

Interim Update	Click the checkbox to enable Interim Update. By default, the RADIUS accounting process needs only start and stop messages to the RADIUS accounting server. With Interim Update enabled, network devices will periodically send an Interim Update (a RADIUS Accounting Request packet containing an "interim-update" value) to the RADIUS server. An Interim Update updates the user's session duration and current data usage.
Interim Update Interval	Enter an appropriate interval between the updates of users' session duration and current data usage.
Accounting Server IP	Enter the IP address of the RADIUS accounting server.
Accounting Port	Enter the UDP destination port on the RADIUS server for accounting requests.
Accounting Password	Enter the password that will be used to validate the communication between network devices and the RADIUS accounting server.
Radius Proxy	With this option enabled, the Controller will act as a proxy to forward the device's authentication messages to the corresponding RADIUS server.
RADIUS CoA	If enabled, TP-Link devices will act as a RADIUS Dynamic Authorization Server and will respond to RADIUS Change-of-Authorization and Disconnect messages sent by the RADIUS servers. This option is only supported by EAP PPSK, EAP MAC-Based Authentication, and EAP WPA-Enterprise.
CoA Password	CoA password is used to authenticate CoA and Disconnect messages sent by the RADIUS servers. The password must be the same as the secret used by RADIUS servers to send the CoA and Disconnect messages.

4. 7. 8 LDAP Profiles

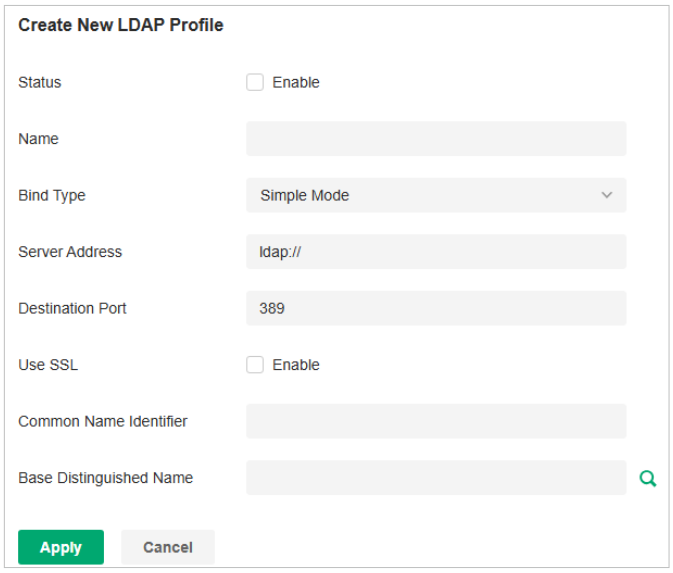
Overview

The Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for maintaining and accessing directory information over a network. LDAP Authentication allows you to bind the device to an LDAP server and use that server to authenticate LAN clients.

Configuration

To configure the LDAP profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Network Profile > LDAP Profile. Click Create New LDAP Profile to add a new profile .



2. Configure the parameters.

Status	Check the box to enable LDAP Authentication.
Name	Specify the profile name.
Bind Type	Select the LDAP Authentication mode: Anonymous Mode, Simple Mode, or Regular Mode.
Server Address	Enter the IP address of the LDAP server.
Destination Port	Enter the port ID of the LDAP server. By default, the port ID is 389 when SSL is disabled and 636 when SSL is enabled.
Use SSL	Determine whether to use SSL for LDAP communication.
Regular DN	Specify the distinguished name (DN) of the administrator account. This parameter is required in Regular mode.
Regular Password	Specify the password of the administrator account. This parameter is required in Regular mode.
Common Name Identifier	Specify the common name for user authentication. It is usually “cn”.
Base Distinguished Name	Specify the user identifier for user authentication. You can click the icon next to it to search and select from the LDAP directory tree.
Additional Filter	Specify the filter for user authentication. It is not supported in Simple Mode and is optional in other modes.
Group Distinguished Name	Specify the group identifier for user authentication. It is not supported in Simple Mode and is optional in other modes.

3. Click Apply to save the profile. Now you can select the predefined entry of LDAP profile when configuring rules of related modules like LDAP Server.

4. 7. 9 APN Profile

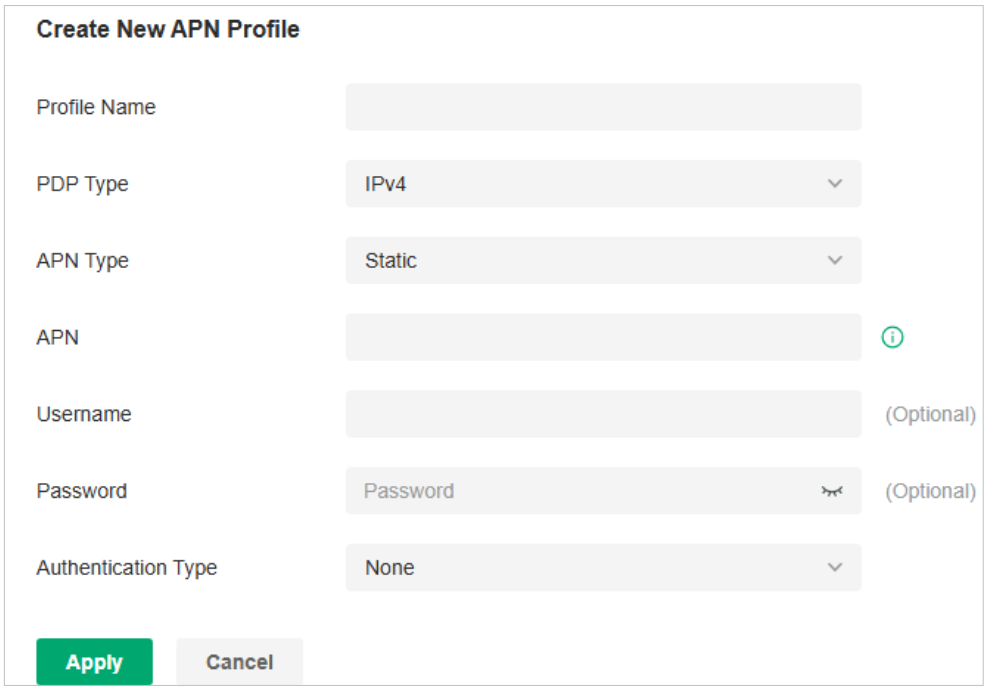
Overview

APN is a network access technology required when using the SIM card to access the internet. It determines which access method the SIM card uses to access the internet.

Configuration

To configure the APN profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Network Profile > APN Profile. Click Create New APN Profile to add a new profile .



2. Configure the parameters.

Profile Name	Specify the name of the profile.
PDP Type	Select the PDP (Packet Data Protocol) type: IPv4, IPv6, or IPv4 & IPv6.
APN Type	Select the APN type: Static or Dynamic.
APN	When APN Type is Static, specify the APN (access point name) provided by your ISP.
Username	Enter the username provided by your ISP. This field is case-sensitive.
Password	Enter the password provided by your ISP. This field is case-sensitive.

Authentication Type	Some ISPs need a specific authentication type, please confirm it with your ISP or keep the default value. None: No authentication is required. PAP: Password Authentication Protocol. The protocol allows a device to establish authentication with a peer using a two-way handshake. Select this option if your ISP requires this authentication type. CHAP: Challenge Handshake Authentication Protocol. The protocol allows a device to establish authentication with a peer using a three-way handshake and periodically checking the peer's identity. Select this option if your ISP requires this authentication type.
Apply to SIM	(For models with dual SIM cards) Select the SIM card to which the APN profile will be applied.

3. Click Apply to save the profile. Now you can select the predefined entry of APN profile when configuring rules of related modules.

4. 8 Authentication

Authentication is a portfolio of features designed to authorize network access to clients, which enhances the network security. Authentication services include 4. 8. 1 Portal, 4. 8. 2 802.1X and 4. 8. 3 MAC-Based Authentication, covering all the needs to authenticate both wired and wireless clients.

4. 8. 1 Portal

Overview

Portal authentication provides authentication service to the clients that only need temporary access to the network, such as the customers in a restaurant or in a supermarket. To access the network, these clients need to enter the authentication login page and use the correct login information to pass the authentication. In addition, you can customize the authentication login page and specify a URL which the authenticated clients will be redirected to.

Portal authentication takes effect on SSIDs and LAN networks. EAPs authenticate wireless clients which connect to the SSID with Portal configured, and the gateway authenticates wired clients which connect to the network with Portal configured. To make Portal authentication available for wired and wireless clients, ensure that both the gateway and EAPs are connected and working properly.

The controller provides several types of Portal authentication:

- **No Authentication**

  With this authentication type configured, clients can pass the authentication and access the network without providing any login information. Clients just need to accept the terms (if configured) and click the Login button.

- **Simple Password**

  With this authentication type configured, clients are required to enter the correct password to pass the authentication. All clients use the same password which is configured in the controller.

- **Hotspot**

  With this authentication type configured, clients can access the network after passing any type of the authentication:

  - **Voucher**

    Clients can use the unique voucher codes generated by the controller within a predefined time usage. Voucher codes can be printed out from the controller, so you can print the codes and distribute them to your costumers to tie the network access to consumption.

  - **Local User**

    Clients are required to enter the correct username and password of the login account to pass the authentication.

  - **SMS**

    Clients can get verification codes using their mobile phones and enter the received codes to pass the authentication.

- **RADIUS**

  Clients are required to enter the correct username and password which are stored in the RADIUS server to pass the authentication.

- **Form Auth**

  Clients are required to fill in a survey created by the network administrator to pass the authentication. It can be used for collecting feedback from your clients.

- **RADIUS Server**

  Clients are required to enter the correct username and password created on the RADIUS server to pass the authentication.

- **External Portal Server**

  The option of External Portal Server is designed for the developers. They can customize their own authentication type like Google account authentication according to the interface provided by the Controller.

Portal authentication can work with Access Control Policy, which grant specific network access to the users with valid identities. You can determine that the clients which didn't pass Portal authentication can only access the network resources allowed by Access Control Policy.

- **Pre-Authentication Access**

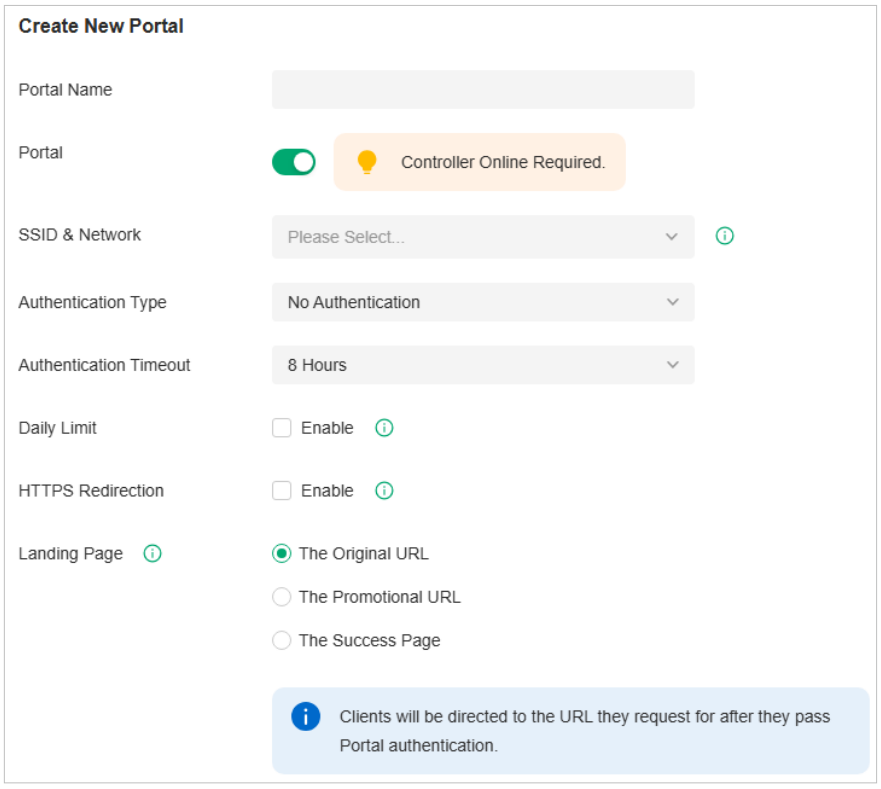
  Pre-Authentication Access allows unauthenticated clients to access the specific network resources.

- **Authentication-Free Client**

  Authentication-Free Clients allows the specific clients to access the specific network resources without authentication.

Create New Portal

1. Launch the controller and access a site. Go to Settings > Authentication > Portal.
2. On Portal tab, click Create New Portal. Specify the portal name and enable Portal.



3. Select the SSIDs and LAN networks for the portal to take effect. The clients connected to the selected SSIDs or LAN networks will have to log into a web page to establish verification before accessing the network.
4. Select the Authentication Type and configure authentication settings.

- **No Authentication**

Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.
Daily Limit	Click the checkbox to enable Daily Limit. With this feature enabled, after authentication times out, clients cannot get authenticated again until the next day. With this feature disabled, after authentication times out, clients can get authenticated again without limit.

- **Simple Password**

Password	Specify the password for the portal.
Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.

- **Hotspot**

Type	Select one or more authentication types according to your needs. Clients can access the network after passing any type of the authentication.

With different types of Hotspot selected, configure the related parameters.

- **Voucher Portal**

Voucher	Select Voucher and click Voucher Manager to manage the voucher codes. Refer to 7. 2. 3 Vouchers for detailed information about how to create vouchers.

- **Local User Portal**

Local User	Select Local User and click User Management to manage the information of the login accounts. Refer to 7. 2. 4 Local Users for detailed information about how to create Local Users.

- **SMS Portal**

Select SMS and configure the required parameters in the SMS section.

SMS	Clients can get verification codes using their mobile phones and enter the received codes to pass the authentication.
Twilio SID	Enter the Account SID for Twilio API Credentials.
Auth Token	Enter the Authentication Token for Twilio API Credentials.
Operating Phone Number	Enter the phone number that is used to send verification messages to the clients.
Maximum User Numbers	Click the checkbox and enter the maximum number of users allowed to be authenticated using the same phone number at the same time.
Authentication Timeout	Select the login duration. The client needs to log in again on the web authentication page to access the network.
Preset Country Code	Enter the default country code that will be filled automatically on the authentication page.

- **RADIUS Portal**

Select RADIUS and configure the required parameters in the RADIUS section.

Authentication Timeout	Clients are required to enter the correct username and password which are stored in the RADIUS server to pass the authentication.
RADIUS Profile	Select the RADIUS profile you have created. If no RADIUS profiles have been created, click Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS profile records the information of the RADIUS server which provides a method for storing the authentication information centrally.

Portal Logout	Check the box to allow clients to log out of the portal by accessing a URL (portal.tplink.net/portal/logout by default). You can change the default URL by editing portal.logout.domain in the omada.properties file. Some devices may require firmware update to support Portal Logout. Please refer to Configuration Result for details.
NAS ID	Configure a Network Access Server Identifier (NAS ID) on the portal. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups.
Disconnected Requests	With the feature enabled, the controller will listen on the receiver port for disconnect requests from the RADIUS server. When the controller receives the disconnect requests in correct format, the controller will terminate the RADIUS authentication session of the clients. Note that the feature is available only when the controller is accessible to the RADIUS server.
Receiver Port	Specify the port on which the controller listens when there are disconnect requests from the RADIUS server. Make sure that the specified port is not in use.
Status	The entry displays the status of the receiver port, including Running, Disabled, and Error. Running means that the port is available, Disabled means that the port is closed, and Error means that the port is already in use.

- **Configuring Form Authentication**

  Select Form Auth and click Create New Survey in the Form Authentication section. Then follow the on-screen instructions to create a survey by adding the type and number of questions you need. You can click Preview to view how the survey looks like on website and phone.

  Click Publish and then the created survey can be used for form authentication. A survey cannot be edited after it is published.

Survey Name	Specify a name for the survey for identification.
Duration	Specify how long clients can use the network after they pass the form authentication.

  Created surveys will be displayed for you to choose for the form authentication.

■ RADIUS Server

Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.
RADIUS Profile	Select the RADIUS profile you have created. If no RADIUS profiles have been created, click Create New RADIUS Profile from the drop-down list or click Manage RADIUS Profile to create one. The RADIUS profile records information of the RADIUS server including the IP address, port and so on.
NAS ID	Configure a Network Access Server Identifier (NAS ID) on the portal. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups.

Disconnected Requests	With the feature enabled, the controller will listen on the receiver port for disconnect requests from the RADIUS server. When the controller receives the disconnect requests in correct format, the controller will terminate the RAIDIUS authentication session of the clients. Note that the feature is available only when the controller is accessible to the RADIUS server.
Receiver Port	Specify the port on which the controller listens when there are disconnect requests from the RADIUS server. Make sure that the specified port is not in use.
Status	The entry displays the status of the receiver port, including Running, Disabled, and Error. Running means that the port is available, Disabled means that the port is closed, and Error means that the port is already in use.
Authentication Mode	Select the authentication protocol for the RADIUS server.
Portal Customization	Select Local Web Portal or External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the controller. The External Web Portal is provided by external portal server. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field.

- **External LDAP Server**

Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.
LDAP Profile	Select the LDAP profile you have created. If no LDAP profiles have been created, click Create New LDAP Profile from the drop-down list or click Manage LDAP Profile to create one. The LDAP profile records information of the LDAP server including the server address, port and so on.
Portal Customization	Select Local Web Portal or External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the controller. The External Web Portal is provided by external portal server. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field.

- **External Portal Server**

Custom Portal Server	Specify the IP address or URL that redirect to an external portal server.

5. Configure redirection and landing settings.

HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

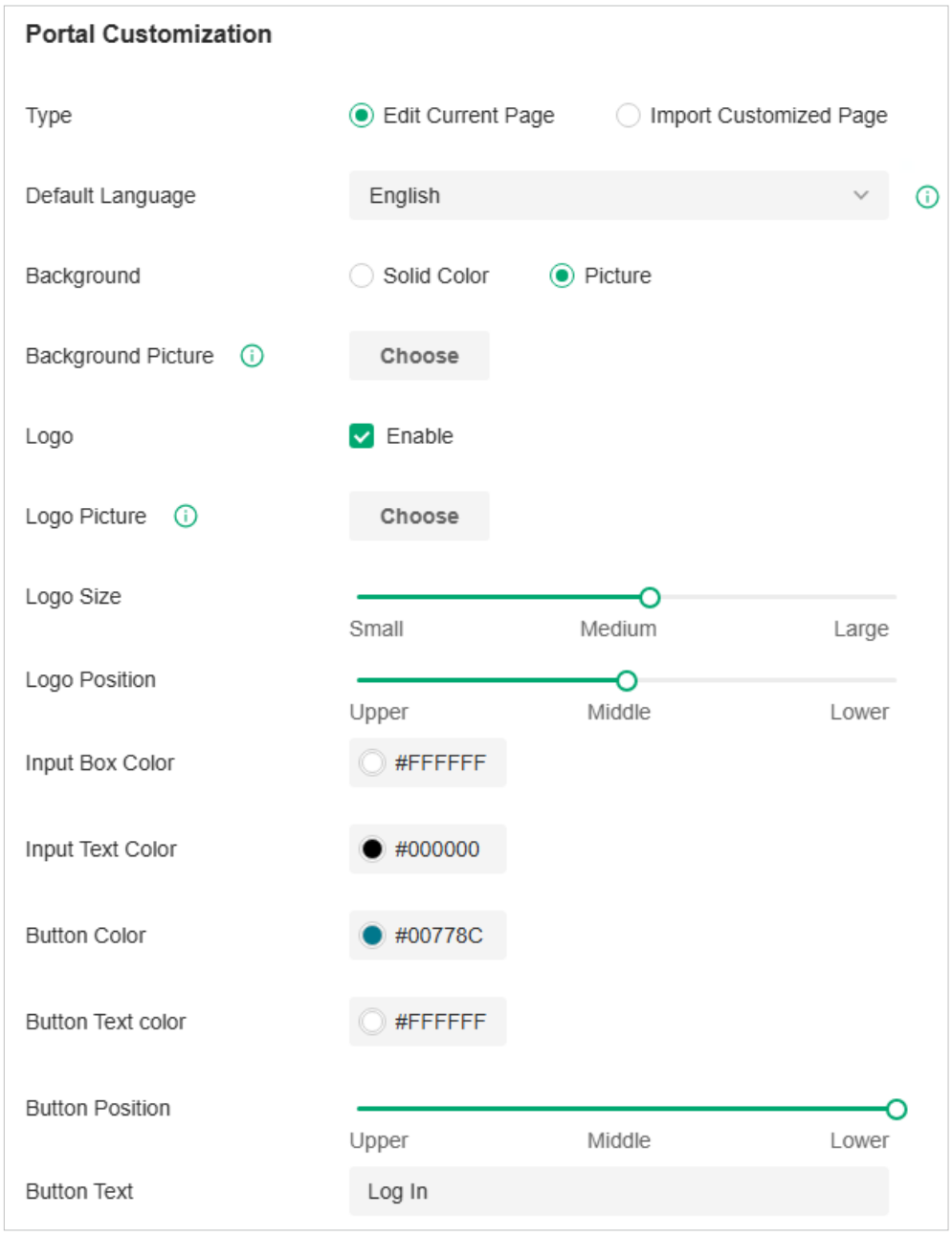
Landing Page	Select which page the client will be redirected to after a successful authentication. The Original URL: Clients are directed to the URL they request for after they pass Portal authentication. The Promotional URL: Clients are directed to the specified URL after they pass Portal authentication.

(Optional) Portal Customization

When creating or editing a portal entry, you can customize the Portal page in the Portal Customization section.

Note:

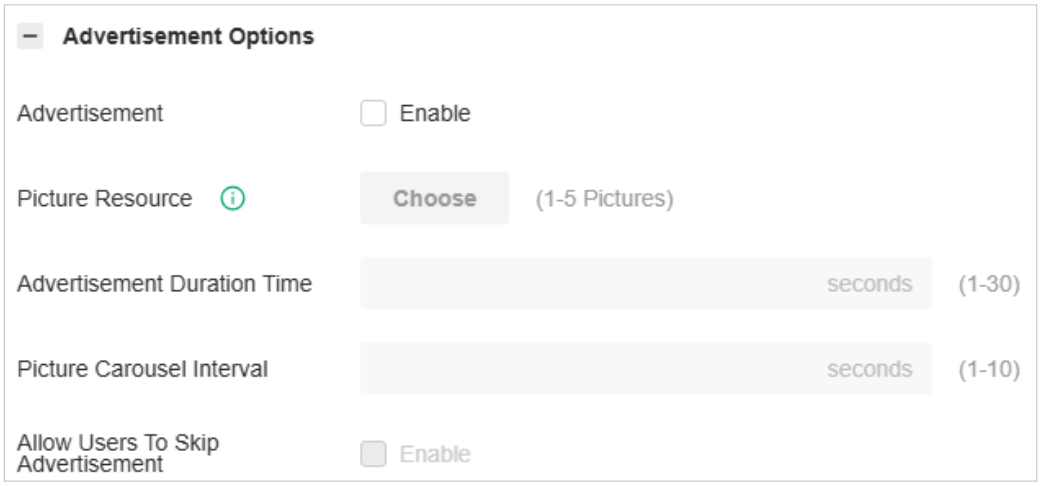
Portal Customization is not available when you configure external authentication types.



Type	Select the type of the Portal page. Edit Current Page: Edit the related parameters to customize the Portal page based on the provided page. Import Customized Page: Click Import to import your unique Portal page for branding it as per your business.
Default Language	Select the default language displayed on the Portal page. The controller automatically adjusts the language displayed on the Portal page according to the system language of the clients. If the language is not supported, the controller will use the default language specified here.
Background	Select the background type. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Picture: Click Choose and select a picture from your PC as the background.
Logo	Click to show the logo on the portal page.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Size/ Logo Position	Adjust the logo size and position on the Portal Page.
Input Box Color/ Input Text Color	(For cetain anthentication types) Configure your desired background and text color for the input box by entering the hexadecimal HTML color code manually or through the color picker.
Button Color/ Button Text Color	Configure your desired background and text color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Position	Select the button position on the Portal Page.
Button Text	Enter the text for the button.
Welcome Information	Click the checkbox and enter text as the welcome information. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.
Terms of Service	Click the checkbox and enter text as the terms of service in the following box. Click Add Terms to enter the name and context of the terms which will appear after a client clicks the link in Terms of Service.
Copyright	Click the checkbox and enter text as the copyright in the following box. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.

Show Redirection Countdown After Authorized	When enabled, the system will show the portal's redirection countdown.

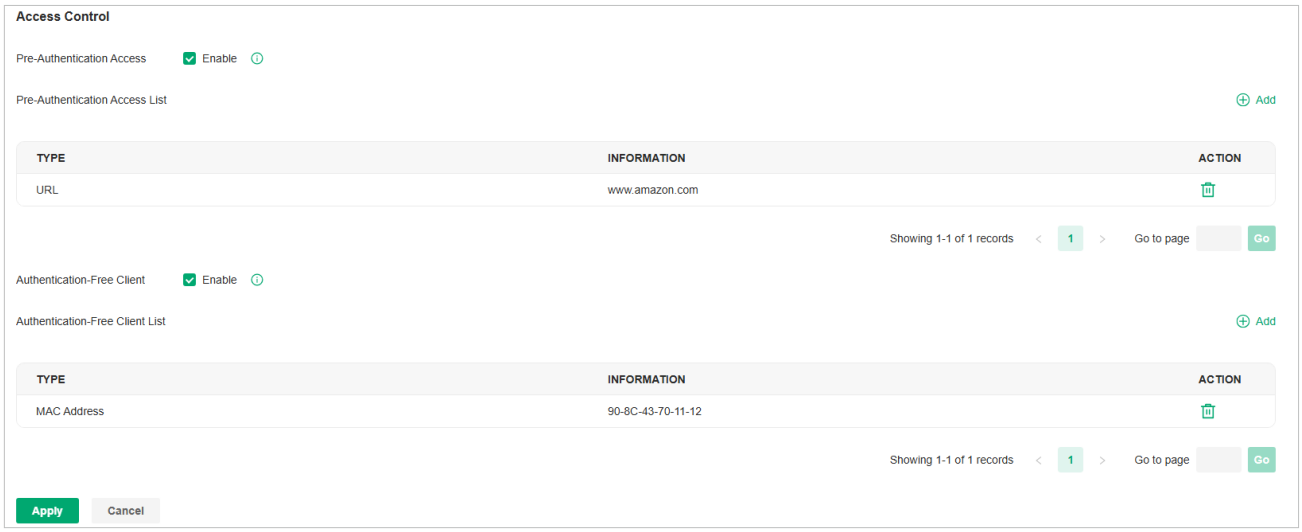
Click Advertisement Options and customize advertisement pictures on the authentication page if needed.



Advertisement	Click the checkbox to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears.
Picture Resource	Click Choose and select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Enter the duration time for the advertisement pictures. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Click the checkbox to allow users to skip the advertisement.

(Optional) Access Control

On Access Control tab, you can configure access control rules if needed.



Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click Add to configure the IP range or URL which unauthenticated clients are allowed to access.
Authentication-Free Policy	Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.
Authentication-Free Client List	Click Add and enter the IP address or MAC address of Authentication-Free clients.

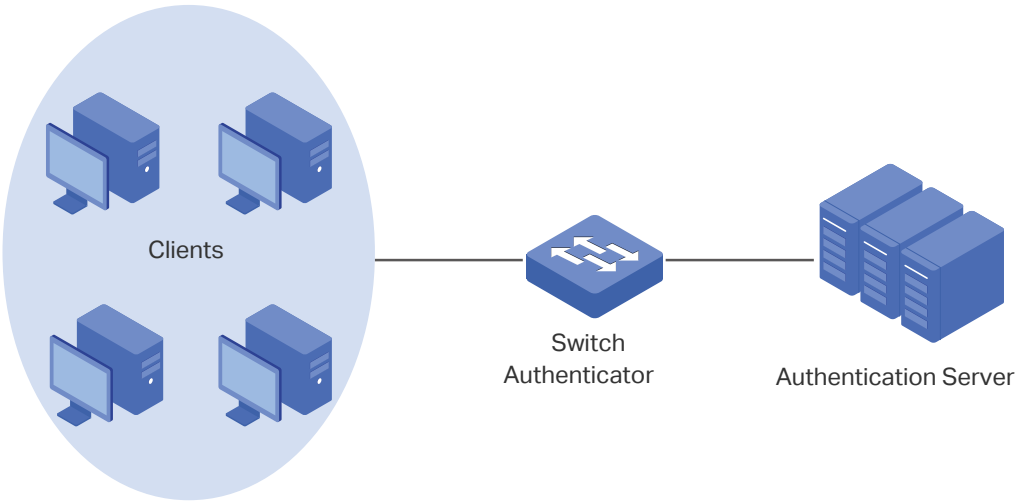
4. 8. 2 802.1X

Overview

802.1X provides port-based authentication service to restrict unauthorized clients from accessing to the network through publicly accessible switch ports. An 802.1X-enabled port allows only authentication messages and forbids normal traffic until the client passes the authentication.

Based on authenticated identity, 802.1X can also deliver customized services. For example, 802.1X and VLAN Assignment together make it possible to assign different authenticated users to different VLANs automatically.

802.1X authentication uses client-server model which contains three device roles: client/supplicant, authenticator and authentication server. This is described in the figure below:



- **Client**

  A client, usually a computer, is connected to the authenticator via a physical port. We recommend that you install TP-Link 802.1X authentication client software on the client hosts, enabling them to request 802.1X authentication to access the LAN.

- **Authenticator**

  An authenticator is usually a network device that supports 802.1X protocol. As the above figure shows, the switch is an authenticator.

  The authenticator acts as an intermediate proxy between the client and the authentication server. The authenticator requests user information from the client and sends it to the authentication server; also, the authenticator obtains responses from the authentication server and sends them to the client. The authenticator allows authenticated clients to access the LAN through the connected ports but denies the unauthenticated clients.

- **Authentication Server**

  The authentication server is usually the host running the RADIUS server program. It stores information of clients, confirms whether a client is legal and informs the authenticator whether a client is authenticated.

Based on authenticated identity, 802.1X can also deliver customized services. For example, 802.1X and VLAN Assignment together make it possible to assign different authenticated users to different VLANs automatically.

Configuration

To complete the 802.1X configuration, follow these steps:

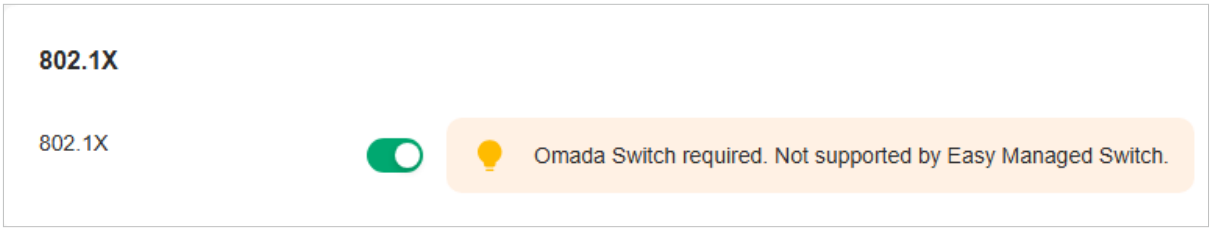
1) Click to enable 802.1X.

2) Select the RADIUS profile you have created and configure other parameters.

3) Select the ports on which 802.1X Authentication will take effect.

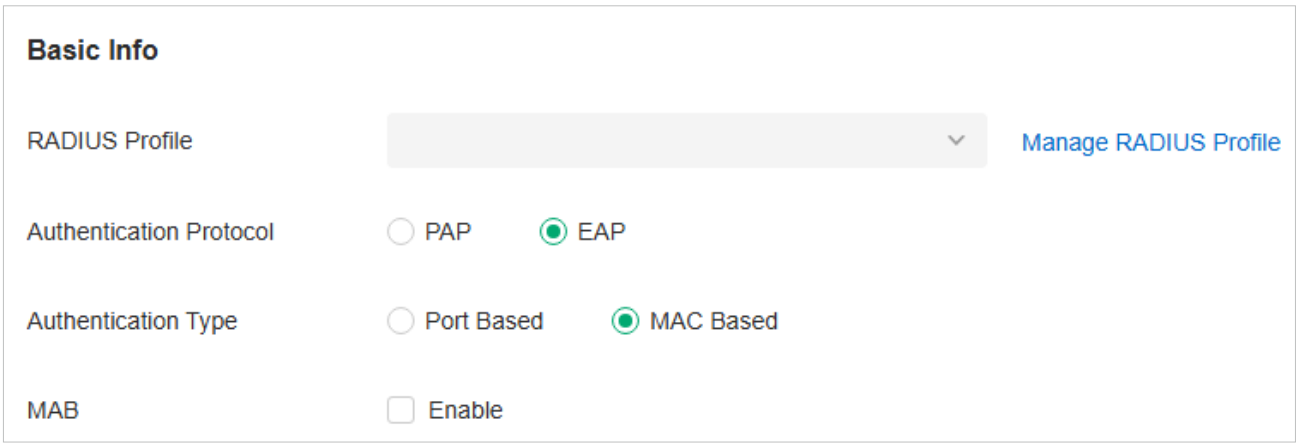
Step 1: Enable 802.1X

Launch the controller and access a site. Go to Settings > Authentication > 802.1X. Click to enable 802.1X.



Step 2: Configure RADIUS Profile and Parameters

Select the RADIUS profile you have created. If no RADIUS profiles have been created, click Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS profile records the information of the RADIUS server which acts as the authentication server during 802.1X authentication.

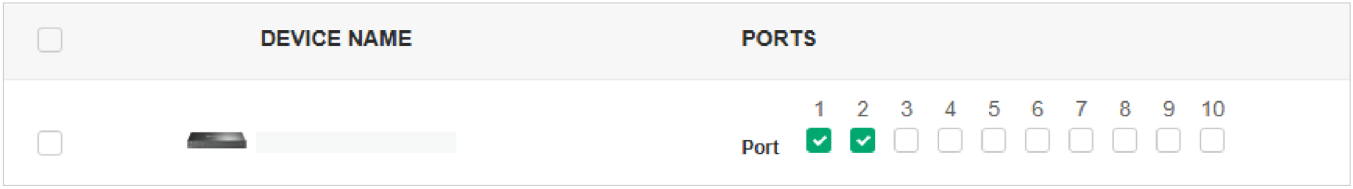


Authentication Protocol	Select the authentication protocol for exchanging messages between the switch and RADIUS server. As a bridge between the client and RADIUS server, the switch forwards messages for them. It uses AP packets to exchange messages with the client, and processes the messages according to the specified authentication protocol before forwarding them to the RADIUS server. PAP: The AP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the RADIUS server. AP: The AP packets are encapsulated in other protocol (such as RADIUS) packets, and transmitted to the authentication server. To use this authentication mechanism, the RADIUS server should support AP attributes.
Authentication Type	Select the 802.1X authentication type. Port Based: After a client connected to the port gets authenticated successfully, other clients can access the network via the port without authentication. MAC Based: Clients connected to the port need to be authenticated individually. The RADIUS server distinguishes clients by their MAC addresses.

VLAN Assignment	This feature allows the RADIUS server to send the VLAN configurations to the port dynamically. After the port is authenticated, the RADIUS server assigns the VLAN based on the username of the client connecting to the port. The username-to-VLAN mappings must be already stored in the RADIUS server database. This feature is available only when the 802.1X authentication type is Port Based.
MAB	MAB (MAC Authentication Bypass) allows clients to be authenticated without any client software installed. MAB is useful for authenticating devices without 802.1X capability like IP phones. When MAB is enabled on a port, the switch will learn the MAC address of the client automatically and send the authentication server a RADIUS access request frame with the client's MAC address as the username and password. MAB takes effect only when 802.1X authentication is enabled on the port.

Step 3: Select the Ports

Select the ports to enable 802.1X authentication or MAB for them. To enable 802.1X authentication, click the unselected ports. 802.1X-enabled ports will be marked with ☑. To enable MAB, click the ports marked with ☑. You can enable MAB only on 802.1X-enabled ports. MAB-enabled ports will be marked with ☑.



Note:

- You are not recommended to enable 802.1X authentication on the switch ports which connects to network devices without 802.1X capability like the router and APs.
- The switch authenticates wired clients which connect to the port with 802.1X enabled. And the gateway authenticates wired clients which connect to the network with Portal configured. Wired clients should pass Portal and 802.1X authentication to access the internet when both are configured.

4. 8. 3 MAC-Based Authentication

Overview

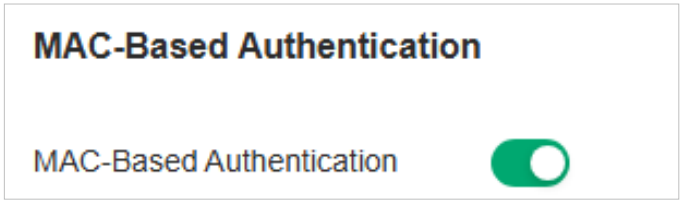
MAC-Based Authentication allows or disallows clients access to wireless networks based on the MAC addresses of the clients. In this authentication method, the controller takes wireless clients' MAC addresses as their usernames and passwords for authentication. The RADIUS server authenticates the MAC addresses against its database which stores the allowed MAC addresses. Clients can access the wireless networks configured with MAC-based authentication after passing authentication successfully.

Note:

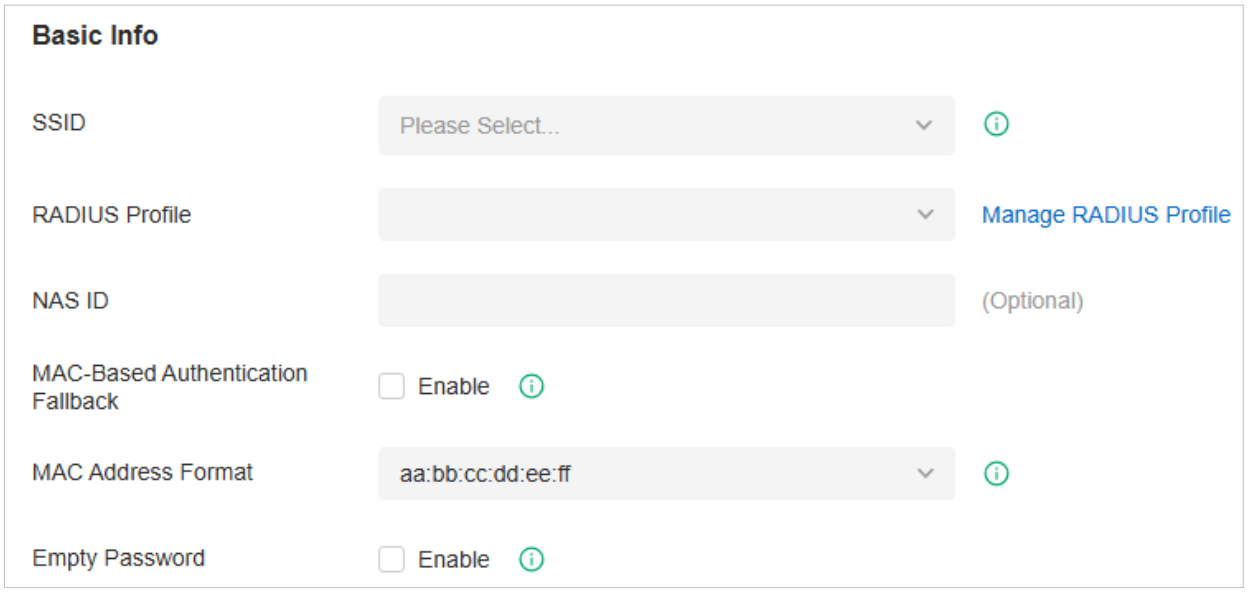
Both MAC-Based Authentication and Portal authentication can authenticate wireless clients. If both are configured on a wireless network, a wireless client needs to pass MAC-Based Authentication first and then Portal authentication for internet access. You can enable MAC-Based Authentication Fallback to allow clients bypass MAC-Based Authentication, which means the client needs to pass either of the two authentication. The client tries MAC-Based Authentication first, and is allowed to try portal authentication if it failed the MAC-Based Authentication.

Configuration

1. Launch the controller and access a site. Go to Settings > Authentication > MAC-Based Authentication. Click to enable MAC-Based Authentication.



2. In the Basic Info, select the SSIDs, RADIUS Profile and other required parameters. Refer to the following table to configure the required parameters and click Save.



SSID	Select one or more SSIDs for MAC-based authentication to take effect.
RADIUS Profile	Select the RADIUS profile you have created. If no RADIUS profiles have been created, click Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS profile records the information of the RADIUS server which acts as the authentication server during MAC-Based Authentication.
NAS ID	Configure a Network Access Server Identifier (NAS ID) for the authentication. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups.
MAC-Based Authentication Fallback	For the wireless network configured with both MAC-Based Authentication and Portal, if you enable this feature, a wireless client needs to pass only one authentication. The client tries MAC-Based Authentication first, and is allowed to try Portal authentication if it failed the MAC-Based Authentication. If you disable this feature as default, a wireless client needs to pass both the MAC-Based Authentication and portal authentication for internet access, and will be denied if it fails either of the authentication.

MAC Address Format	Select clients' MAC address format which the controller uses for authentication. Then configure the MAC addresses in the specified format as usernames for the clients on the RADIUS server.
Empty Password	Click to allow a blank password for MAC-Based Authentication. With this option disabled, the password will be the same as the username.

4. 9 Services

Services provide convenient network services and facilitate network management. You can set fixed IP address for certain device in DHCP Reservation, configure servers or terminals in DDNS, SNMP, UPnP, and SSH, schedule the devices in Reboot Schedule, PoE Schedule and Upgrade Schedule, and export the information in Export Data, and more.

4. 9. 1 DHCP Reservation

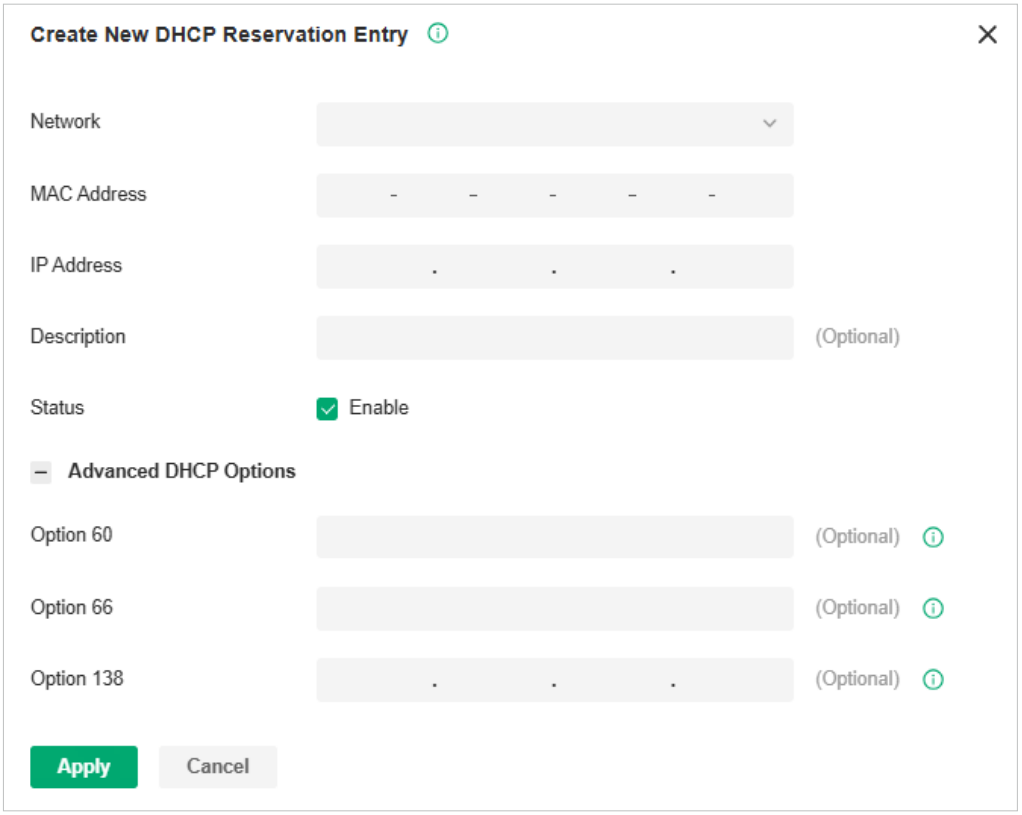
Overview

It is convenient for networks to use Dynamic IP addresses assigned by Dynamic Host Configuration Protocol (DHCP), however, for devices that need to be reliably accessed, it is ideal to set fixed IP addresses for them. DHCP Reservation allows you to reserve specific IP addresses for devices in your network, and centrally manage the IP addresses.

Configuration

- **To manually add DHCP Reservation entries:**

1. Launch the controller and access a site. Go to Settings > Services > DHCP Reservation.
2. Click Create New DHCP Reservation Entry and configure the parameters. Then click Apply.

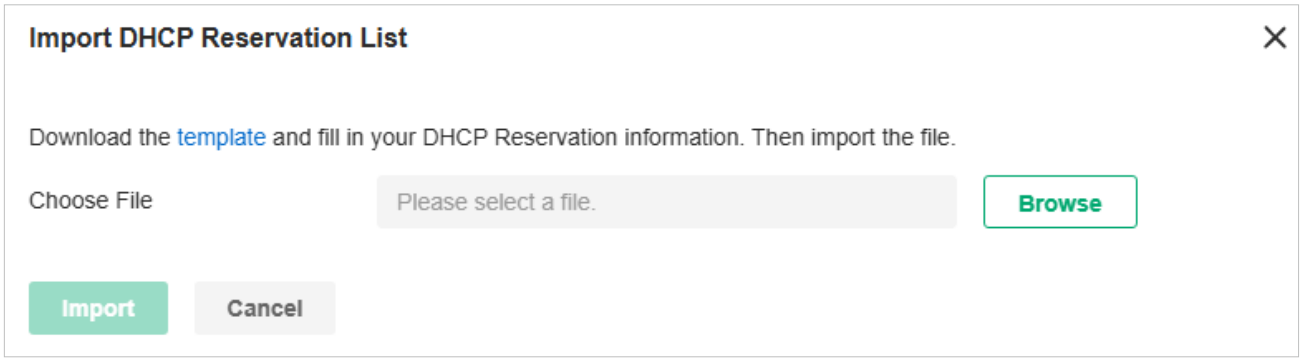


Network	Select the network the DHCP reservation entry is used for.

MAC Address	Specify the MAC address of the device for which you want to reserve an IP address.
IP Address	Specify the fixed IP address for the device.
Description	Enter description for the entry for identification.
Status	Enable or disable the entry.
Advanced DHCP Options	Configure the advanced DHCP options if needed. Option 60: Enter the value for DHCP Option 60. DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs. Option 66: Enter the value for DHCP Option 66. It specifies the TFTP server information and supports a single TFTP server IP address. Option 138: Enter the value for DHCP Option 138. It is used in discovering the devices by the system.

- **To import DHCP Reservation entries in batch:**

1. Launch the controller and access a site. Go to Settings > Services > DHCP Reservation.
2. Click Export to export the template in csv format. Based on this template, you can add custom address reservation entries that need to be imported.
3. Click Import and import the customized template. You can download the template, then edit and upload it for batch import.



4. 9. 2 Dynamic DNS

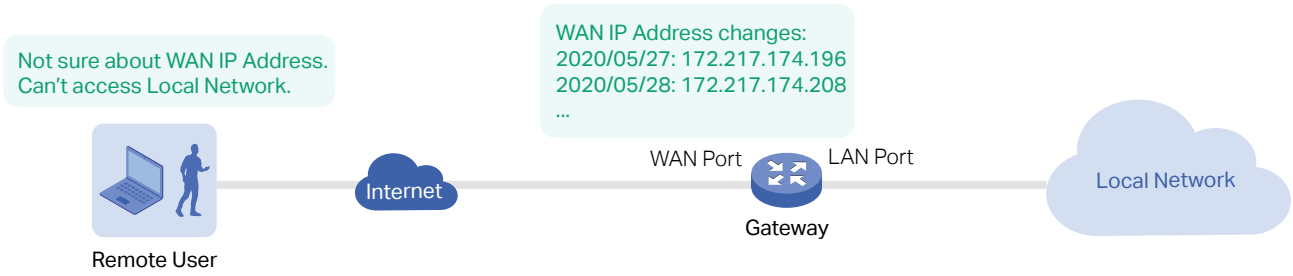
Overview

WAN IP Address of your gateway can change periodically because your ISP typically employs DHCP among other techniques. This is where Dynamic DNS comes in. Dynamic DNS assigns a fixed domain name to the WAN port of your gateway, which facilitates remote users to access your local network through WAN Port.

Let's illustrate how Dynamic DNS works with the following figures.

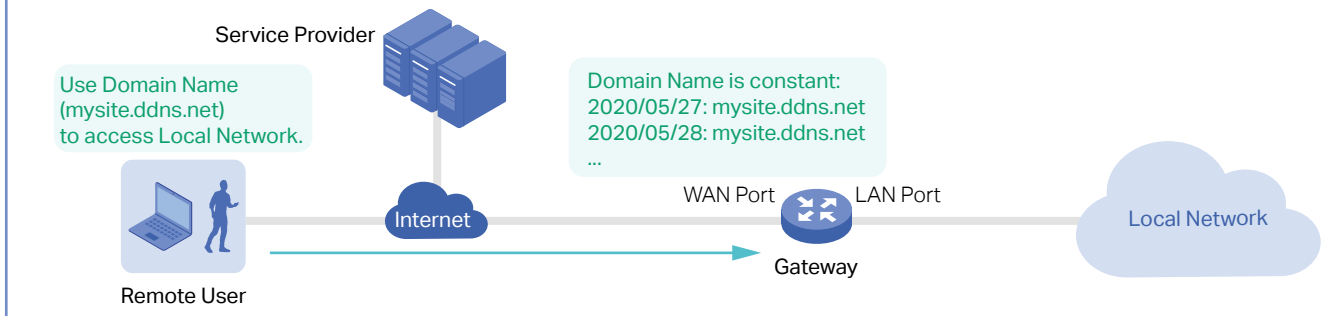
Before:

- WAN IP Address can change periodically, if it's dynamically assigned by the ISP using DHCP among other techniques.
- Remote User doesn't know what WAN IP Address is exactly at the moment, and cannot access Local Network.



After:

- Remote User can simply use Domain Name to access Local Network through WAN Port.
  In this example, Domain Name is mysite.ddns.net.

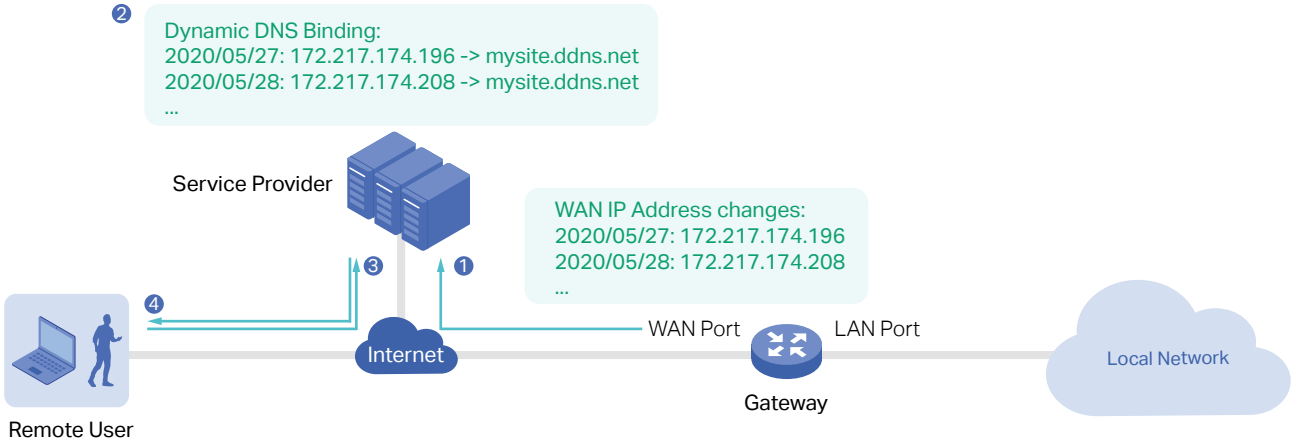


Prerequisite:

- Choose one Service Provider from the four that the controller supports, i.e. DynDNS, No-IP, Peanuthull, Comexe, TP-Link Dynamic DNS.
- Register at your Service Provider, then you get your Username and Password.
- Get your Domain Name from your Service Provider.

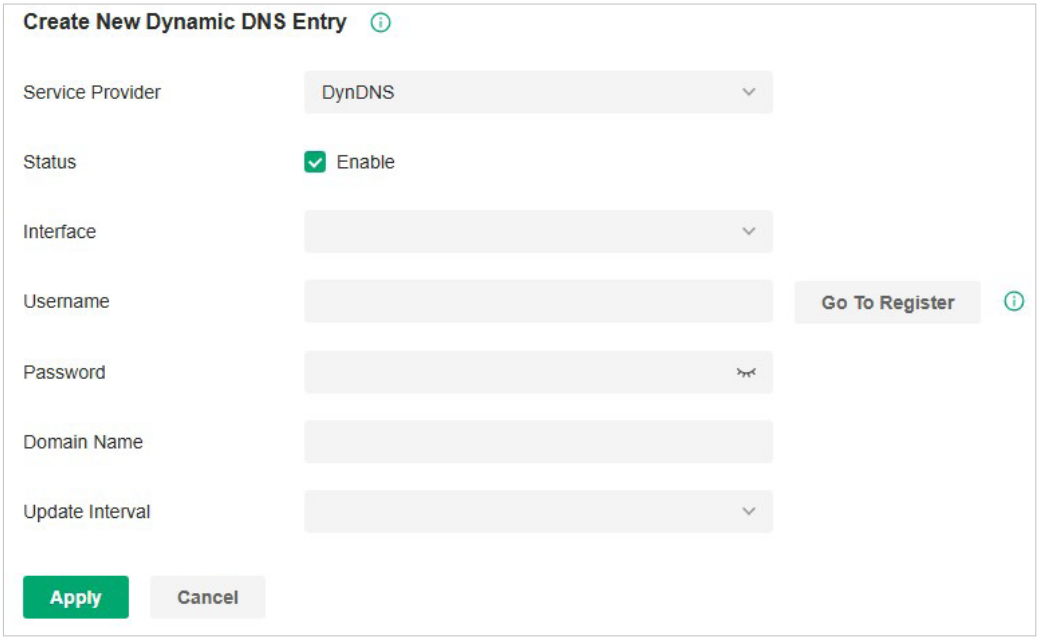
How Dynamic DNS works:

1. Gateway informs Service Provider of WAN IP Address.
2. Service Provider binds WAN IP Address with Domain Name and keeps it updated as WAN IP Address changes.
3. Remote User requests for WAN IP Address by sending Domain Name to Service Provider.
4. Service Provider replies with WAN IP Address, which Remote User actully uses to access Local Network through WAN Port.



Configuration

Launch the controller and access a site. Go to Settings > Services > Dynamic DNS. Click Create New Dynamic DNS Entry, to load the following page. Configure the parameters and click Create.



Service Provider	Select your service provider which Dynamic DNS works with.
Status	Enable or disable the Dynamic DNS entry.
Interface	Select the WAN Port which the Dynamic DNS entry applies to.
Username	Enter your username for the service provider. If you haven't registered at the service provider, click Go To Register.
Password	Enter your password for the service provider.
Domain Name	Enter the Domain Name which is provided by your service provider. Remote users can use the Domain Name to access your local network through WAN port.
Interval Mode	Choose to use fixed or custom interval.
Update Interval	Specify the update interval to report the changes of the WAN IP address for the DDNS service.

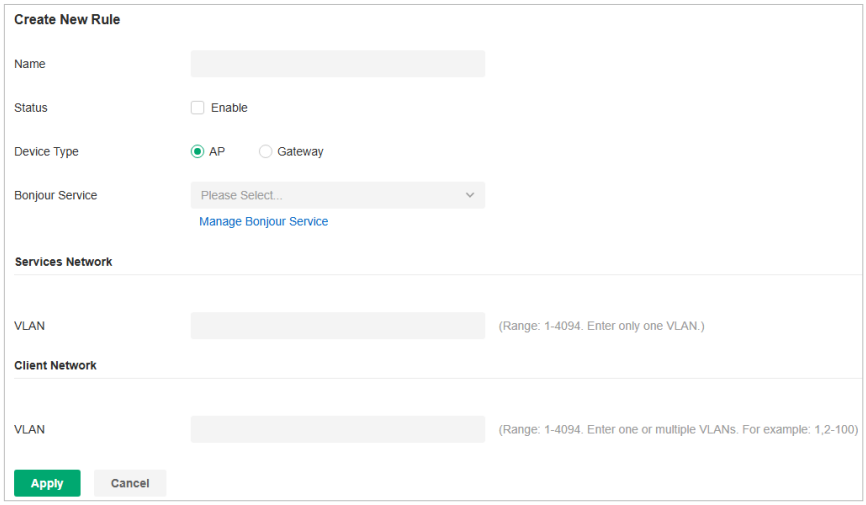
4. 9. 3 mDNS

Overview

mDNS (Multicast DNS) Repeater can help forward mDNS request/reply packets between different VLANs. With this function, you can create a forwarding rule to allow the devices in the specified Client VLAN to discover the mDNS service in the specified Service VLAN. You can also specify the services to be forwarded.

Configuration

1. Launch the controller and access a site. Go to Settings > Services > mDNS.
2. Click Create New Rule. Configure the parameters.



Name	Specify the rule name for identification.
Status	Enable or disable this rule.
Device Type	Specify the device type for which the rule takes effect.
Bonjour Service	Specify the services to be forwarded.
Services Network - VLAN	When Device Type is AP, specify the VLANs where the mDNS services are located. You can enter VLAN ranges or VLAN IDs separated by comma.
Client Network - VLAN	When Device Type is AP, specify the VLANs where the Client devices are located. You can enter VLAN ranges or VLAN IDs separated by comma.
Services Network - Network	When Device Type is Gateway, specify the networks where the mDNS services are located.
Client Network - Network	When Device Type is Gateway, specify the networks where the Client devices are located.

3. Apply the settings.

4. 9. 4 SNMP

Overview

SNMP (Simple Network Management Protocol) provides a convenient and flexible method for you to configure and monitor network devices. Once you set up SNMP for the devices, you can centrally manage them with an NMS (Network Management Station).

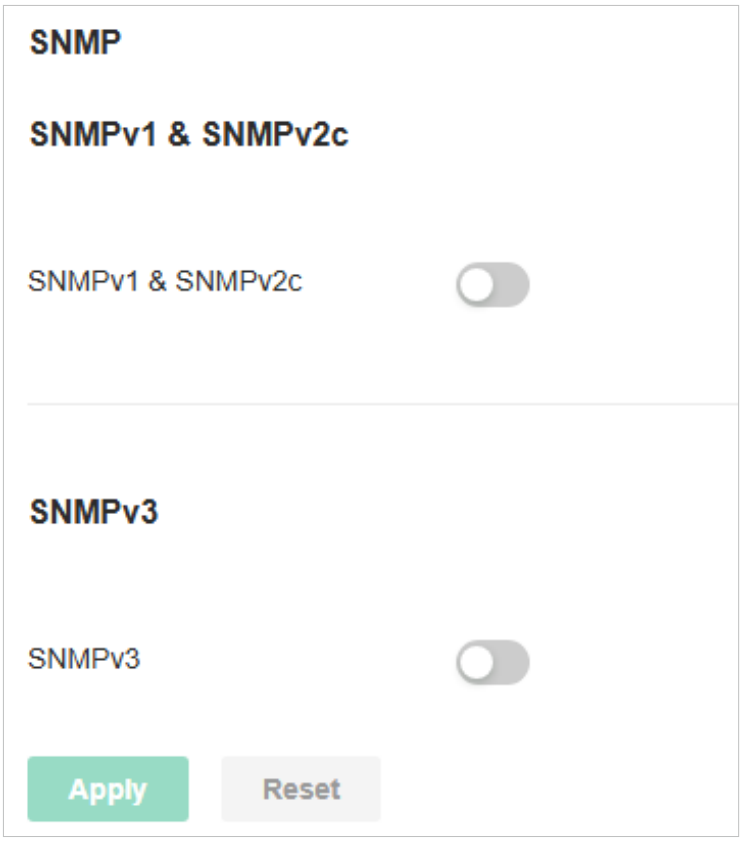
The controller supports multiple SNMP versions including SNMPv1, SNMPv2c and SNMPv3.

Note:

If you use an NMS to manage devices which are managed by the controller, you can only read but not write SNMP objects.

Configuration

Launch the controller and access a site. Go to Settings > Services > SNMP and configure the parameters. Then click Apply.



SNMPv1 & SNMPv2c	Enable or disable SNMPv1 and SNMPv2c globally.
Community String	With SNMPv1 & SNMPv2c enabled, specify the Community String, which is used as a password for your NMS to access the SNMP agent. You need to configure the Community String correspondingly on your NMS.
SNMPv3	Enable or disable SNMPv3 globally.
Username	With SNMPv3 enabled, specify the username for your NMS to access the SNMP agent. You need to configure the username correspondingly on your NMS.
Password	With SNMPv3 enabled, specify the password for your NMS to access the SNMP agent. You need to configure the password correspondingly on your NMS.

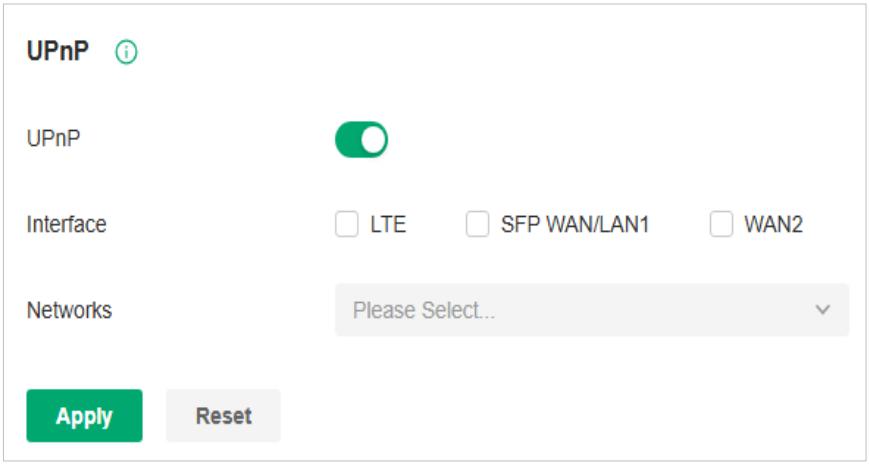
4. 9. 5 UPnP

Overview

UPnP (Universal Plug and Play) is essential for applications including multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) and remote assistance, etc. With the help of UPnP, the traffic between the endpoints of these applications can freely pass the gateway, thus realizing seamless connections.

Configuration

Launch the controller and access a site. Go to Settings > Services > UPnP. Enable UPnP globally and configure the parameters. Then click Apply.



Interface	Select the WAN port where UPnP takes effect.
Networks	Select the LAN interface where UPnP takes effect.

4. 9. 6 SSH

Overview

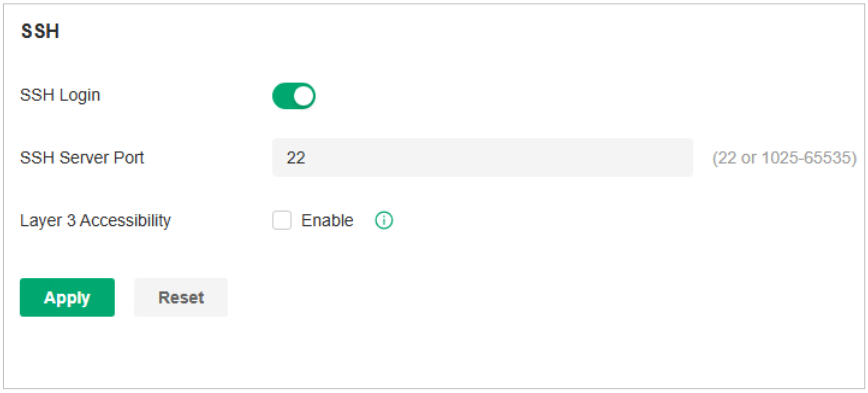
SSH (Secure Shell) provides a method for you to securely configure and monitor network devices via a command-line user interface on your SSH terminal.

Note:

If you use an SSH terminal to manage devices which are managed by the controller, you can only get the User privilege.

Configuration

Launch the controller and access a site. Go to Settings > Services > SSH. Enable SSH Login globally and configure the parameters. Then click Apply.



SSH Server Port	Specify the SSH Sever Port which your network devices use for SSH connections. You need to configure the SSH Server Port correspondingly on your SSH terminal.
Layer 3 Accessibility	With this feature enabled, the SSH terminal from a different subnet can access your devices via SSH. With this feature disabled, only the SSH terminal in the same subnet can access your devices via SSH.

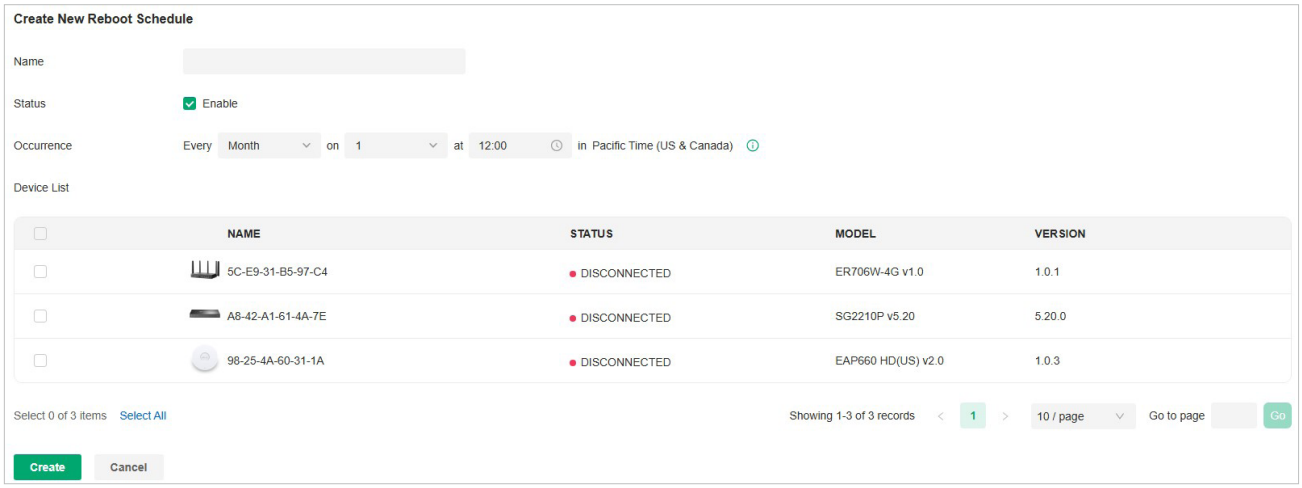
4. 9. 7 Reboot Schedule

Overview

Reboot Schedule can make your devices reboot periodically according to your needs. You can configure Reboot Schedule flexibly by creating multiple Reboot Schedule entries.

Configuration

1. Launch the controller and access a site. Go to Settings > Services > Reboot Schedule. Click Create New Reboot Schedule to load the following page and configure the parameters.



Name	Enter the name to identify the Reboot Schedule entry.
Status	Enable or disable the Reboot Schedule entry.
Occurrence	Specify the date and time for the devices to reboot.
Devices List	Select the devices which the Reboot Schedule applies to.

2. Click Create. The new Reboot Schedule entry will be added to the table.

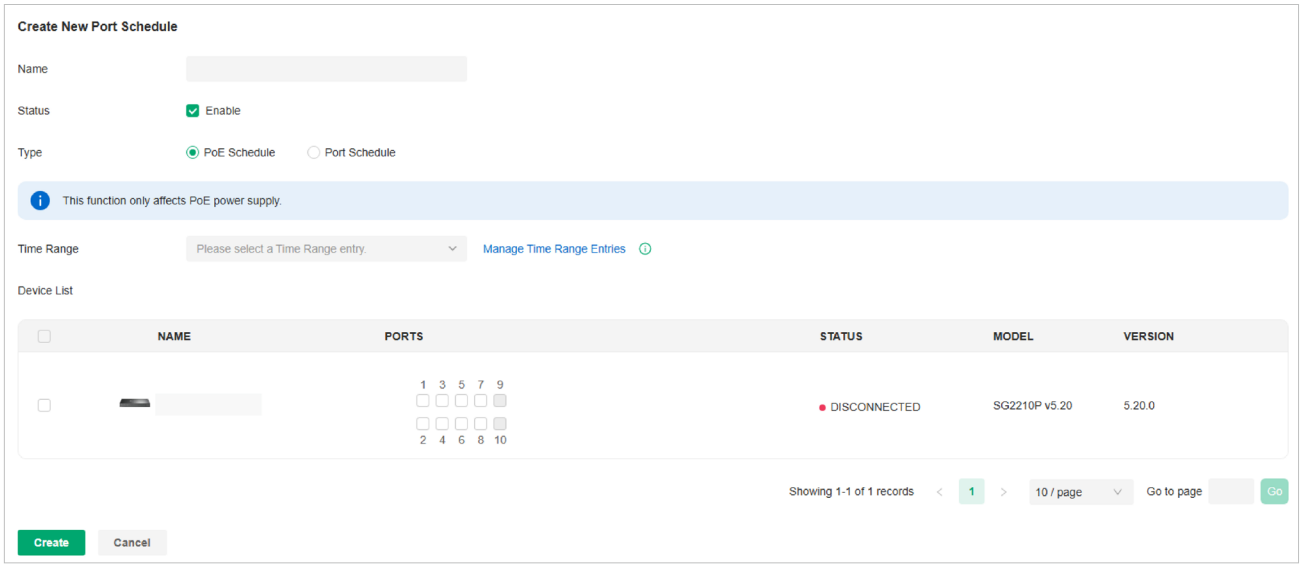
4. 9. 8 Port Schedule

Overview

In Port Schedule, you can set schedules to control the PoE feature of the PoE switch or control the on/off behavior of the switch port. When the PoE feature is disabled, the PoE switches will not supply power to the connected PoE devices during the specified time period, but the switches can still transmit data; when the Port feature is disabled, please check your topology and related configurations to avoid network problems. You can configure PoE or Port Schedule flexibly by creating multiple entries.

Configuration

1. Launch the controller and access a site. Go to Settings > Services > Port Schedule. Click Create New Port Schedule to load the following page and configure the parameters.



Name	Enter the name to identify the schedule entry.
Status	Enable or disable the schedule entry.
Type	Type:Specify the schedule type: PoE Schedule: This function only affects PoE power supply. Port Schedule: This function affects LAN connections of ports but does not affect PoE power supply. To avoid network problems, please check your topology and related configurations before turning off ports.

Time Range	When the Type is PoE Schedule, select the time range when the PoE switches will supply power to the powered devices. when the Type is Port Schedule, select the time range when the switches will turn on the designated ports. You can create a Time Range entry by clicking Create New Time Range Entry from the drop down list.
Devices List	When Type is PoE Schedule, select the PoE switch and PoE port to apply the schedule. When Type is Port Schedule, select the switch and port to apply the schedule.

2. Click Create. The new schedule entry will be added to the table.

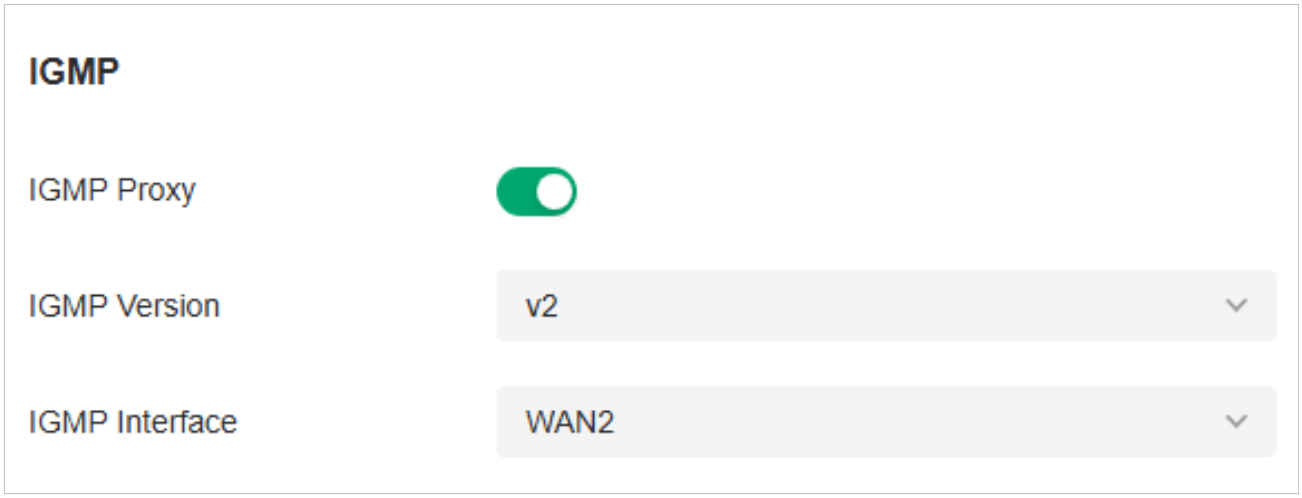
4. 9. 9 IPTV

Overview

IPTV includes two sections: IGMP and IPTV. In IGMP settings, you can enable IGMP proxy to detect multicast group membership information and thus the router is able to forward multicast packets based upon the information. IPTV settings allows you to enable Internet/IPTV/Phone service provided by your ISP.

Configuration

1. Launch the controller and access a site. Go to Settings > Services > IPTV > IGMP, configure the parameters. If you want to configure the IPTV settings, go to next step; if you don't want to configure the IPTV settings, click Apply.

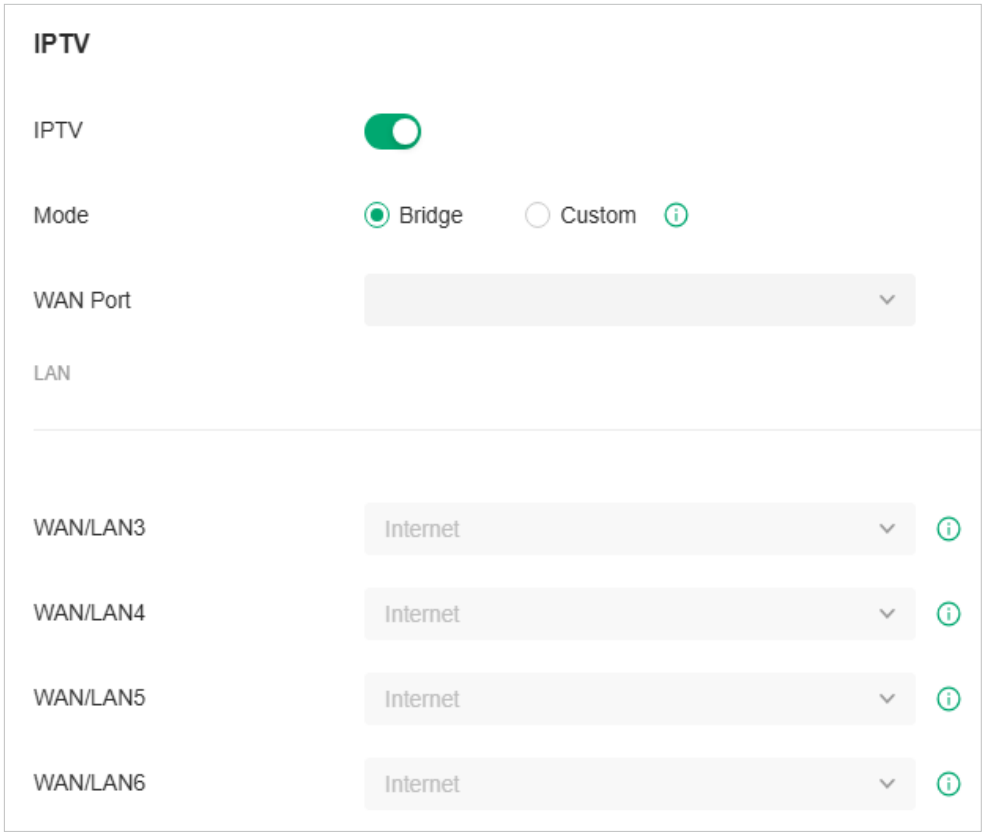


IGMP Proxy	Enable IGMP Proxy. IGMP Proxy sends IGMP querier packets to the LAN ports to detect if there is any multicast member connected to the LAN ports.

IGMP Version	Select the IGMP version as V2 or V3. The default is IGMP V2.
IGMP Interface	Select the WAN port on which the IGMP Proxy takes effect.

2. Go to Settings > Services > IPTV > IPTV, enable the IPTV features and choose the mode as Bridge or Custom according to your ISP. Then configure the corresponding parameters. Click Apply.

   Note that the IPTV section will be hidden if your device is an earlier version that does not support this feature.



IPTV	Enable IPTV feature.
Mode	Select the appropriate Mode according to your ISP. Bridge: Select this mode if your ISP requires no other parameters. Custom: Select this mode if your ISP provides necessary parameters, and configure the parameters according to the requirements of your ISP.
WAN Port	Select the WAN port on which the IPTV settings take effect.
Port Mode	Select the appropriate Port Mode of the LAN ports to determine which port is used to support Internet service, IPTV service, or IP Phone service.

4. 9. 10 DNS Proxy

Overview

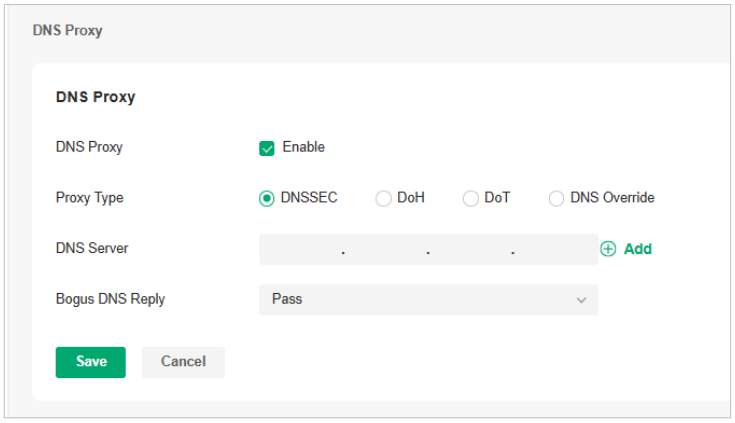
DNS Proxy provides the LAN side clients with the DNS query service. It forwards the DNS request from the LAN side clients to the selected upstream DNS server and forwards the DNS reply accordingly.

DNSSEC (DNS Security Extensions), DoT (DNS over TLS), DoH (DNS over Https), and DNS Override are security options for DNS Proxy. DNSSEC will verify the integrity of DNS records, and DoT / DoH will encrypt the query. DNS Override lets you choose your preferred DNS servers.

All the options need an upstream DNS server that supports them.

Configuration

1. Launch the controller and access a site. Go to Settings > Services > DNS Proxy.
2. Configure the parameters, then save the settings.



DNS Proxy	Enable or disable the DNS Proxy.
Proxy Type	Specify a security option to apply.
DNS Server	Specify the upstream DNS server which the DNS requests will be forwarded to. For DoT and DoH, the system provides some known public DNS servers that support these security options. For DoH, the upstream DNS servers are usually websites with https URLs. For DNSSEC and DoT, servers are usually IP address.
Bogus DNS Reply	This is an special option for DNSSEC. Choose to pass/drop the bogus reply if the integrity of DNS records failed to be verified (which means the DNS record may be modified and is not trustable).

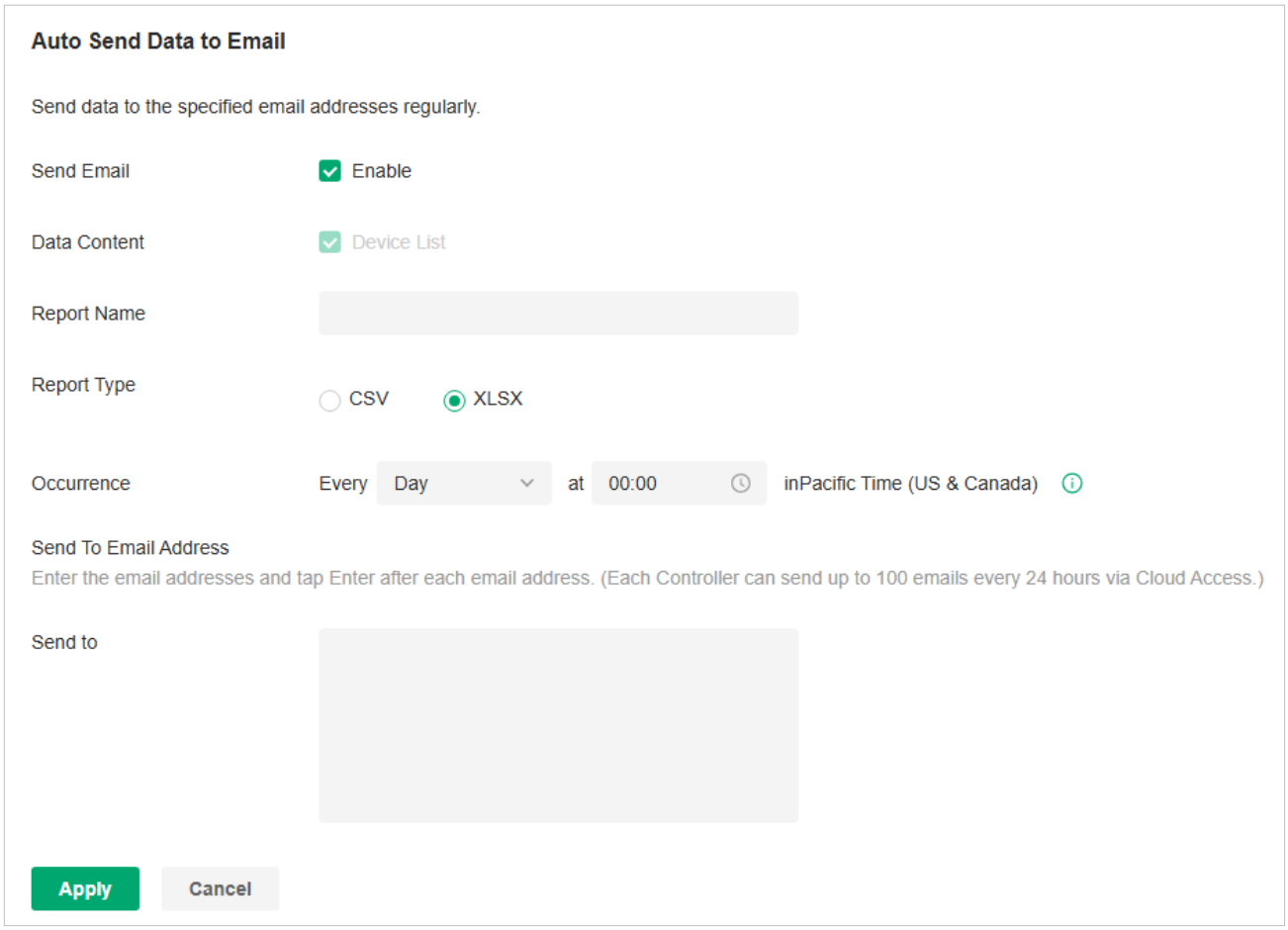
4. 9. 11 Auto Send Data to Email

Overview

In Export Data, you can export the data of the Controller to monitor or debug the connected devices.

Configuration

1. Launch the controller and access a site. Go to Settings > Services > Auto Send Data to Email.
2. Enable Send Mail, configure the parameters, then save the settings.



4. 10 SIM

If your network has devices that connect to the internet via the SIM card, such as the 4G Wi-Fi router, you can configure SIM settings.

4. 10. 1 Statistics

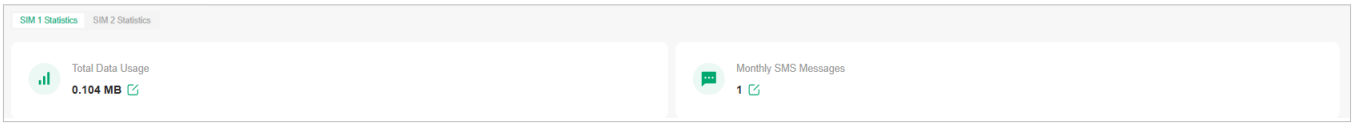
Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > SIM > Statistics.

Statistics Overview

In the upper cards on the Statistics page, you can have a overview of the total/monthly statistics calculated according to the billing/counting method you set. You can click the edit icon to correct the statistics.

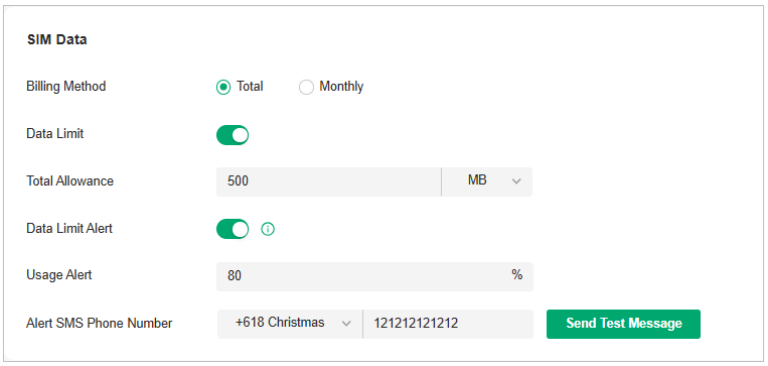
For models with dual SIM cards, you can click each tab to view its statistics.

Note that the data statistics is for reference only, and the actual data shall be subject to your carrier. You can send messages to your carrier for the most accurate data usage statistics.



Manage SIM Data

In the SIM Data section, you can view the data statistics and set a data limit to better control your data usage so that you will not exceed the data package provided by your carrier.

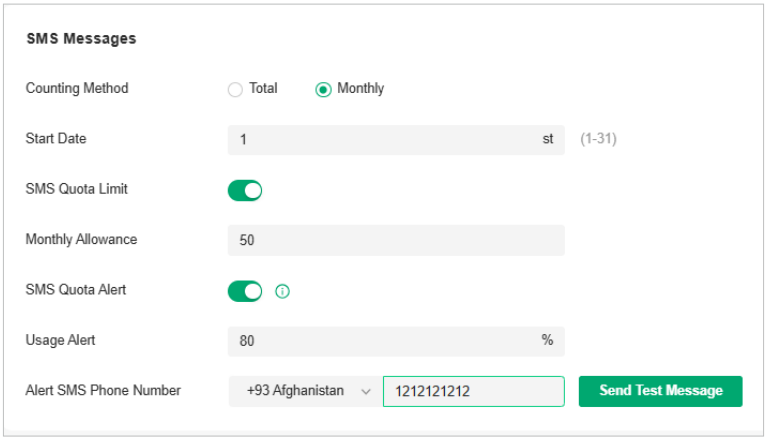


Billing Method	Select the billing method, Total count or Monthly count. If you select the Monthly count, select a Start Date for each monthly count cycle. For example, 2nd indicates that the monthly count cycle is from the 2nd of this month to the 1st of the next month.
Data Limit	Specify whether to enable the data limit function. If turned on, the network will be disconnected when your data usage reaches the allowance.

Total Allowance/ Monthly Allowance	Enter the total/monthly allowance provided by your carrier. The device will automatically disconnect from the internet when your data usage reaches the allowance.
Data Limit Alert	Specify whether to enable the SMS alert of data limit. If turned on, the alert message will be sent when your data usage reaches the set allowance percentage or the set allowance.
Usage Alert	Set the usage alert percentage. The alert message will be sent when your data usage reaches the set allowance percentage.
Alert SMS Phone Number	Enter the phone number to receive the SMS alert message when your data usage reaches the set allowance percentage or the set allowance.
Send Test Message	Send a test SMS to confirm that the number can receive the SMS alert message.

Manage SMS Messages

In the SMS Messages section, you can set SMS quota to better manage SMS usage so that it does not exceed your set quota.



Counting Method	Select the counting method, Total count or Monthly count. If you select the Monthly count, select a Start Date for each monthly count cycle. For example, 2nd indicates that the monthly count cycle is from the 2nd of this month to the 1st of the next month.
SMS Quota Limit	Specify whether to enable the SMS quota limit function. If turned on, your device will be unable to send SMS messages when your SMS quantity reaches the allowance.
Total Allowance/ Monthly Allowance	Enter the total/monthly allowance provided by your carrier. Your device will be unable to send SMS messages when your SMS quantity reaches the allowance.

SMS Quota Alert	Specify whether to enable the SMS alert of SMS limit. If turned on, the alert message will be sent when your SMS quantity reaches the set allowance percentage. Note that the alert messages will also be counted in your SMS quantity.
Usage Alert	Set the usage alert percentage. The alert message will be sent when your SMS quantity reaches the set allowance percentage.
Alert SMS Phone Number	Enter the phone number to receive the SMS alert message when your SMS quantity reaches the set allowance percentage.
Send Test Message	Send a test SMS to confirm that the number can receive the SMS alert message.

4. 10. 2 SMS Message

■ SMS Inbox Message

SMS Inbox displays the messages you have received.

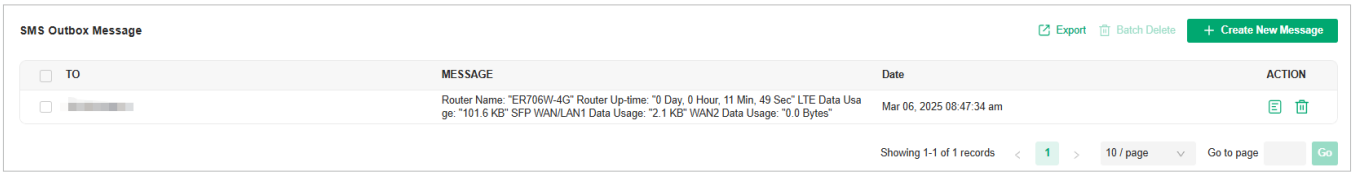
Click the Detail icon to view the SMS details. Click the Delete icon to delete the SMS. You can also batch read or delete entries.



■ SMS Outbox Message

SMS Outbox displays the messages you have successfully sent.

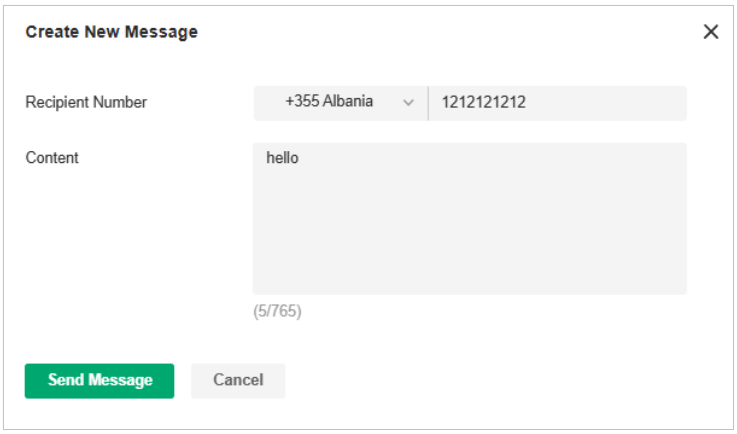
Click the Detail icon to view the SMS details. Click the Delete icon to delete the SMS. You can also batch delete entries.



Click Export to save outbox messages of specific time period locally.



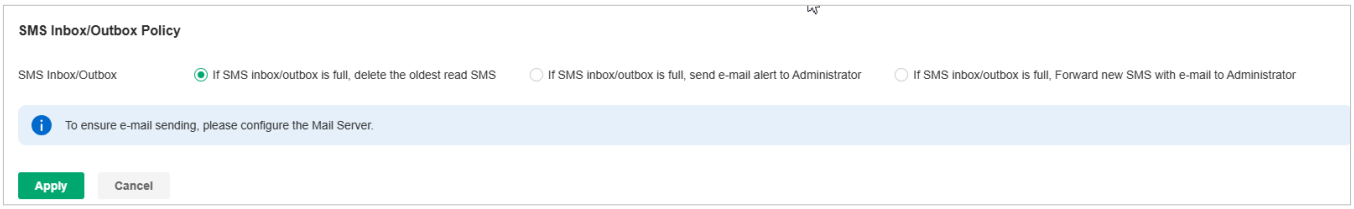
Click Create New Message to send a message.



4. 10. 3 SMS Settings

■ SMS Inbox/Outbox Policy

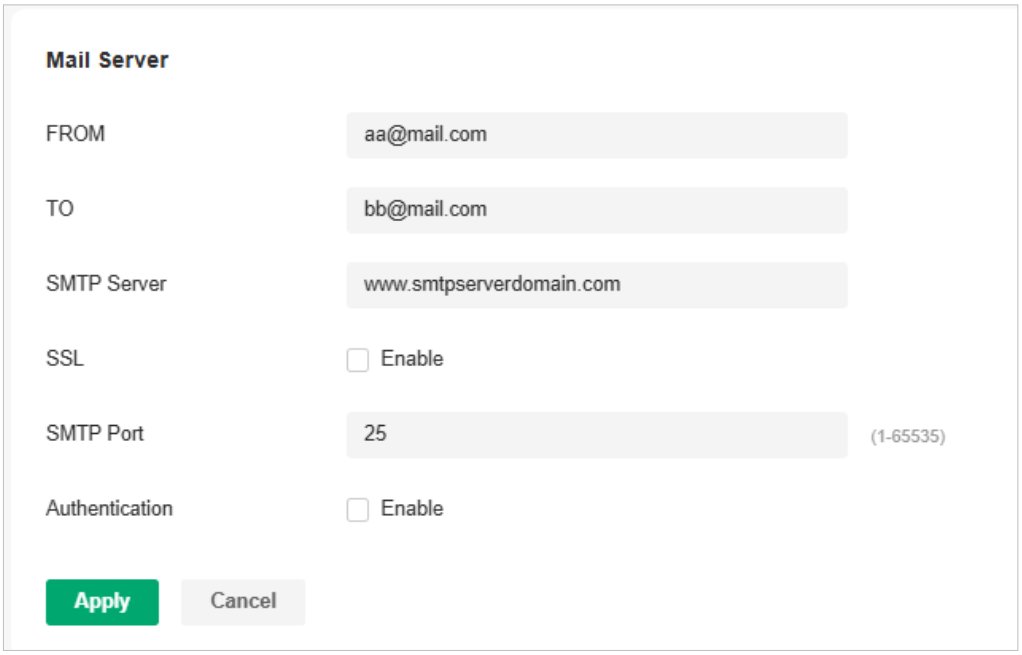
In this section, you can set policies related to receiving inboxes.



SMS Inbox/Outbox	Select the SMS Inbox/Outbox Policy. If SMS inbox/outbox is full, delete the oldest read SMS: When the inbox/outbox is full, delete the oldest read SMS to receive the new SMS. If SMS inbox/outbox is full, send e-mail alert to Administrator: When the inbox/outbox is full, send an email to the administrator, and does not receive the new SMS. To ensure email sending, please configure the Mail Server. If SMS inbox/outbox is full, forward new SMS with e-mail to Administrator: When the inbox/outbox is full, forward the new SMS to the administrator via email. To ensure email sending, please configure the Mail Server.

■ Mail Server

In this section, you can configure mail-related parameters. The SMS Inbox/Outbox Policy module will use the configuration information to send emails.

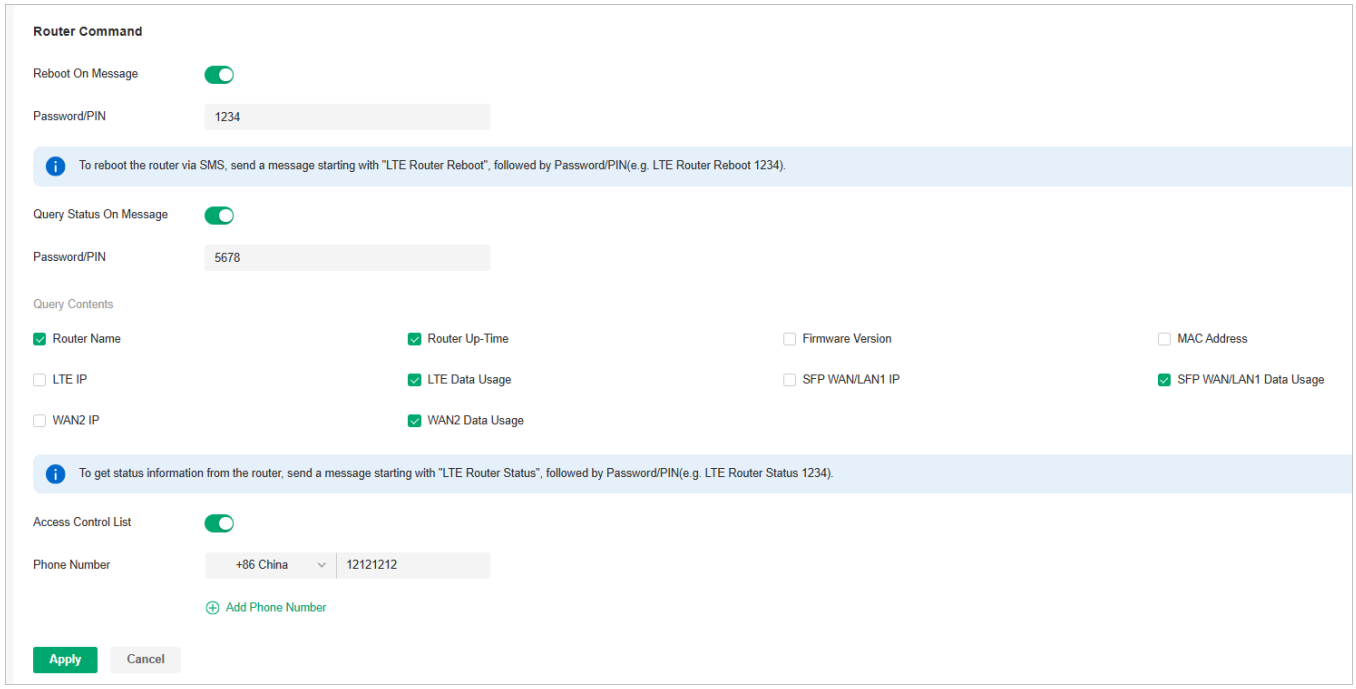


FROM	Enter the email address of the sender.
TO	Enter the email address of the receiver, which can be the same as or different from the sender's email address.
SMTP Server	Enter the domain name or IP address of the SMTP server.
SSL	When enabled, the data will be transmitted based on the SSL protocol.
SMTP Port	Enter the port used by the SMTP server according to the instructions of your email service provider.

Authentication	If the login of the mailbox requires a username and authorization code, enable this option and configure the following parameters: User Name: Enter your email address as the username. Authorization Code: Enter the authorization code that enables a third party to log into the mailbox according to the instructions of your email service provider. Note that the authorization code is not the mailbox's password.

■ Router Command

In this section, you can send specific commands via SMS to interact with the router, and only specific users are allowed to perform these interactions.



Reboot On Message	This feature is used to reboot the router via SMS. Enable this feature and enter the router's Password/PIN. Then you can send a message starting with "LTE Router Reboot", followed by the router's Password/PIN (e.g. LTE Router Reboot 1234) to reboot the router.
Query Status On Message	This feature is used to get status information from the router via SMS. Enable this feature, enter the router's Password/PIN, and choose the query contents. Then you can send a message starting with "LTE Router Status", followed by the router's Password/PIN (e.g. LTE Router Status 1234) to get status information from the router.
Access Control List	This feature is used to configure the allow phone number list of the above functions. Enable this feature, select the international telephone area code, and enter the phone number. You can add one or more phone numbers, and only these phone numbers can interact with the router via SMS.

4. 11 CLI Configuration

CLI configuration is essentially to configure devices via command lines. It is a supplementary means of GUI configuration. CLI configuration may conflict with GUI configuration.

The Controller supports two types of CLI configuration: Site CLI and Device CLI.

- **Site CLI**

  Site CLI supports batch configuration of devices that support CLI configuration on the site.

- **Device CLI**

  Device CLI supports batch configuration of selected devices.

Currently, CLI configuration only supports switches. Please refer to CLI Reference Guide to understand the CLI commands of TP-Link switches.

If you need to use CLI configuration, please read the precautions and User Guide carefully. You can contact TP-Link technical support if necessary.

After applying the CLI configuration, you can go to **Devices** > **Application Result** to view the configuration results.

General Precautions

1. The GUI and CLI configuration should be planned globally according to the actual network topology and requirements.
2. To avoid conflicts, it is recommended not to use the CLI to configure the existing functions of the GUI.
   a. When adopting a new device, the Controller will apply configurations to the device in the order of GUI, Site CLI, and then Device CLI. If there is a configuration conflict, the configuration applied last takes effect.
   b. CLI profiles (including Site CLI profiles and Device CLI profiles) will only be sent to devices once after applied, unless the "Apply Again" button in the Application Result is clicked to trigger the full configurations application.
   c. When a device upgrades its firmware, the Controller will apply the full configurations to the device in the order of GUI, Site CLI, and then Device CLI.
   d. Since the configurations applied later will overwrite the previous configurations, the configuration results of different devices may be different after the same function has been modified repeatedly via GUI, Site CLI and Device CLI.
3. The Controller will not verify the existing GUI and CLI configurations of devices. Be sure to check the existing configurations before performing new configurations. Otherwise, unexpected results may occur after the configurations are applied, and the devices may even go offline.
4. To avoid configuration conflicts, if you really need to use the CLI to configure a certain function, it is recommended not to configure it via GUI at the same time.

5. To avoid disconnection of devices from the Controller due to configuration errors or conflicts, it is recommended to configure VLAN, VLAN Interface, IP Address, ACL, etc. via GUI, and avoid modifying related configurations via CLI.

Repeated Configurations

When the same function is configured via CLI multiple times, the previous configuration may be overwritten, and the last configuration shall prevail.

a. It is recommended to confirm the currently effective commands via the CLI configuration viewing function "Show Running Config".

b. If you need to cancel a certain configuration, use the "no" command.

c. If you need to modify a certain configuration, you can enter a new command to overwrite the configuration.

d. Apply the final configuration, and confirm that the function is configured correctly and takes effect via the CLI configuration viewing function.

Execution Failures

If a CLI command fails to be executed, an error will be reported and subsequent commands will be executed. You can view the error details via the error message, and the commands that have been successfully executed before will not be undone. It is recommended to follow the steps below:

a. Use the CLI configuration viewing function (Show Running Config) to confirm the commands that have taken effect. If you need to cancel them, you can enter "no" commands and apply them to devices.

b. Troubleshoot and correct the command error, regenerate the CLI configuration, and apply it to devices.

Command Modification

If you need to modify the commands issued via CLI, please follow the steps below:

a. Use the CLI configuration view function (Show Running Config) to confirm the commands that have taken effect, and sort out the commands that need to be canceled.

b. Enter "no" commands to cancel the configurations, and apply them to devices.

Prohibited Commands

1. CLI commands such as modifying user name and password, managing VLAN, SDM profile, reboot, reset, upgrade, import and export configurations have been prohibited. When using other CLI commands, please also pay attention to avoid affecting the management of the Controller.
2. Device CLI supports the variable function. The variable content does not have too many restrictions, for example, you can enter CLI commands, but it is not recommended to use it in this way.

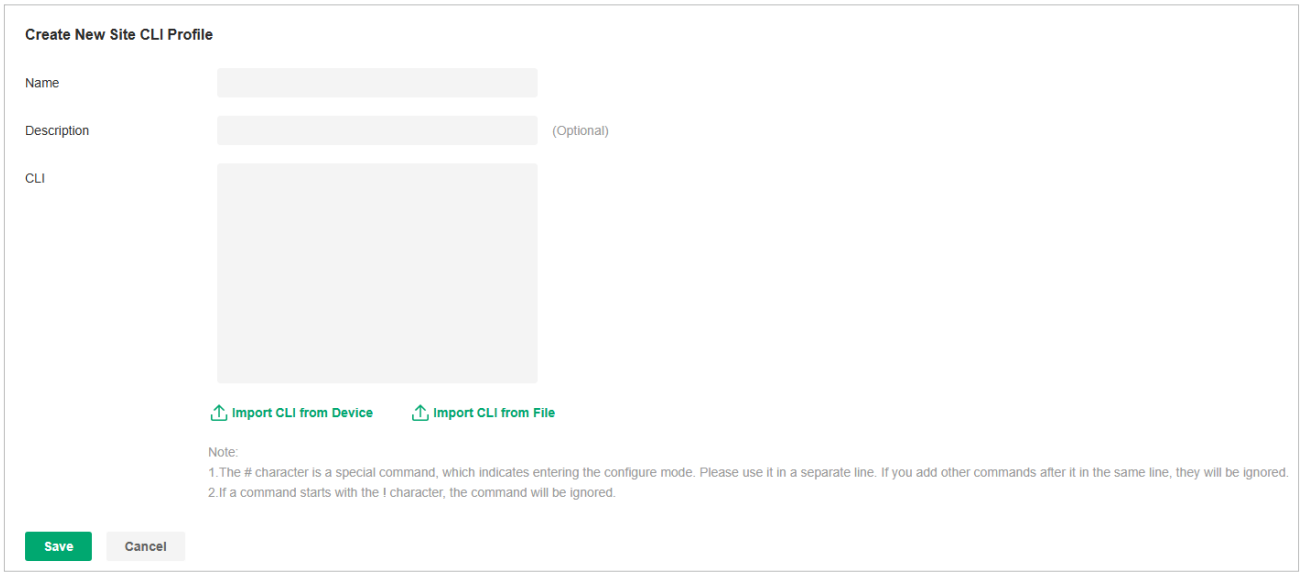
4. 11. 1 Site CLI

Overview

Site CLI enables batch configurations of all devices that support CLI configuration on the site via command lines.

Configuration

1. Go to Settings > CLI Configuration > Site CLI.
2. Click Create New Site CLI Profile and create a CLI profile according to your needs.



Note:

- The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.
- If a command starts with the ! character, the command will be ignored.

Name	Specify the name of the CLI profile.
Description	(Optional) Enter a description for identification.
CLI	Enter the command lines manually.
Import CLI from Device	Click and select a device that supports CLI configuration to import its running config.
Import CLI from File	Click and select an existing command file to import command lines.

3. Click Save to add the profile. The new profile is in inactive state and will not be applied to devices.



4. Click Apply to apply the CLI. The profile will change to active state and apply configurations to all devices that support CLI configuration on the site.

Note:

Once the profile becomes active, you will be unable to edit it.

To check whether the profile is successfully applied to devices and takes effect, click View CLI Details to view the configuration results on the Devices > Application Result page.

Note:

Deleting a CLI profile will not take effect on existing configurations on devices. To delete the configurations, use the "no" command.

4. 11. 2 Device CLI

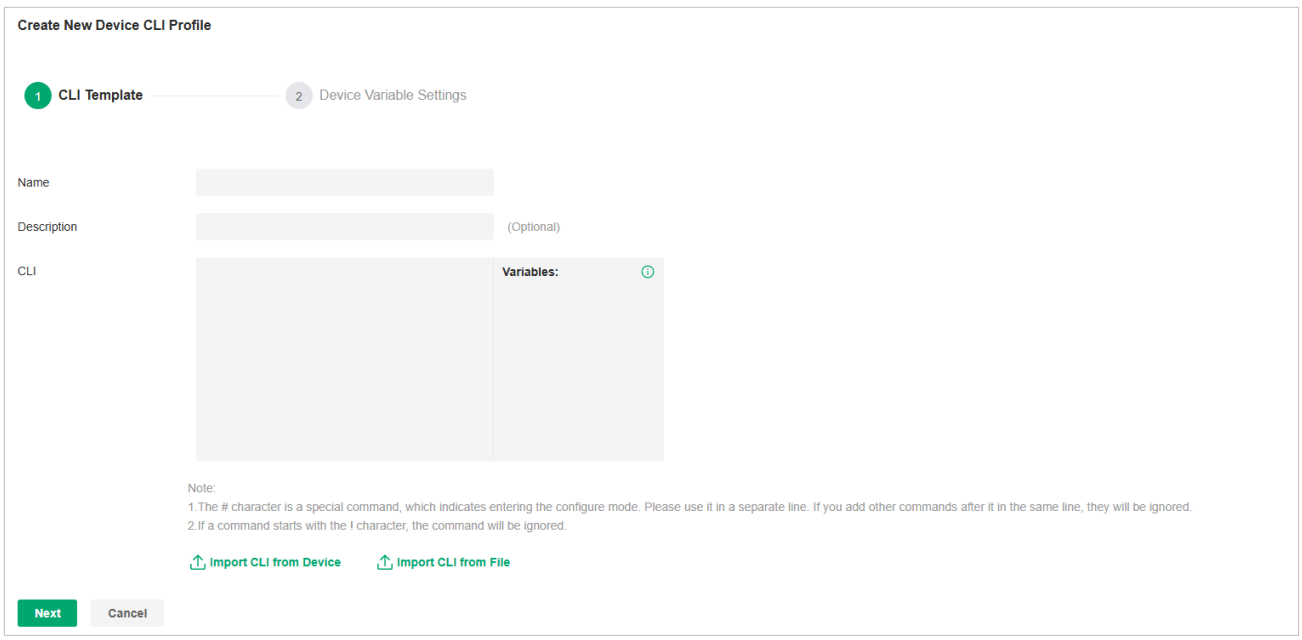
Overview

Device CLI enables batch configuration of specific devices via command lines.

Device CLI supports variables. You can use the %x% format to define a variable x, and then set different values for different switches. When the Controller applies the Device CLI configuration to switches, it will automatically modify the variable %x% to the values you set.

Configuration

1. Go to Settings > CLI Configuration > Device CLI. Click Create New Device CLI Profile and create a CLI profile according to your needs.

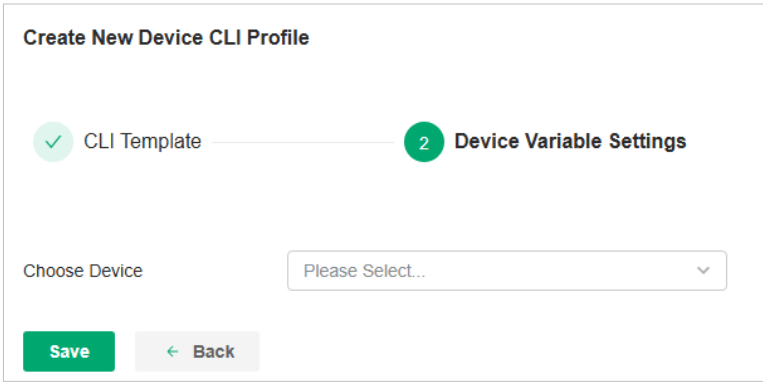


Note:

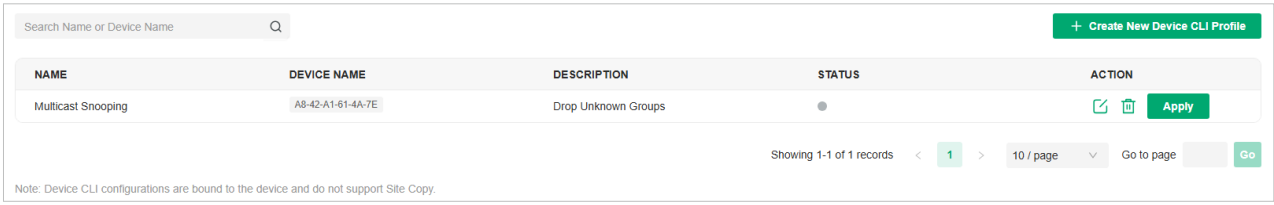
- The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.
- If a command starts with the ! character, the command will be ignored.

Name	Specify the name of the CLI profile.
Description	(Optional) Enter a description for identification.
CLI	Enter the command lines manually. You can enter %xxx% in the CLI template to define variables.
Import CLI from Device	Click and select a device that supports CLI configuration to import its running config.
Import CLI from File	Click and select an existing command file to import command lines.

2. Click Next. Select the devices to apply the CLI profile.



3. Click Save to add the profile. The new profile is in inactive state and will not be applied to devices.



4. Click Apply to apply the CLI. The profile will change to active state and apply configurations to the devices you selected.

Note:

Once the profile becomes active, you will be unable to edit it.

To check whether the profile is successfully applied to devices and takes effect, click View CLI Details to view the configuration results on the Devices > Application Result page.

Note:

Deleting a CLI profile will not take effect on existing configurations on devices. To delete the configurations, use the "no" command.

Chapter 5

Configure the SDN Controller

Controller Settings control the appearance and behavior of the controller and provide methods of data backup, restore and migration:

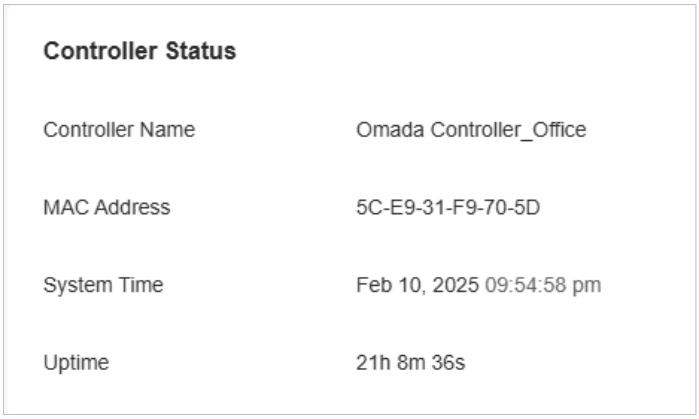
- 5. 1 System Settings
- 5. 2 Controller Settings
- 5. 3 UI Interaction
- 5. 4 History Data Retention
- 5. 5 Server Settings
- 5. 6 Account Security
- 5. 7 Maintenance
- 5. 8 Migration
- 5. 9 Export Data
- 5. 10 Cloud Access

5. 1 System Settings

Launch the controller and access the Global View. Go to Settings > System Settings.

5. 1. 1 Controller Status

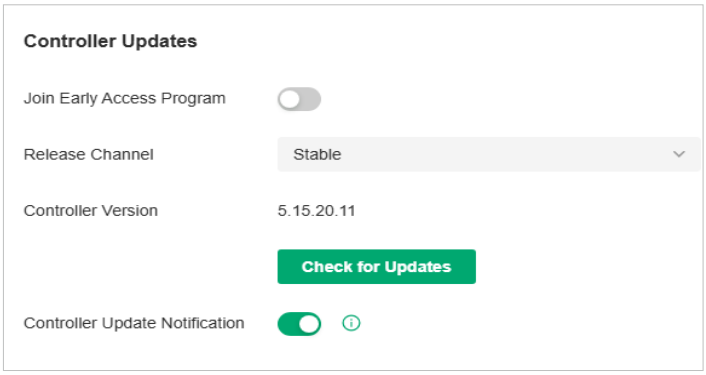
In Controller Status, you can view the controller-related information and status.



Controller Name	Displays the controller name, which identifies the controller. You can specify the controller name in 5. 2. 1 General Settings.
MAC Address	Displays the MAC address of the controller.
System Time	Displays the system time of the controller. The system time is based on the time zone which you configure in 5. 2. 1 General Settings.
Uptime	Displays how long the controller has been working.

5. 1. 2 Controller Updates

In Controller Updates, you can view the controller version information and check for updates.



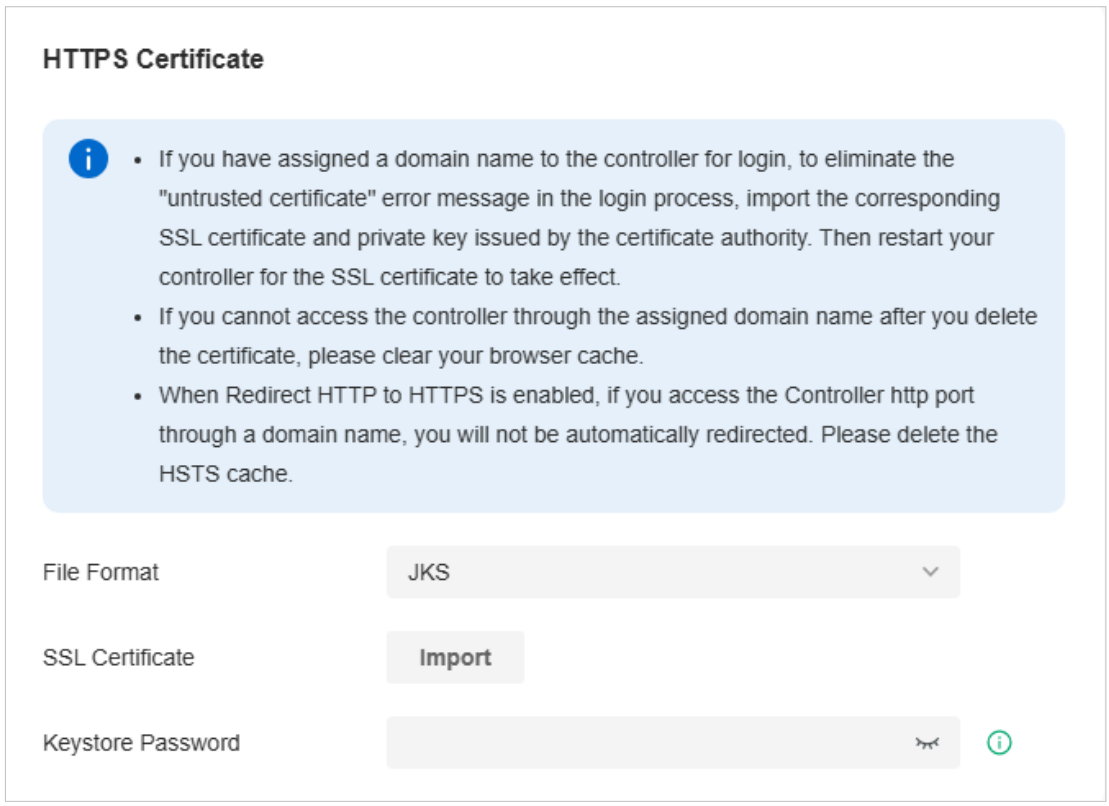
Join Early Access Program	Enable the option to join the program and check for firmware in the Release Channel > Beta for upgrading, so you can try out in-development features and help improve them.
Release Channel	Select the Release Channel of the controller to check whether the corresponding Channel has a newer version.
Controller Version	Displays the software version of the controller.
Check for Updates	Click to check for any updates of the controller.
Controller Update Notification	Enable the option and the system will query the cloud for controller firmware updates.

5. 1. 3 HTTPS Certificate

If you have assigned a domain name to the controller for login, to eliminate the “untrusted certificate” error message in the login process, import the corresponding SSL certificate and private key issued by the certificate authority in HTTPS Certificate.

Note:

- HTTPS Certificate configuration is only available for the Software Controller and Hardware Controller.
- You need to restart you controller for the imported SSL certificate to take effect.



File Format	Select the format of your certificate, and import the certificate file.
SSL Certificate	Import the SSL certificate to create an encrypted link between the controller and server. JKS: Import your SSL certificate and enter the Keystore Password if your SSL certificate has the password. Otherwise, leave it blank. PFX: Import your SSL certificate and enter the Private Key Password if your SSL certificate has the password. Otherwise, leave it blank. PEM: Import your SSL certificate and SSL Key.

Note:

For the PEM-formatted certificate:

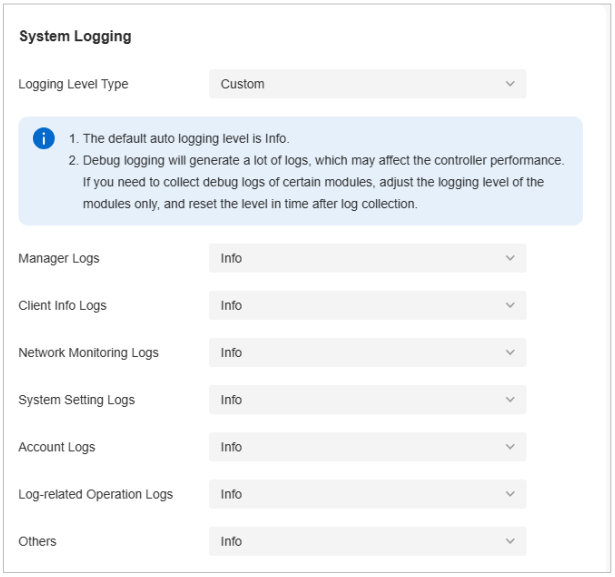
- Starts with: -----BEGIN CERTIFICATE-----
- Ends with: -----END CERTIFICATE-----
- Certificate chain is supported and no blank line is allowed between two certificate chains.

For the PEM-formatted key:

- RSA encryption is required.
- Starts with: -----BEGIN RSA PRIVATE KEY-----
- Ends with: -----END RSA PRIVATE KEY -----
- The key can be placed behind certificate file, and they can be imported together.

5. 1. 4 System Logging

In System Logging, you can customize the log level if needed.



Logging Level Type	Choose whether to customize the log level.

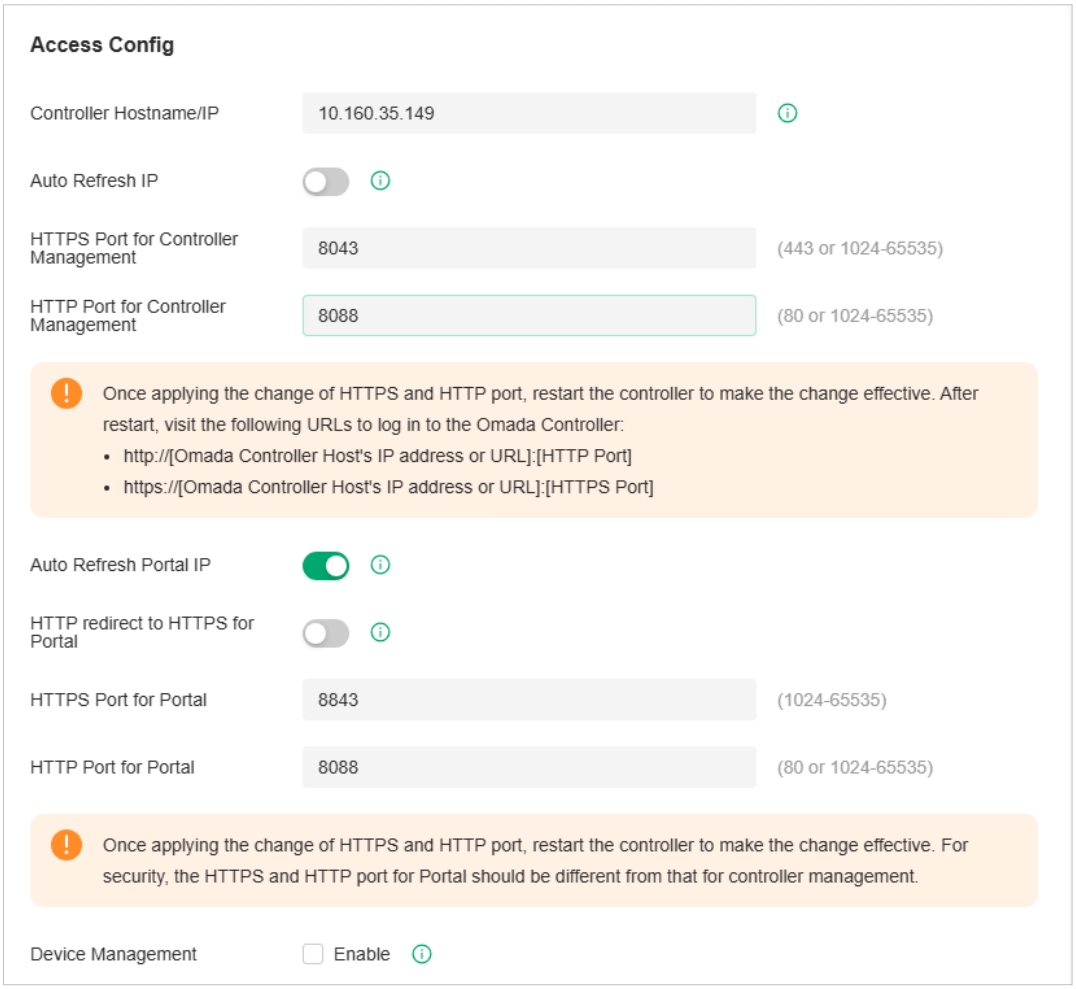
Manager Logs	Select the log level of the manager module, which mainly includes device management and site-related configurations.
Client Info Logs	Select the log level of the client info module, which mainly includes functions related to client monitoring.
Network Monitoring Logs	Select the log level of the network monitoring module, which mainly includes functions related to data monitoring.
System Setting Logs	Select the log level of the system setting module, which mainly includes system data related functions.
Account Logs	Select the log level of the account module, which mainly includes account-related functions.
Log-related Operation Logs	Select the log level of the log-related operation module, which mainly includes related functions of the log page.
Others	Select the log level of other modules.

5. 1. 5 Access Config

In Access Config, you can specify the port used by the controller for management and portal.

Note:

- Access Config is only available on the Software Controller and Hardware Controller.
- Once applying the change of HTTPS and HTTP port, restart the controller to make the change effective.
- For security, the HTTPS and HTTP port for Potal should be different from that for controller management.



Controller Hostname/IP	Enter the hostname or IP address of the controller which will be used as the Controller URL in the notification email for resetting your controller password. You can keep it default and IP address recognized by the controller will be used as the Controller URL.
Auto Refresh IP	(Only for hardware controller) Enable the feature and the hardware controller will refresh its IP address automatically.
HTTPS Port for Controller Management	Specify the HTTPS port used by the controller for management. After setting the port, you can visit https://[Controller Host's IP address or URL]:[HTTPS Port] to log in to the Controller.
HTTP Port for Controller Management	Specify the HTTP port used by the controller for management. After setting the port, you can visit https://[Controller Host's IP address or URL]:[HTTP Port] to log in to the Controller.
Auto Refresh Portal IP	When enabled, the device will automatically use the actual IP address of the Controller as the portal redirection destination. When disabled, you need to enter a domain name or IP address that clients can access.
HTTP redirect to HTTPS for Portal	If enabled, clients will be redirected to Captive Portal using HTTPS instead of HTTP.

HTTPS Port for Portal	Specify the HTTPS port used by the controller for Portal.
HTTP Port for Portal	Specify the HTTP port used by the controller for Portal.
Device Management	When enabled, the controller will apply the Device Management Hostname/IP you specified to managed devices for remote management.

5. 2 Controller Settings

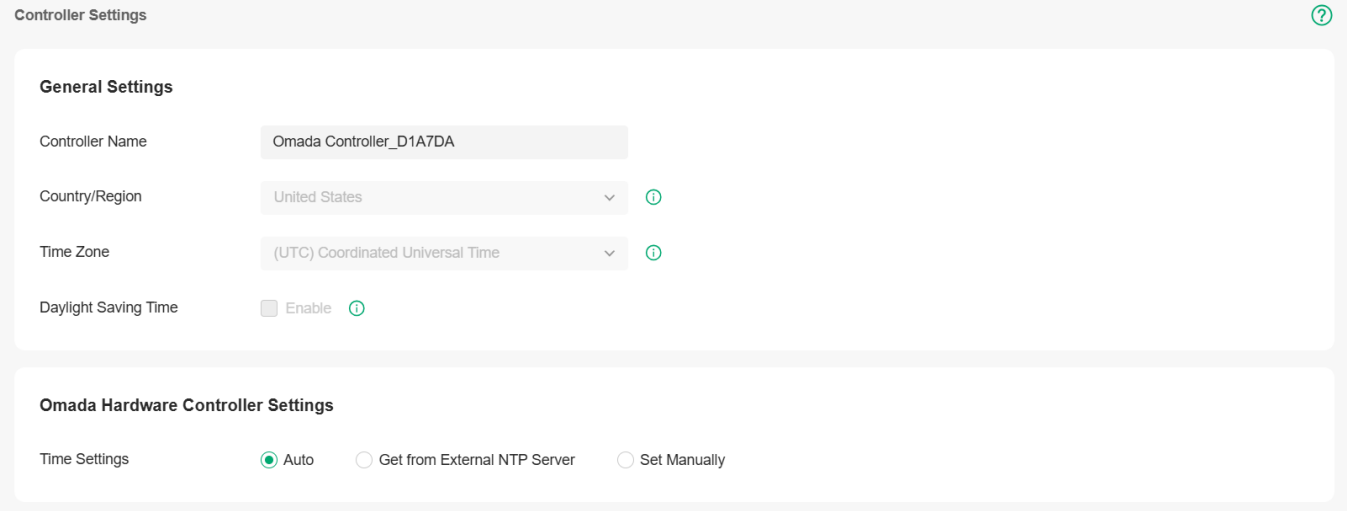
Launch the controller and access the Global View. Go to Settings > Controller Settings.

5. 2. 1 General Settings

In General Settings, you can configure general settings of the controller.

■ For Hardware Controller and Integrated Gateway (Controller)

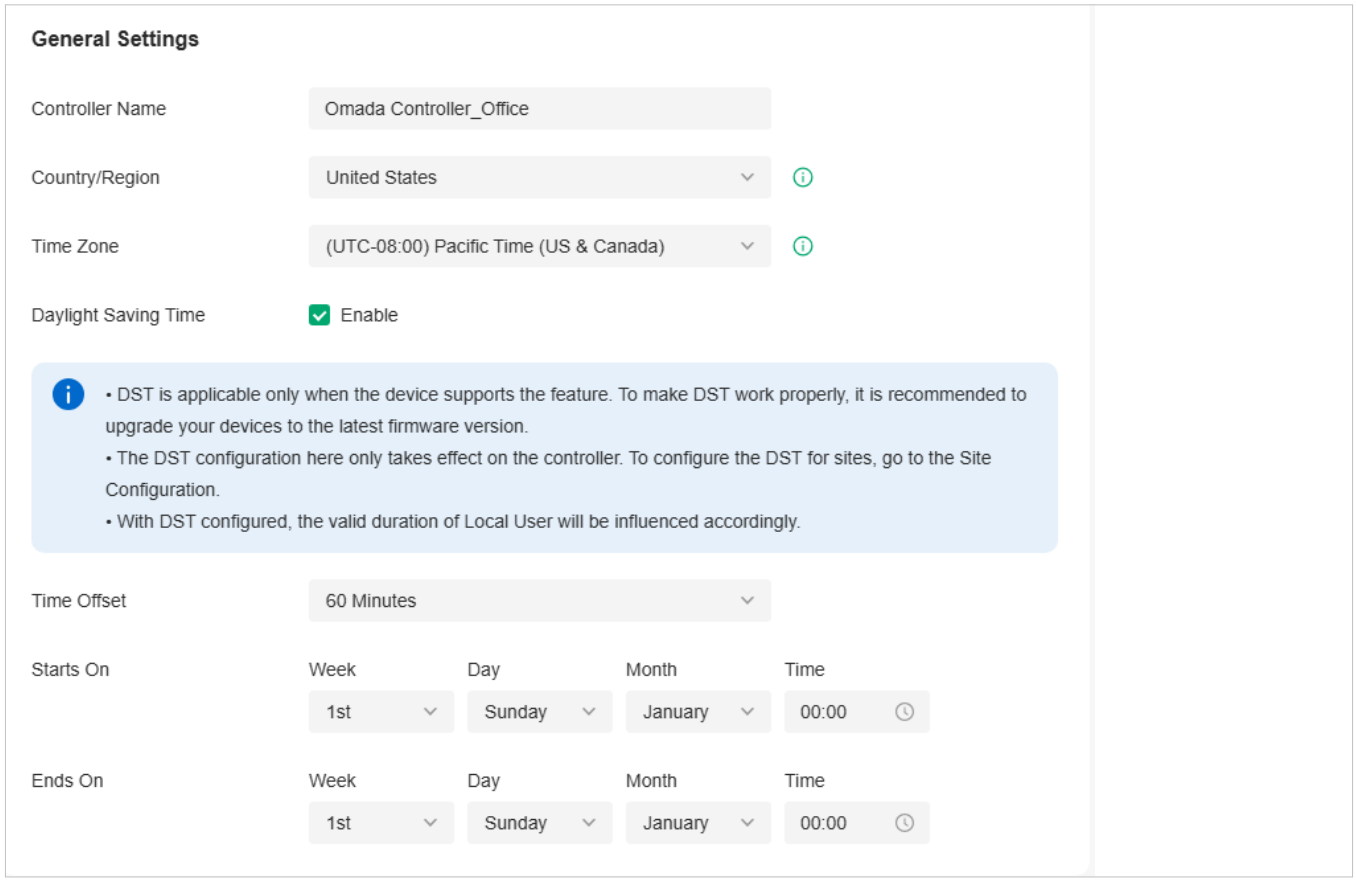
Note: The Country/Region, Time Zone, and Daylight Saving Time settings are the same as those of the default site.



Controller Name	Specify the Controller Name to identify the controller.
Country/Region	Select the location of the controller. The configuration here only takes effect on the controller. To configure the Country/Region for sites, go to the Site Configuration.
Time Zone	Select the Time Zone of the controller according to your region. For controller settings and statistics, time is displayed based on the Time Zone. The configuration here only takes effect on the controller. To configure the Time Zone for sites, go to the Site Configuration.
Time Settings	Choose a method to set the system time. Auto: Get the time automatically from the built-in NTP server. Get from External NTP Server: Specify one or multiple NTP servers to get time from. The NTP server will be applied to all APs under the site. The controller will first use the specified external NTP server to get time; if that fails, it will then use the built-in NTP server. Set Manually: Set the system time manually.
Primary NTP Server/ Secondary NTP Server	Enter the IP address of the primary and secondary NTP (Network Time Protocol) server. NTP servers assign network time to the controller.

Daylight Saving Time	Enable the feature if your country/region implements DST. When it is enabled, the DST icon will appear on the upper right, showing the DST settings and status.
Time Offset	Select the time added in minutes when Daylight Saving Time starts.
Starts On	Specify the time when the DST starts. The clock will be set forward by the time offset you specify.
Ends On	Specify the time when the DST ends.The clock will be set back by the time offset you specify.

For Software Controller / Cloud-Based Controller

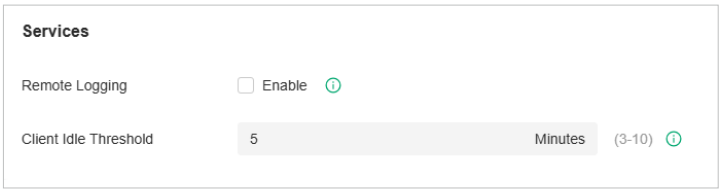


Controller Name	Specify the Controller Name to identify the controller.
Country/Region	Select the location of the controller. The configuration here only takes effect on the controller. To configure the Country/Region for sites, go to the Site Configuration.

Time Zone	Select the Time Zone of the controller according to your region. For controller settings and statistics, time is displayed based on the Time Zone. The configuration here only takes effect on the controller. To configure the Time Zone for sites, go to the Site Configuration.
Daylight Saving Time	Enable the feature if your country/region implements DST.
Time Offset	Select the time added in minutes when Daylight Saving Time starts.
Starts On	Specify the time when the DST starts. The clock will be set forward by the time offset you specify.
Ends On	Specify the time when the DST ends.The clock will be set back by the time offset you specify.

5. 2. 2 Services

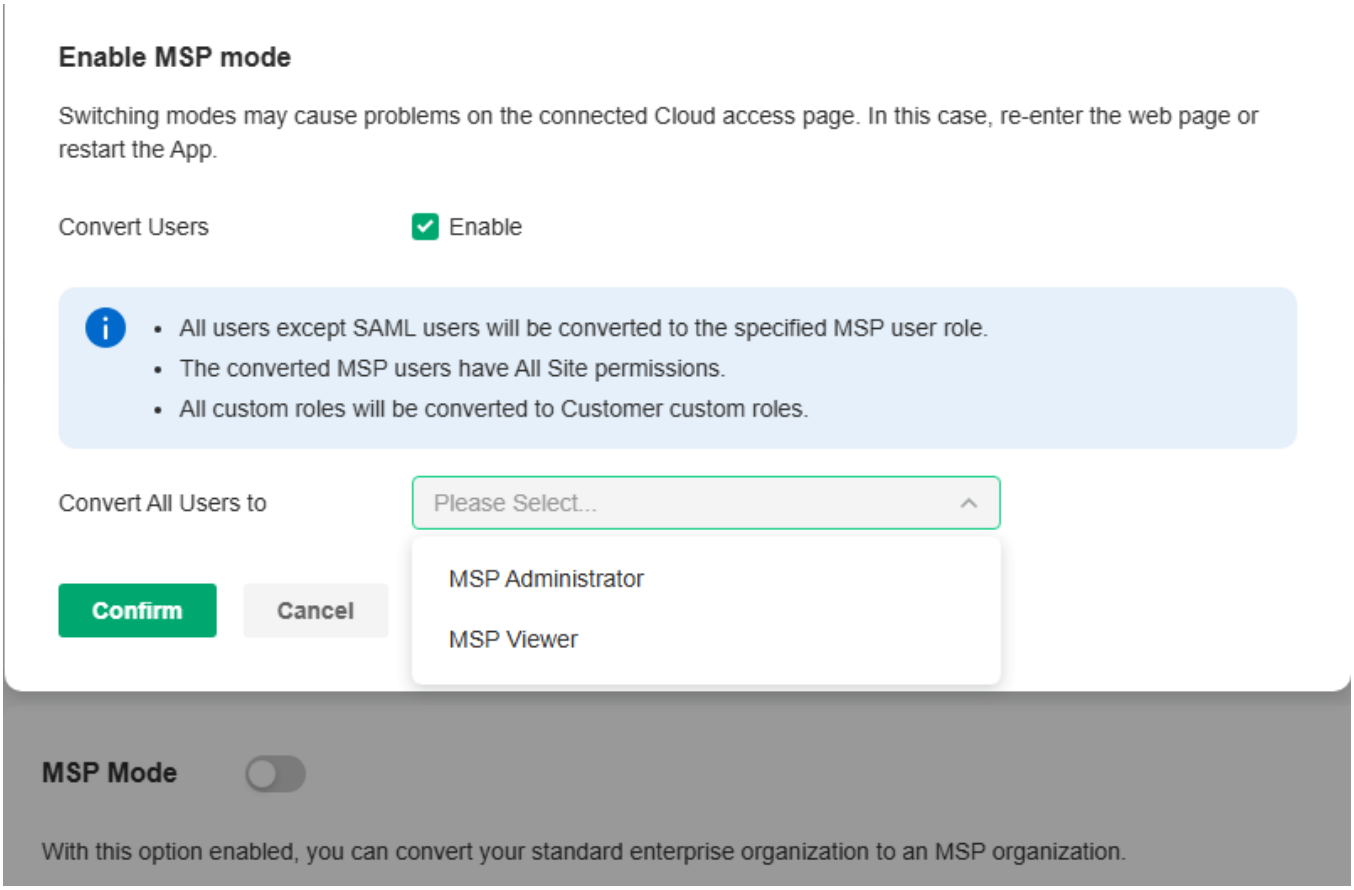
In Services, you can configure remote logging and client idle threshold.



Remote Logging	With this feature configured, Omada Controller will send the system log to the log server once it is generated. When enabled, you need to specify the Syslog Server IP/Hostname and Syslog Server Port.
Client Idle Threshold	The controller will consider a client offline (thus disconnect it) when it is idle for longer than the specified threshold. If the specified threshold is too short, clients may be disconnected frequently.

5. 2. 3 MSP Mode

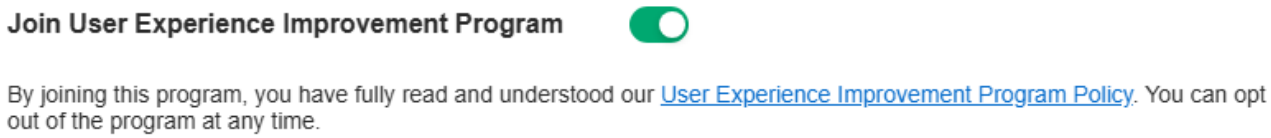
In MSP Mode, you can convert your standard enterprise organization to an MSP organization. For more settings in MSP mode, refer to 10 Manage Customer Networks in MSP Mode.



Convert Users	When enabled, all users except SAML users will be converted to the specified MSP user role. The converted MSP users have All Site permissions. All custom roles will be converted to Customer custom roles.
Convert All Users to	Select to convert all users to MSP Administrator or MSP Viewer.

5. 2. 4 Join User Experience Improvement Programm

You can participate in the user experience improvement program and help improve the quality and performance of TP-Link products by sending statistics and usage information.

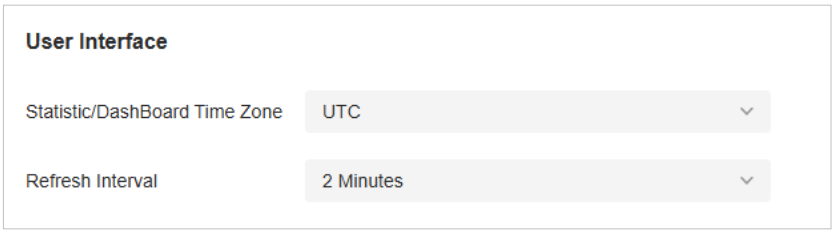


5. 3 UI Interaction

Launch the controller and access the Global View. Go to Settings > UI Interaction.

5. 3. 1 User Interface

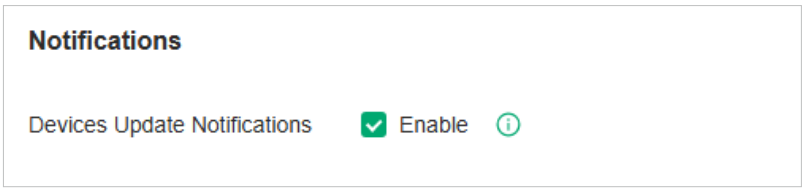
In User Interface, you can customize the User Interface settings of the controller according to your preferences.



Statistic/Dashboard Timezone	Select which Timezone the time of statistics and the dashboard is based on. Site's: Site's Timezone is set in Site Configuration of the corresponding site. Browser's: Browser's Timezone is synchronized with the browser configuration. Controller's: Controller's Timezone is set in General Settings of the controller. UTC: UTC (Coordinated Universal Time) is the common time standard across the world.
Refresh Interval	Select how often the controller automatically refreshes the data displayed on the page.

5. 3. 2 Notifications

In Notifications, you can enable the Devices Update Notification feature to receive an update notification when a new firmware version for your device is available..

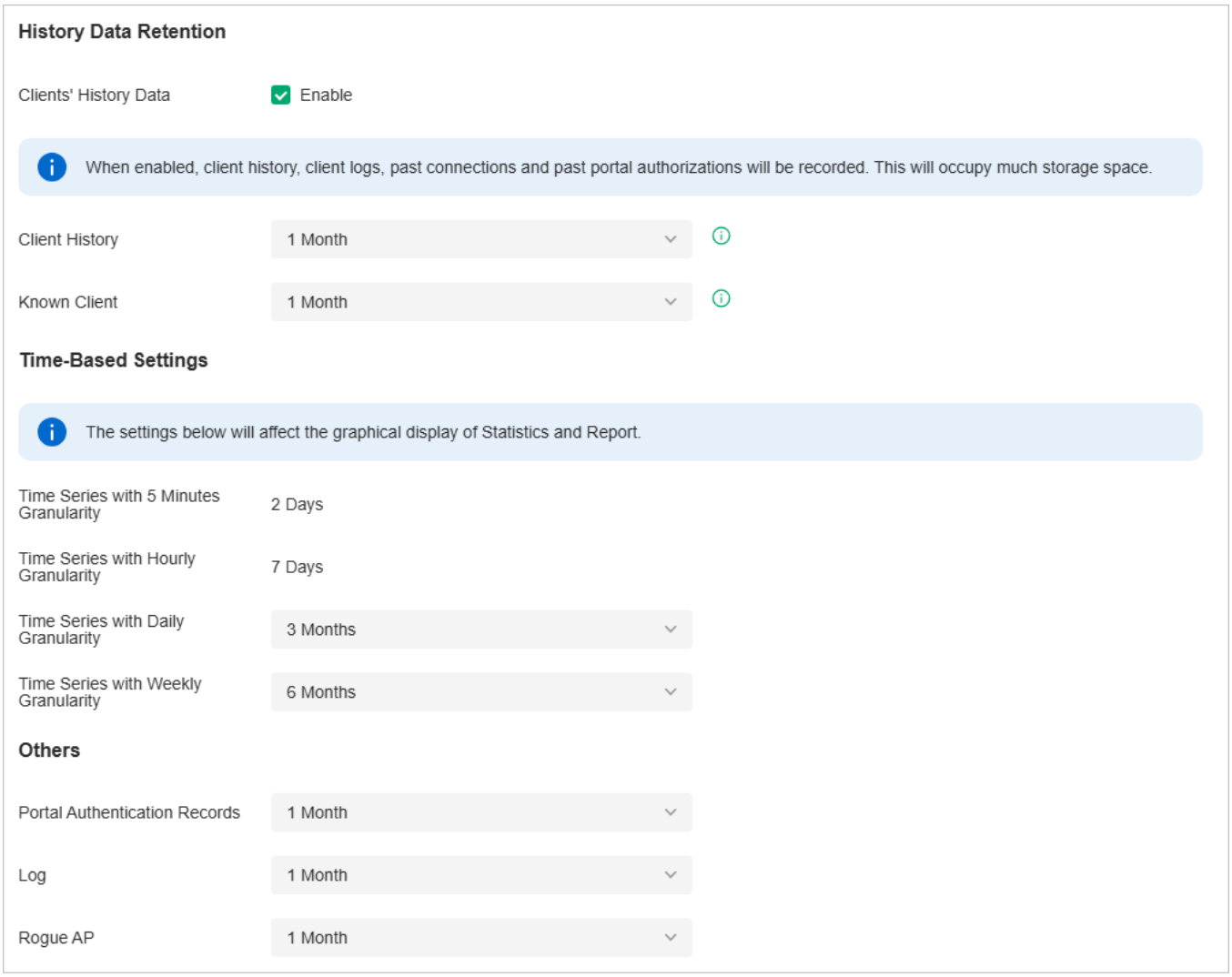


Devices Update Notification	With this feature enabled, you will receive an update notification when a new firmware version for your device is available.

5. 4 History Data Retention

In History Data Retention, you can specify how the controller retains its data.

Launch the controller and access the Global View. Go to Settings > History Data Retention.



Clients' History Data	When enabled, known clients, client history and client logs will be recorded. This will occupy much storage space.
Client History	Specify the retention time of client online and offline records. Corresponding to Insight-Past Connection.
Known Client	Specify the retention time of known client data. Corresponding to Insight-Known Clients.
Time Series with 5 Minutes Granularity	Displays the retention time of AP, switch, gateway, and client data. Corresponding to 5-minute statistics.
Time Series with Hourly Granularity	Displays the retention time of AP, switch, gateway, and client data. Corresponding to hourly statistics.
Time Series with Daily Granularity	Specify the retention time of AP, switch, gateway, and client data. Corresponding to daily statistics.

Time Series with Weekly Granularity	Specify the retention time of client data. Corresponding to weekly statistics.
Portal Authentication Records	Specify the retention time of portal authorization records. Corresponding to Insight-Past Portal Authorization.
Log	Specify the retention time of logs.
Rogue AP	Specify the retention time of scanned Rogue APs. Corresponding to Insight-Rogue APs.

5. 5 Server Settings

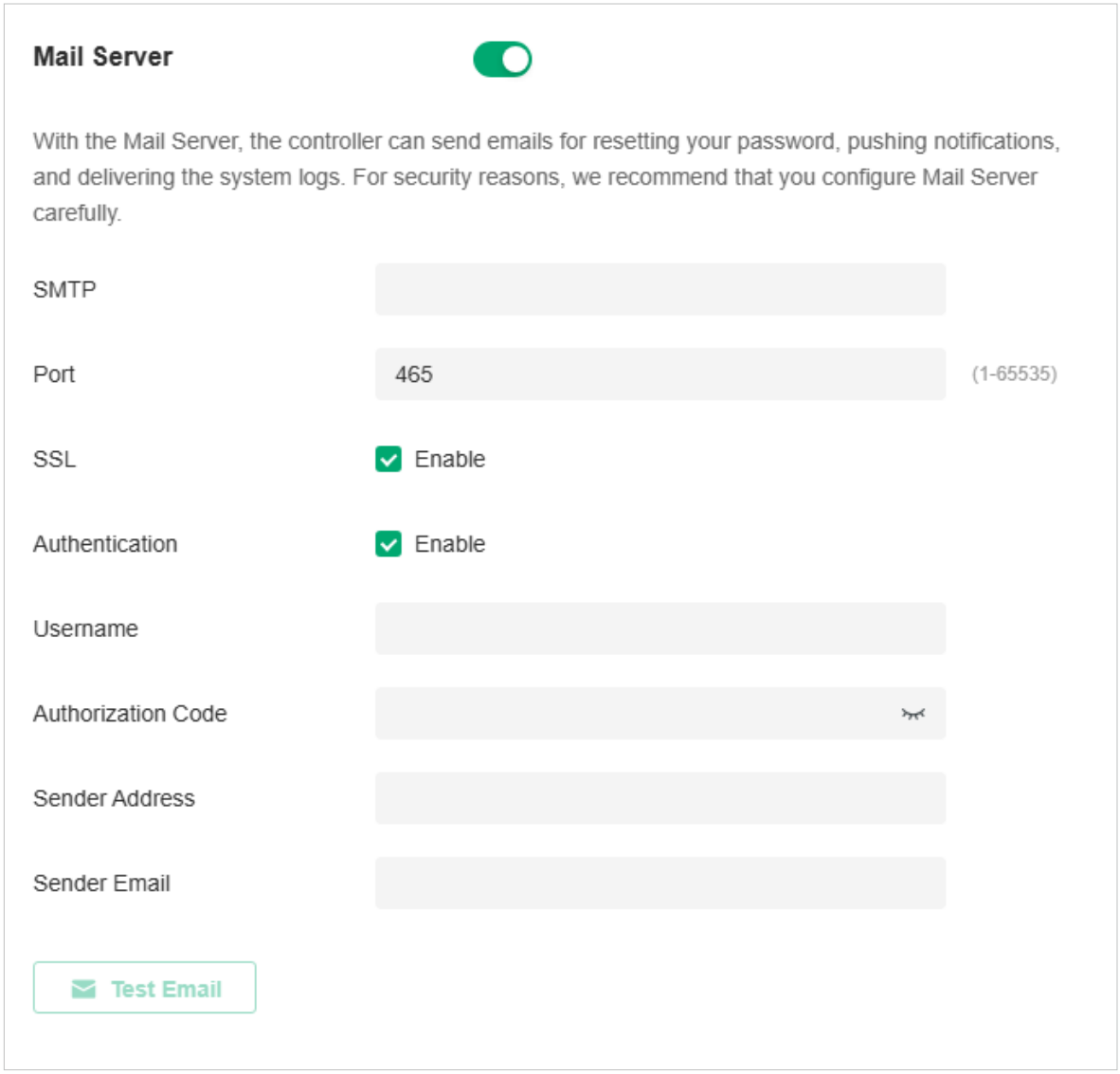
Launch the controller and access the Global View. Go to Settings > Server Settings.

5. 5. 1 Mail Server

With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. The Mail Server feature works with the SMTP (Simple Mail Transfer Protocol) service provided by an email service provider.

Configuration

1. Log in to your email account and enable the SMTP (Simple Mail Transfer Protocol) Service. For details, refer to the instructions of your email service provider.
2. Launch the controller and access the Global View. Go to Settings > Server Settings. Enable Mail Server and configure the parameters. Then apply the settings.



SMTP	Enter the URL or IP address of the SMTP server according to the instructions of the email service provider.
Port	Configure the port used by the SMTP server according to the instructions of the email service provider.
SSL	Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller and the SMTP server.
Authentication	Enable or disable Authentication according to the instructions of the email service provider. If Authentication is enabled, the SMTP server requires the username and password for authentication.
Username	When Authentication is enabled, enter your email address as the username.
Authorization Code	When Authentication is enabled, enter the authorization code as the password, which is provided by the email service provider when you enable the SMTP service.
Sender Address	(Optional) Specify the sender address of the email. If you leave it blank, the controller uses your email address as the Sender Address.
Test Emal	Test the Mail Server configuration by sending a test email to an email address that you specify.

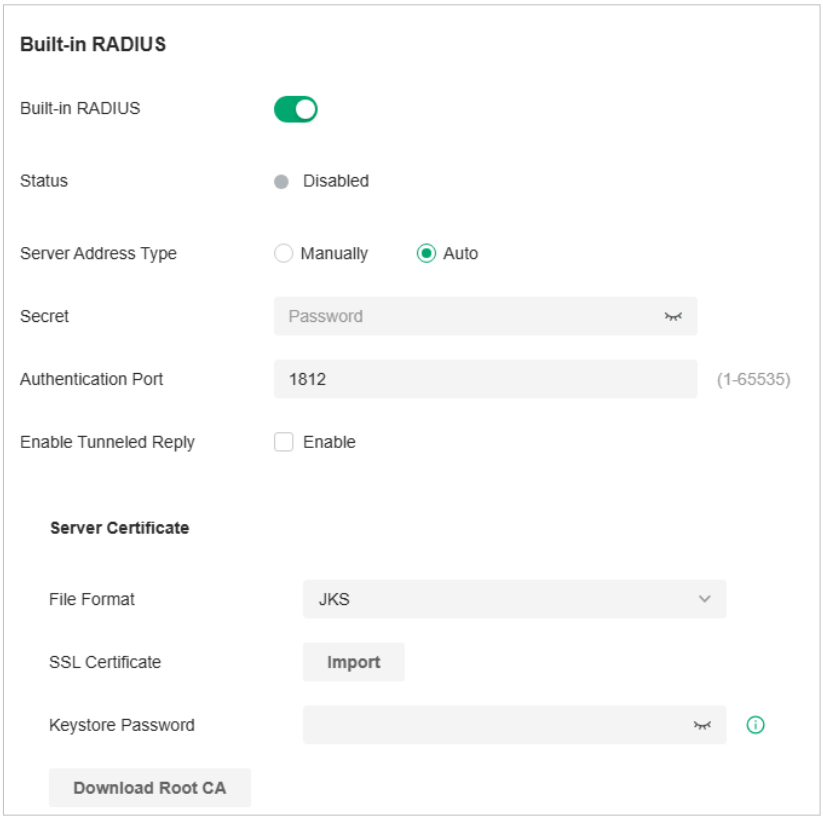
5. 5. 2 Built-in RADIUS

A RADIUS server maintains a database which stores the identity information of legal users. It authenticates users against the database when the users are requesting to access the network, and provides authorization and accounting services for them.

For the Software Controller and Hardware Controller, you can set up the built-in RADIUS server for user authentication.

Note:

Built-in RADIUS server is only available for the Software Controller and Hardware Controller.



Built-in RADIUS	Toggle on to enable the built-in RADIUS server.
Status	Displays the current status of the server.
Server Address Type	Specify the built-in server address type. When the controller is on a computer with multiple network adapters, and the type is configured as Auto, the server address will be sent to the device according to the ports connected to the device. When the type is configured as Manual, the user needs to manually configure the server's IP address, which should be the address the device can communicate with.
Secret	Specify the RADIUS server key.
Authentication Port	Specify the RADIUS server authentication port.
Enable Tunneled Reply	Enable this option if you want to allow the reply of the Tunneled Reply-related attributes to the device. Only after this option is enabled can the client be assigned a VLAN.
File Format	Select the format of your certificate, and import the certificate file.

SSL Certificate	Import the SSL certificate to create an encrypted link between the controller and server. JKS: Import your SSL certificate and enter the Keystore Password if your SSL certificate has the password. Otherwise, leave it blank. PFX: Import your SSL certificate and enter the Private Key Password if your SSL certificate has the password. Otherwise, leave it blank. PEM: Import your SSL certificate and SSL Key.
Download Root CA	Export the installable built-in authentication server root certificate. If the user uploads a certificate, the root certificate of the uploaded certificate will be exported; otherwise the default root certificate will be exported. The DNS name of the default root certificate is "Omada".

Note:

For the PEM-formatted certificate:

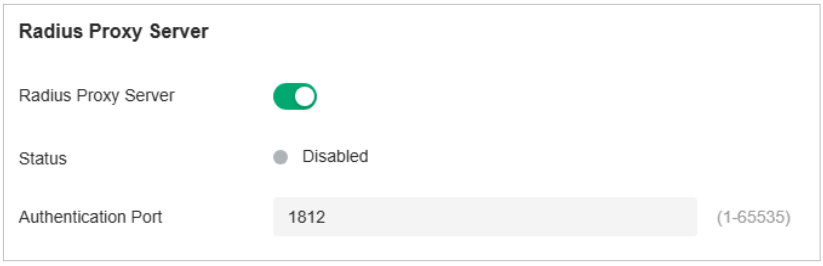
- Starts with: -----BEGIN CERTIFICATE-----
- Ends with: -----END CERTIFICATE-----
- Certificate chain is supported and no blank line is allowed between two certificate chains.

For the PEM-formatted key:

- RSA encryption is required.
- Starts with: -----BEGIN RSA PRIVATE KEY-----
- Ends with: -----END RSA PRIVATE KEY -----
- The key can be placed behind certificate file, and they can be imported together.

5. 5. 3 Radius Proxy Server

A Radius proxy authenticates and authorizes users or devices and also tracks the usage of those services. You can configure the Radius Proxy Server for user authentication.



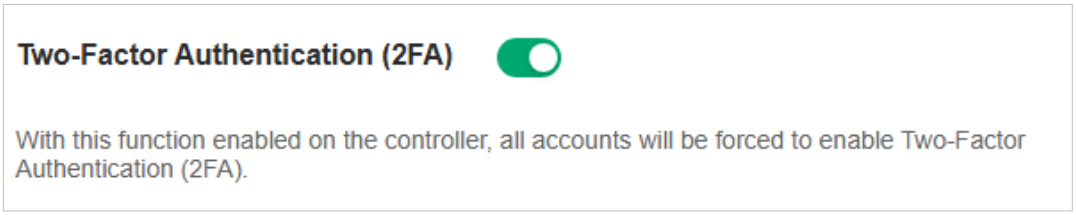
Radius Proxy Server	Toggle on to enable the Radius Proxy Server.
Status	Displays the current status of the server.
Authentication Port	Specify the port that the controller listens for to receive radius messages from devices.

5. 6 Account Security

Launch the controller and access the Global View. Go to Settings > Account Security.

5. 6. 1 Two-Factor Authentication (2FA)

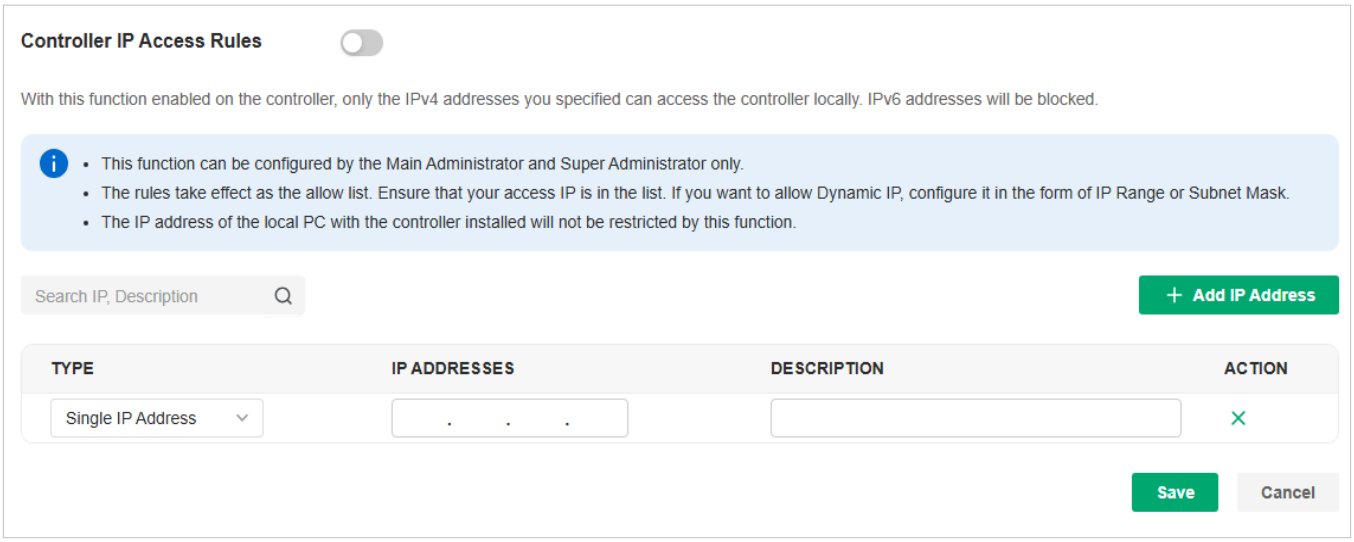
You can enable Two-Factor Authentication (2FA) to improve the security of the controller.



Two-Factor Authentication (2FA)	This function improves the security of the controller by requiring two factors of identification to access resources and data. With this function enabled, all accounts will be forced to enable 2FA upon user login. You can also enable 2FA for accounts on the Admin > User page.

5. 6. 2 Controller IP Access Rules

You can enable Controller IP Access Rules, so that only the IPv4 addresses you specified can access the controller locally. IPv6 addresses will be blocked.



Type	Specify the IP address type: Single IP Address, Single Subnet Mask, or IP Range.
IP Addresses	Specify the IP addresses that are allowed to access the controller.
Description	Enter a description for identification.

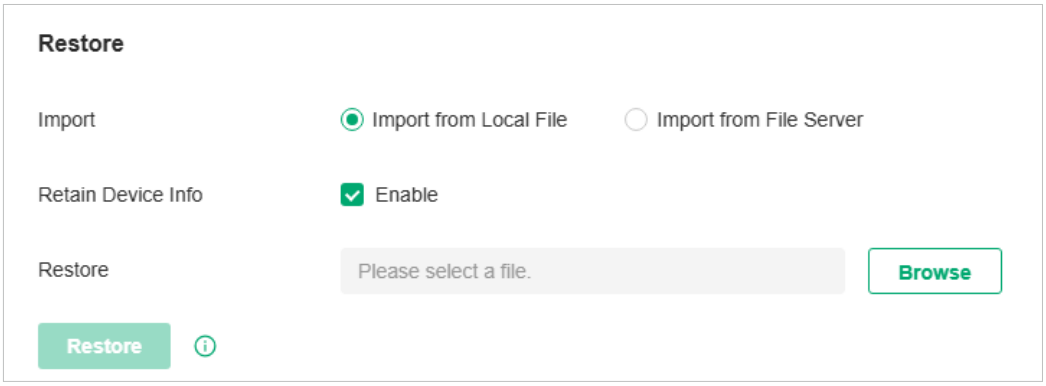
5. 7 Maintenance

You can back up the configuration and data of your controller to prevent any loss of important information.

If necessary, restore the controller to a previous status using the backup file.

5. 7. 1 Restore

Launch the controller and access the Global View. Go to Settings > Maintenance. In Restore, click Browse and select a backup file from your computer or file server. Click Restore.



Note:

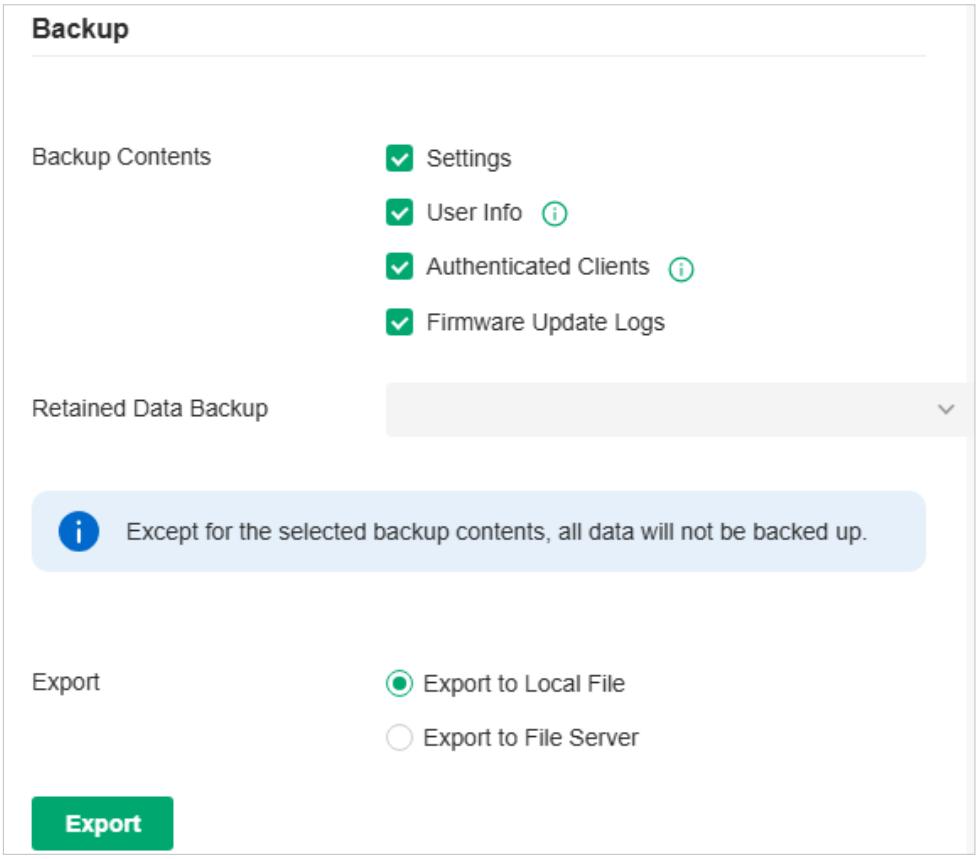
- The controller will be restored to the selected file and all current configurations will be lost.
- Only the configuration file of controller v5.0.x or above is supported.
- The current controller only supports the configuration file of the controller with the same or a smaller first-three-part version number (Major.Minor.Patch).

Import	Select where you store the restore file. Import from Local File: Import the data locally. It is not supported when accessing the controller via cloud. Import from File Server: Import the data from a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.
Retain Device Info	Select this option if you want to retain device information.
Restore	Select the backup file to restore the information.

5. 7. 2 Backup

Launch the controller and access the Global View. Go to Settings > Maintenance. In Backup, click Export to export and save the backup file.

If you want to export the data to a file server, configure the parameters accordingly and click Export.



Backup Contents	Select the data contents to back up. Settings: All the controller settings will be backed up. User Info: All local and cloud user information except for the main admin will be retained. Make sure Cloud Access is enabled on the Controller to be restored. Otherwise the Cloud account will not be retained correctly. Authenticated Clients: The authenticated client information will be backed up and can be used to verify clients for portal authentication. It is recommended to select this option if your network uses portal authentication. Firmware Update Logs: The firmware update logs will be backed up.
Retained Data Backup	Select the length of time in days that data will be backed up. 7 Days/30 Days/60 Days/90 Days/180 Days/365 Days: Back up the data in the recent days. All Time: (Only for Software Controller) Back up all data in the controller.
Export	Select where you want to export the data to. Export to Local File: Export and save the data locally. It is not supported when accessing the controller via cloud. Export to File Server: Export and save the data to a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.

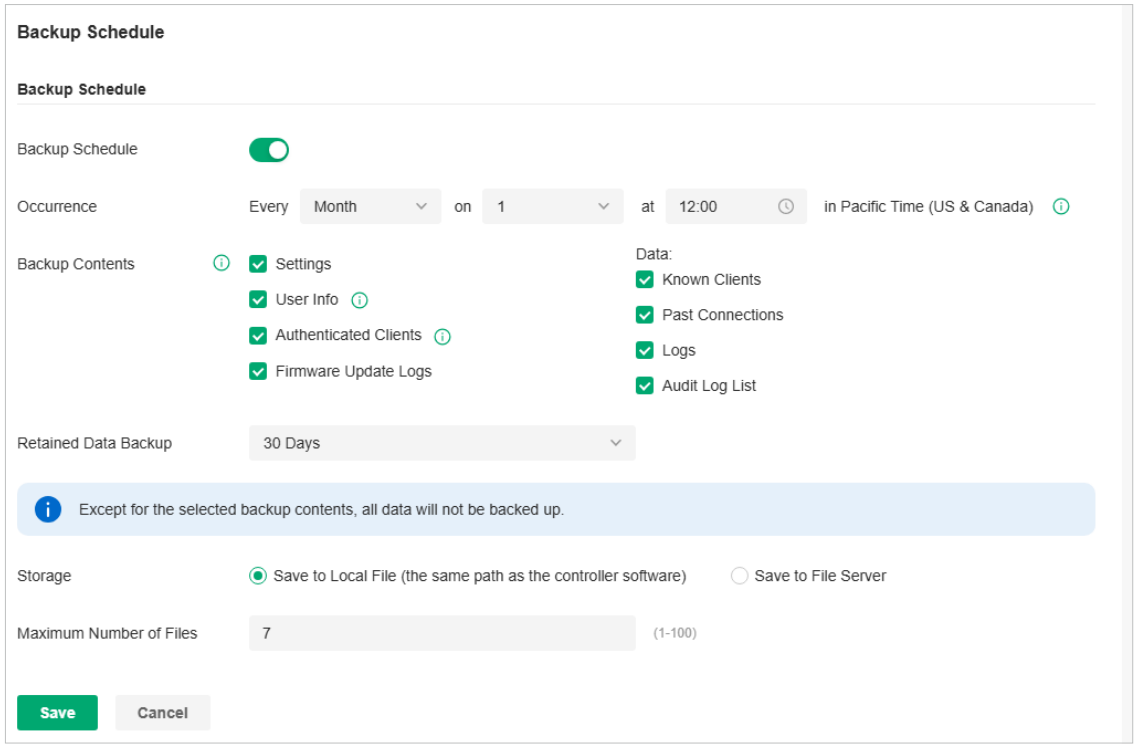
5. 7. 3 Backup Schedule

With Backup Schedule enabled, the controller will be scheduled to back up the configurations and data automatically at the specified time. You can easily restore the configurations and data when needed.

Note:

- On Omada Cloud-Based Controller, there is no need to configure Backup Schedule. It will automatically save the configurations and data on the cloud.

Launch the controller and access the Global View. Go to Settings > Maintenance. In Backup Schedule, enable Backup Schedule and configure the parameters. Click Save.

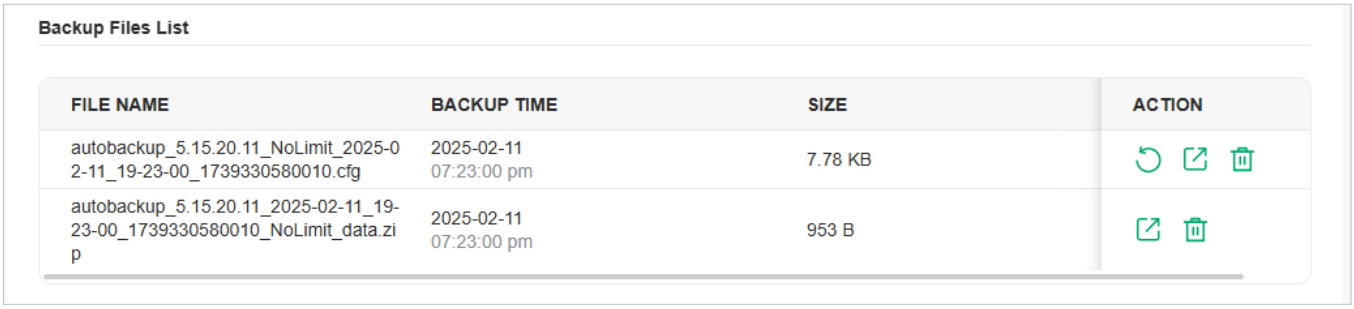


Occurrence	Specify when to perform Auto Backup regularly. Select Every Day, Week, Month, or Year first and then set a time to back up files. Note the time availability when you choose Every Month. For example, if you choose to automatically backup the data on the 31st of every month, Backup Schedule will not take effect when it comes to the month with no 31st, such as February, April, and June.

Backup Contents	Select the data contents to back up. Settings: All the controller settings will be backed up. User Info: All locPast Connectionsal and cloud user information except for the main admin will be retained. Make sure Cloud Access is enabled on the Controller to be restored. Otherwise the Cloud account will not be retained correctly. Authenticated Clients: The authenticated client information will be backed up and can be used to verify clients for portal authentication. It is recommended to select this option if your network uses portal authentication. Firmware Update Logs: The firmware update logs will be backed up. Known Clients: Back up the list of the known clients. Past Connections: Back up the list of the past connections. To export past connections data, you need to first enable Client's History Data in 5.4 History Data Retention. Logs: Back up the list of the logs. Audit Log List: Back up the list of the audit logs.
Retained Data Backup	Select the length of time in days that data will be backed up. 7 Days/30 Days/60 Days/90 Days/180 Days/365 Days: Back up the data in the recent days. All Time: (Only for Software Controller) Back up all data in the controller.
Storage	Select where you want to save the backup file. Save to Local File: The backup file will be saved as a local file. Save to File Server: The backup file will be saved in the specified file server.
Saving Path	(Only for Hardware Controller) Select a path to save the backup files.
Maximum Number of Files	(When selecting Save to Local File) Specify the maximum number of backup files to save.
Type	(When selecting Save to File Server) Specify the file server you are using. Four types of file server are available: FTP, TFTP, SFTP, and SCP.
Server Hostname/IP	(When selecting Save to File Server) Specify the Hostname/IP corresponding to the file server.
Port	(When selecting Save to File Server) Specify the port corresponding to the file server.
FTP Username	(When selecting FTP as File Server) Specify the username of the FTP file server.
FTP Password	(When selecting FTP as File Server) Specify the password of the FTP file server.

SFTP Username	(When selecting SFTP as File Server) Specify the username of the SFTP file server.
SFTP Password	(When selecting SFTP as File Server) Specify the password of the SFTP file server.
SCP Username	(When selecting SCP as File Server) Specify the username of the SCP file server.
SCP Password	(When selecting SCP as File Server) Specify the password of the SCP file server.
File Path	(When selecting Save to File Server) Specify the file path.

You can view the name, backup time and size of backup files in Backup Files List.



To restore, export or delete the backup file, click the icon in the Action column.

	Restore the configurations and data in the backup file. All current configurations will be replaced after the restoration. To keep the backup data safe, please wait until the operation is finished. This will take several minutes.
	Export the backup file. The exported file will be saved in the saving path of your web browser.
	Delete the backup file.

Note:

If the backup file is saved to file server and the type SCP / TFTP is selected, it will not included in the Backup Files List, and it cannot be exported, restored, or deleted.

5. 8 Migration

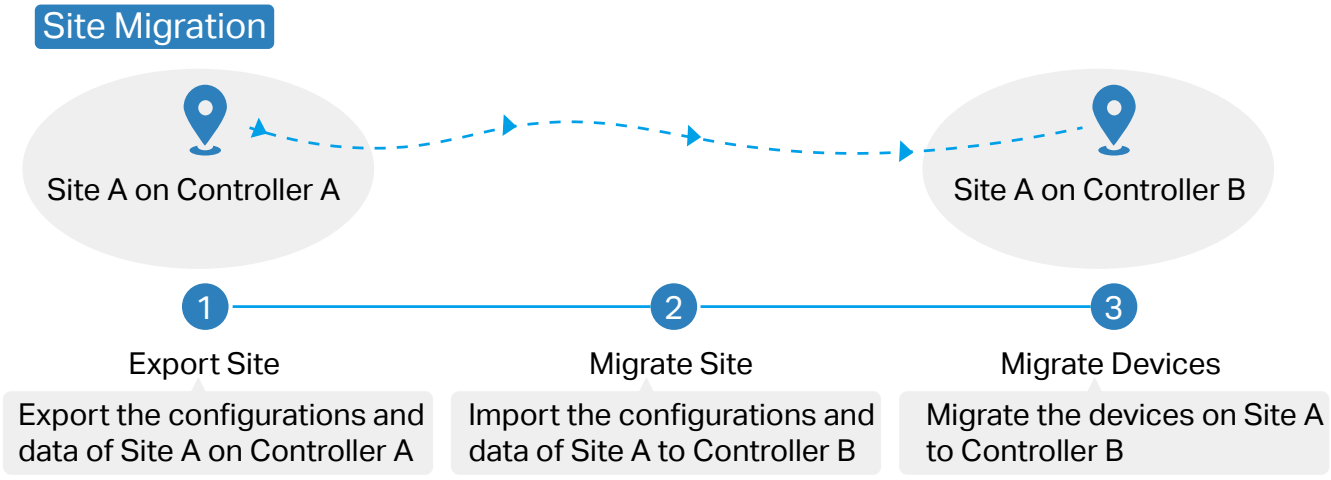
Migration services allow users to migrate the configurations and data to any other controller. Migration services include Site Migration and Controller Migration, covering all the needs to migrate both a single site and the whole controller.

5. 8. 1 Site Migration

Overview

Site Migration allows the administrators to export a site from the current controller to any other controller that has the same version. All the configurations and data of the site will be migrated to the target controller.

The process of migrating configurations and data from a site to another controller can be summarized in three steps: Export Site, Migrate Site and Migrate Devices.



Step 1: Export Site

Export the configurations and data of the site to be migrated as a backup file.

Step 2: Migrate Site

In the target controller, import the backup file of the original site.

Step 3: Migrate Devices

Migrate the devices which are on the original site to the target controller.

Configuration

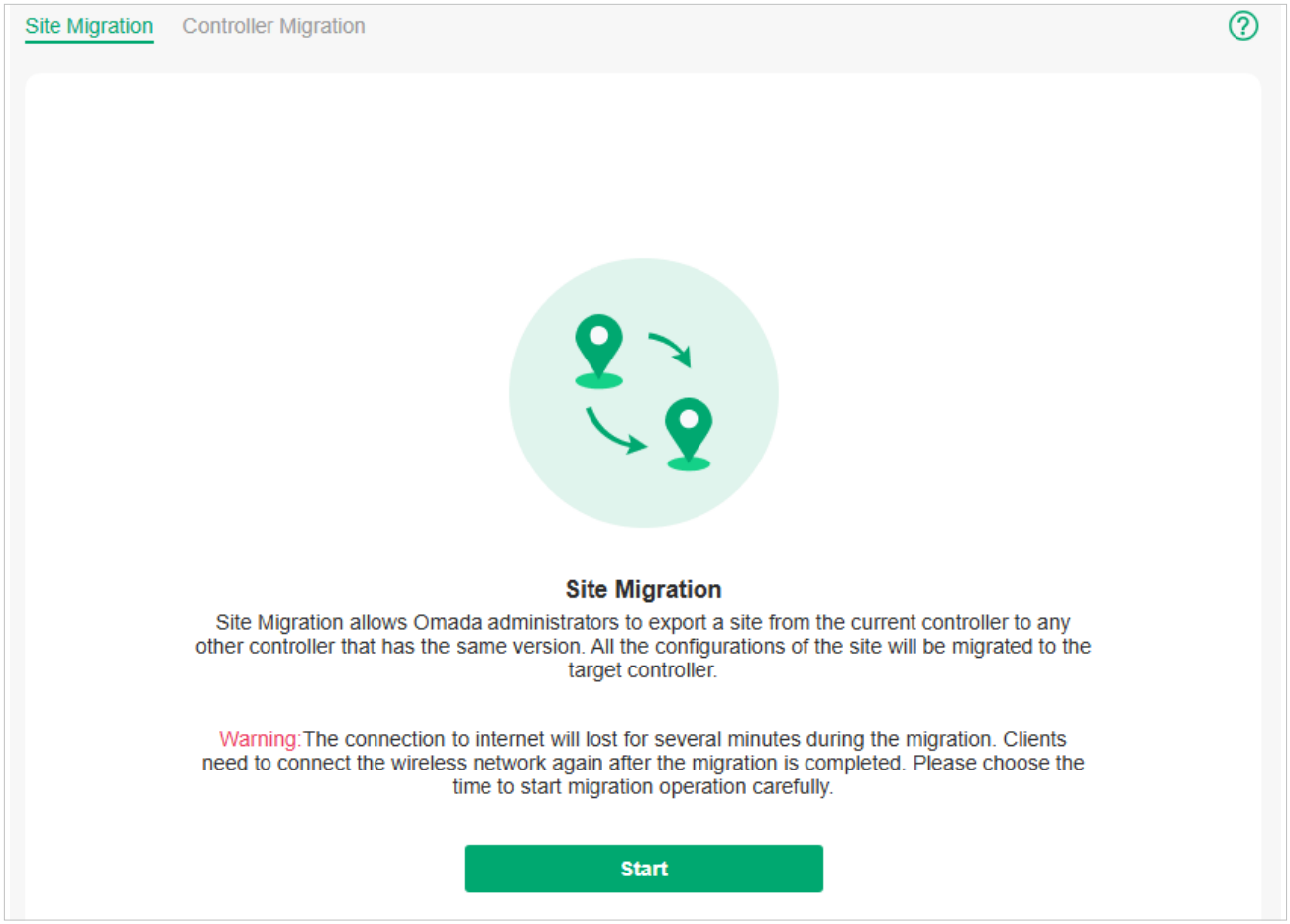
To migrate a site to another controller, follow these steps below.

Note:

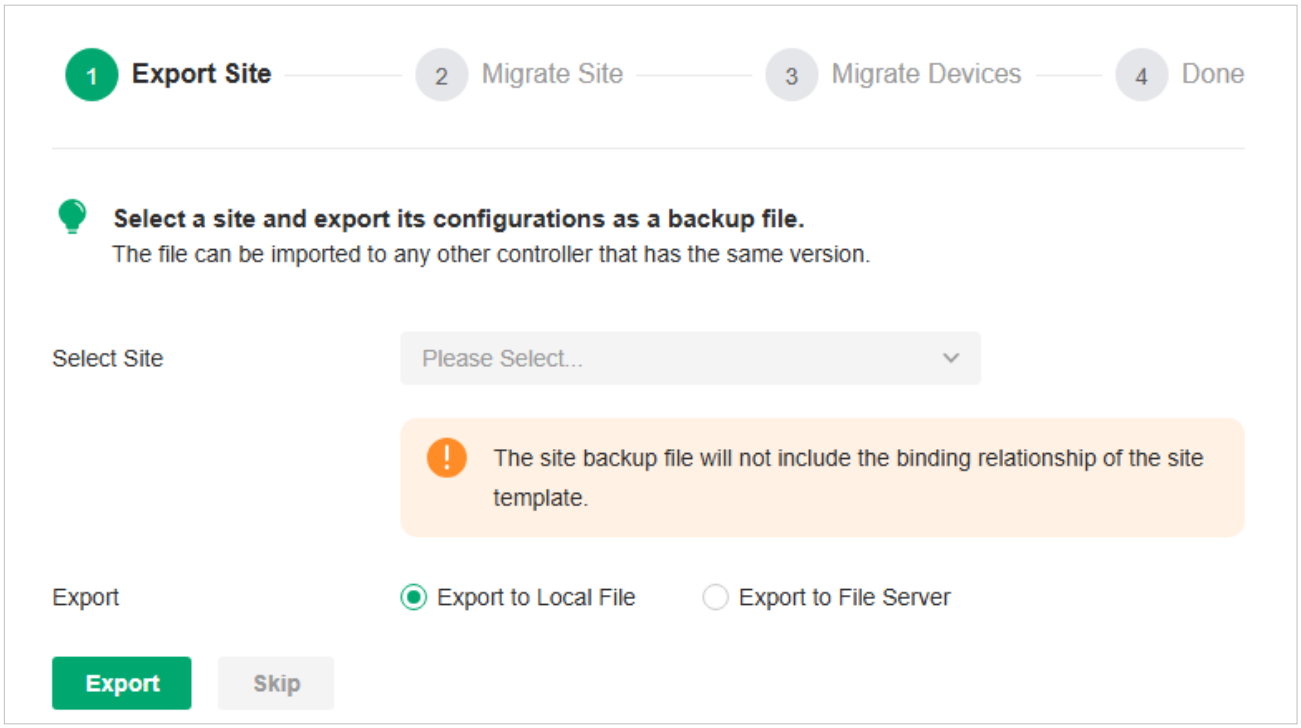
The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Step 1: Export Site

1. Launch the controller and access the Global View. Go to Settings > Migration. On the Site Migration tab, click the start button on the following page.

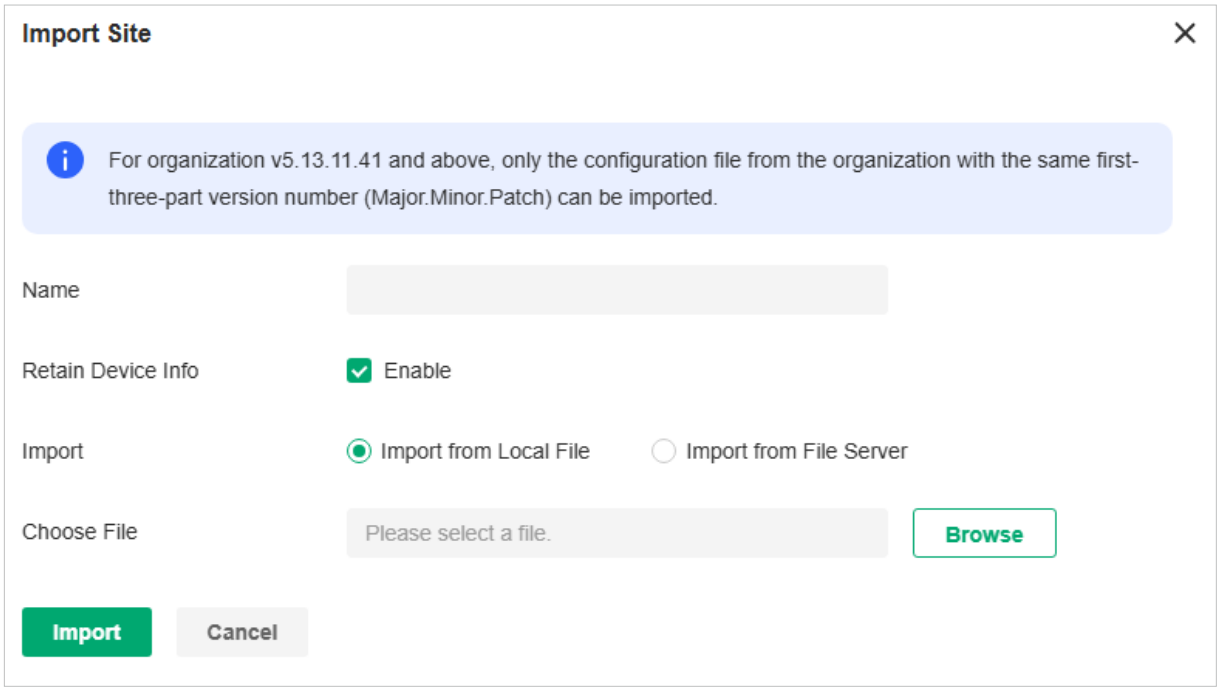


2. Select the site to be imported into the second controller in the Select Site drop-down list. Select where you want to export and save the backup file. Click Export to download the file of the current site. If you have backed up the file, click Skip.

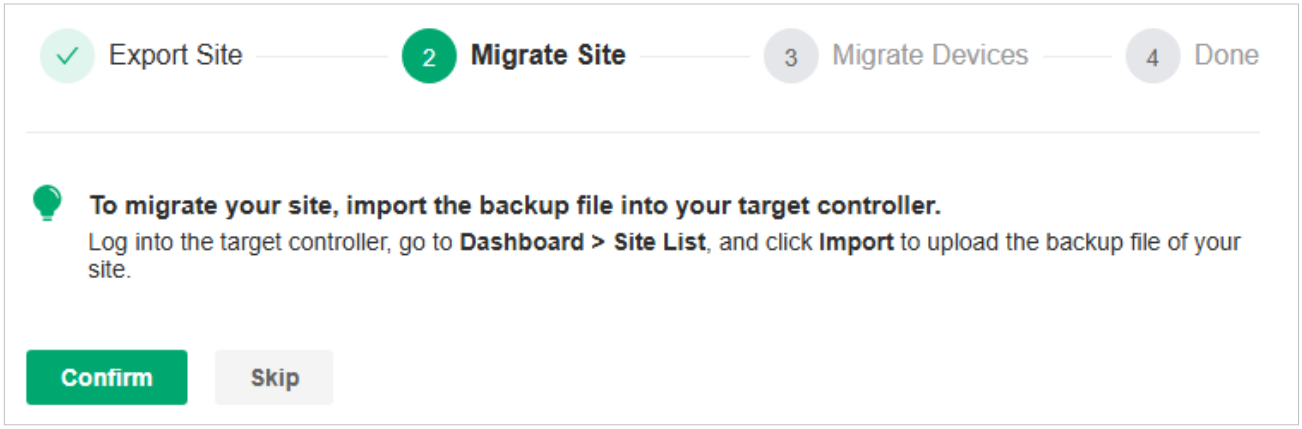


Step 2: Migrate Site

1. Start and log in to the target controller, go to Dashboard > Site List, and click Import Site to upload the backup file of your site, and then the following window will pop up. Note that for organization v5.13.11.41 and above, only the configuration file from the organization with the same first-three-part version number (Major.Minor.Patch) can be imported.

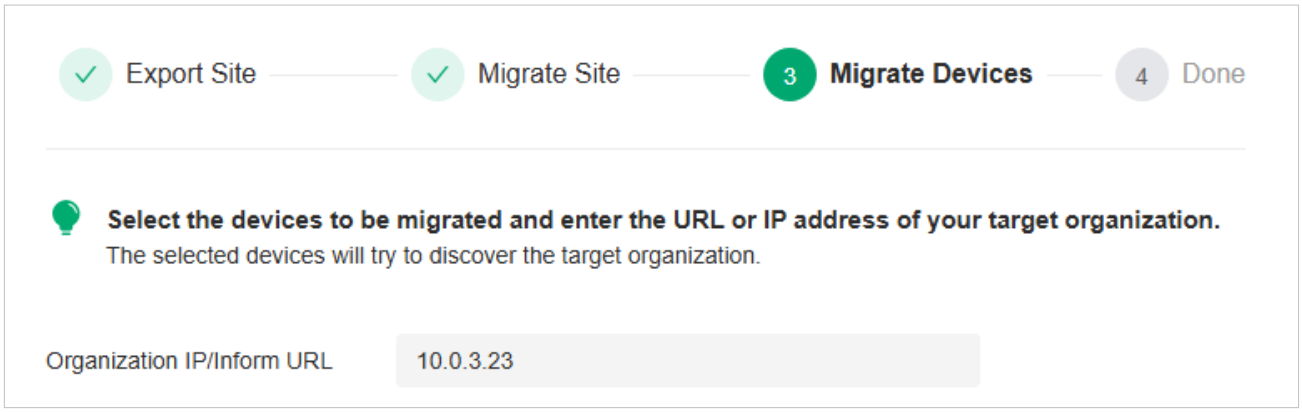


2. Enter a unique name for the new site. Click Browse to upload the file of the site to be imported and click Import to import the site.
3. After the file has been imported to the target controller, go back to the previous controller and click Confirm.



Step 3: Migrate Devices

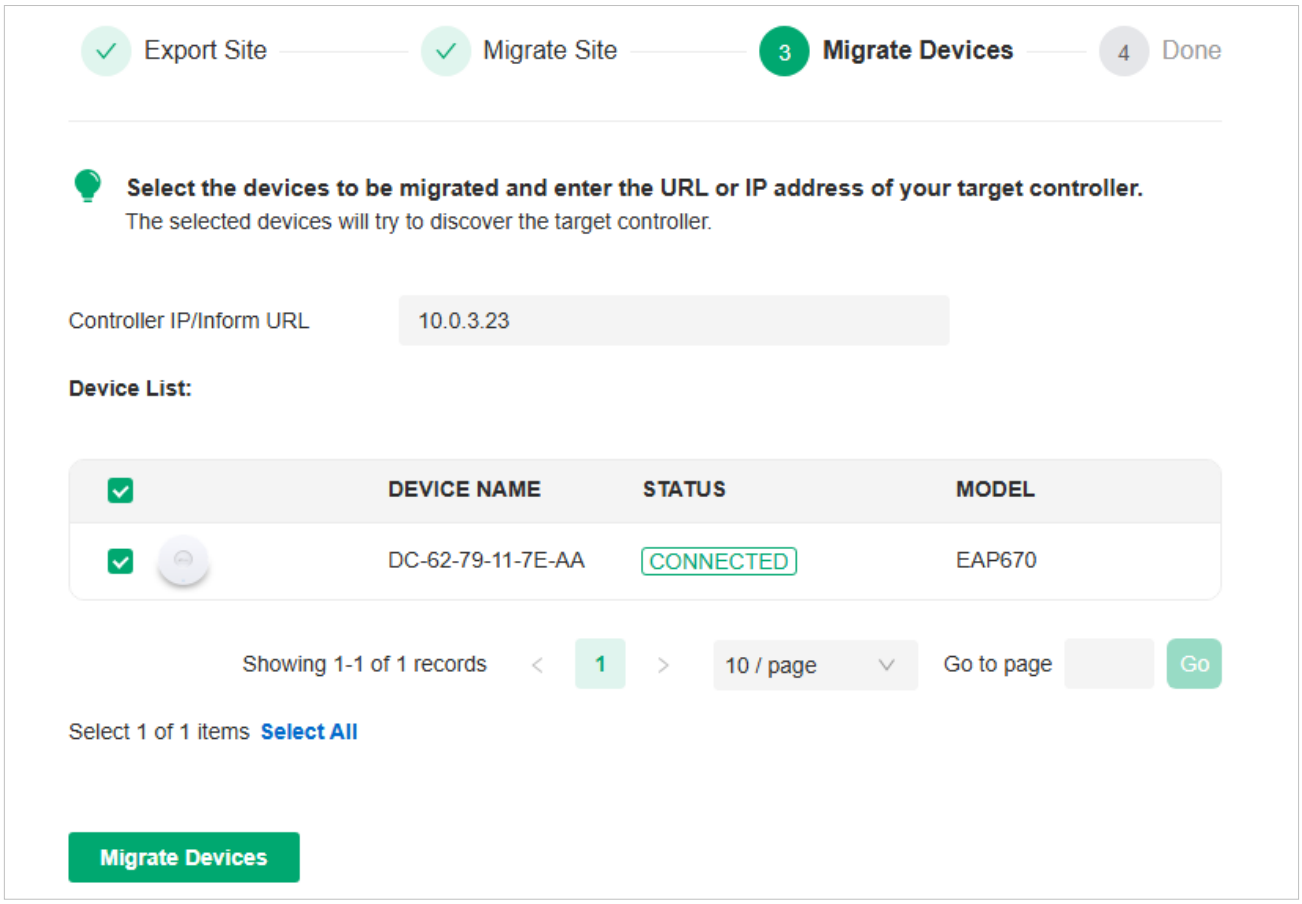
1. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



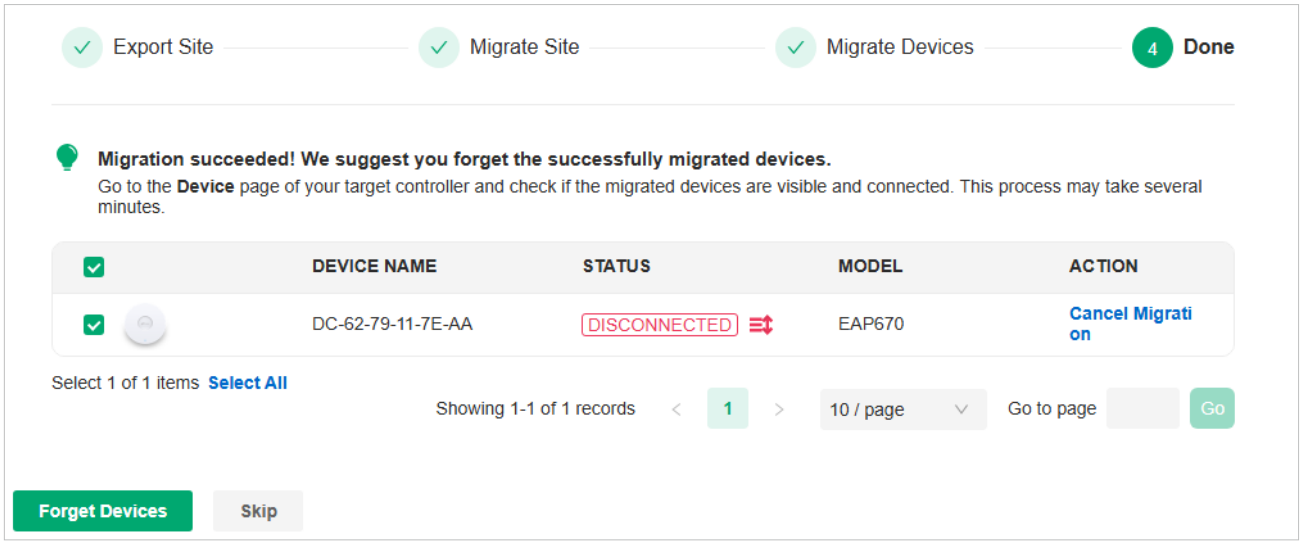
Note:

Make sure that you enter the correct IP address or URL of the target controller to establish the communication between managed devices and your target controller. Otherwise the managed devices cannot be adopted by the target controller.

2. Select the devices that are to be migrated by clicking the box next to each device. By default, all the devices are selected. Click Migrate Devices to migrate the selected devices to the target controller.



3. Verify that all the migrated devices are visible and connected on the target controller. When all the migrated devices are in Connected status on the Device page on the target controller, click Forget Devices to finish the migration process.



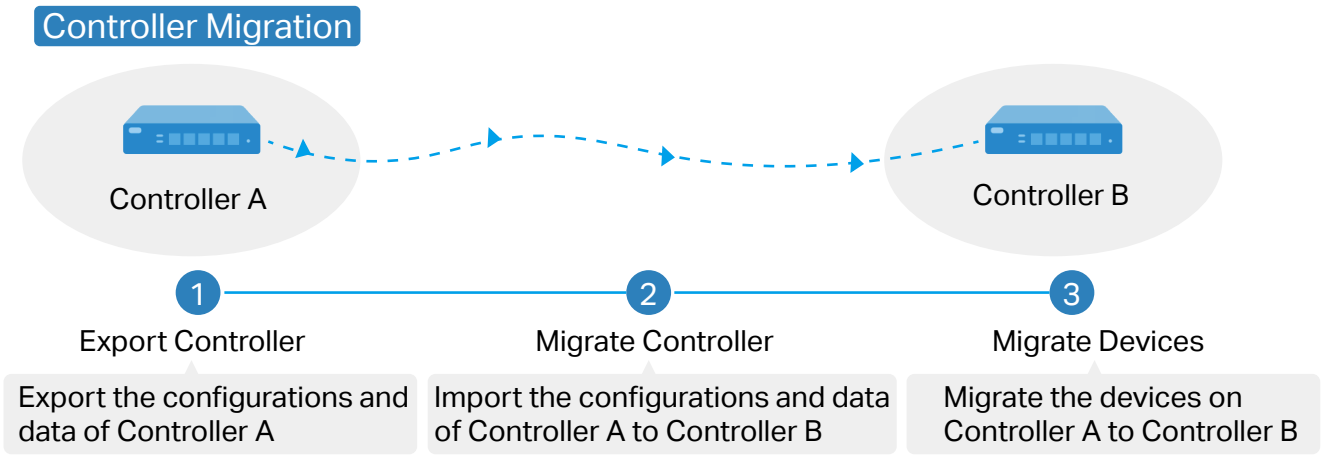
4. When the migration process is completed, all the configuration and data are migrated to the target controller. You can delete the previous site if necessary.

5. 8. 2 Controller Migration

Overview

Controller Migration allows administrators to migrate the configurations and data from the current controller to any other controller that has the same version.

The process of migrating configurations and data from the current controller to another controller can be summarized in three steps: Export Controller, Migrate Controller and Migrate Devices.



Step1: Export Controller

Export the configurations and data of the current controller as a backup file.

Step2: Migrate Controller

In the target controller, import the backup file of the current controller.

Step3: Migrate Devices

Migrate the devices on the current controller to the target controller.

Configuration

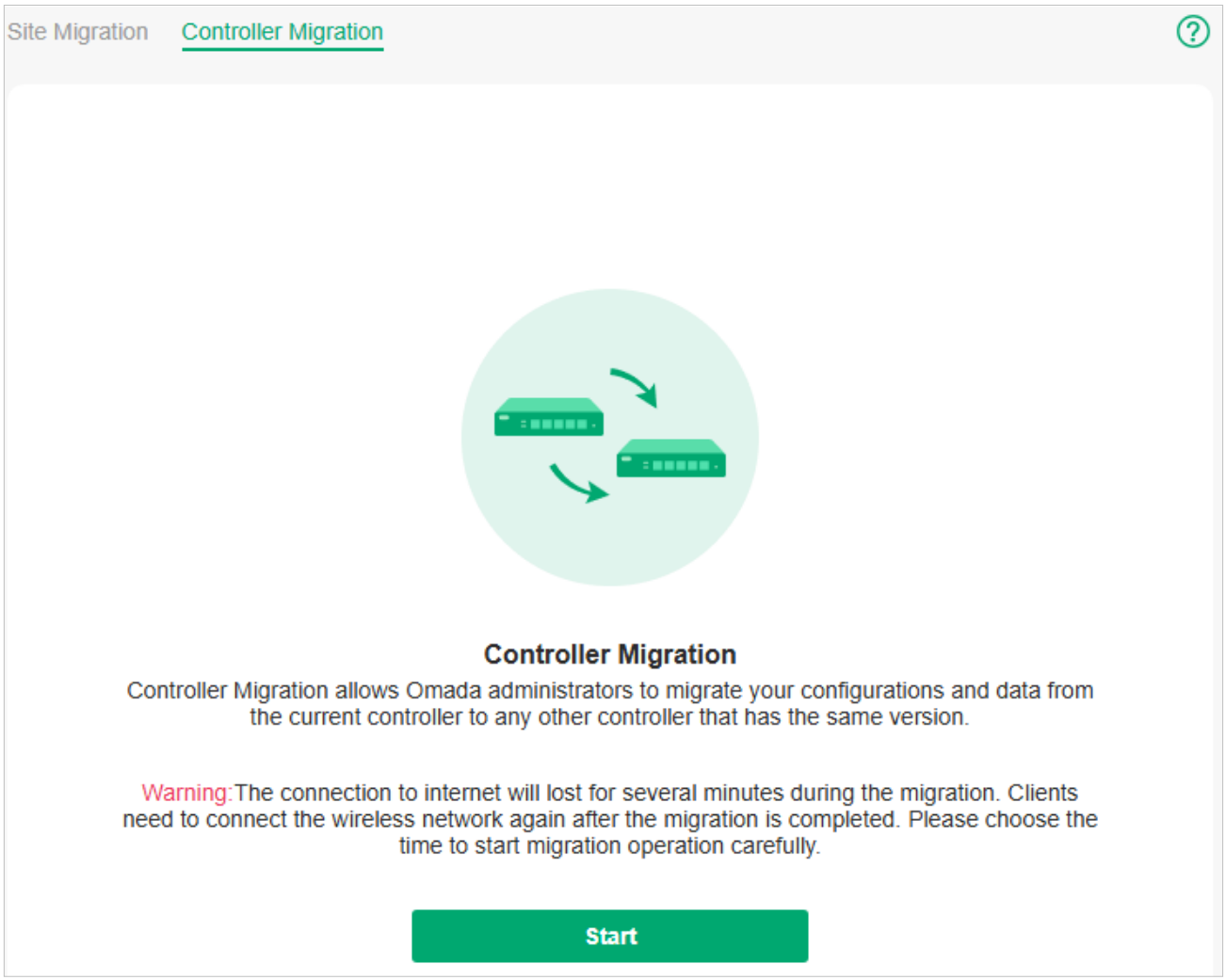
To migrate your controller, follow these steps below.

Note:

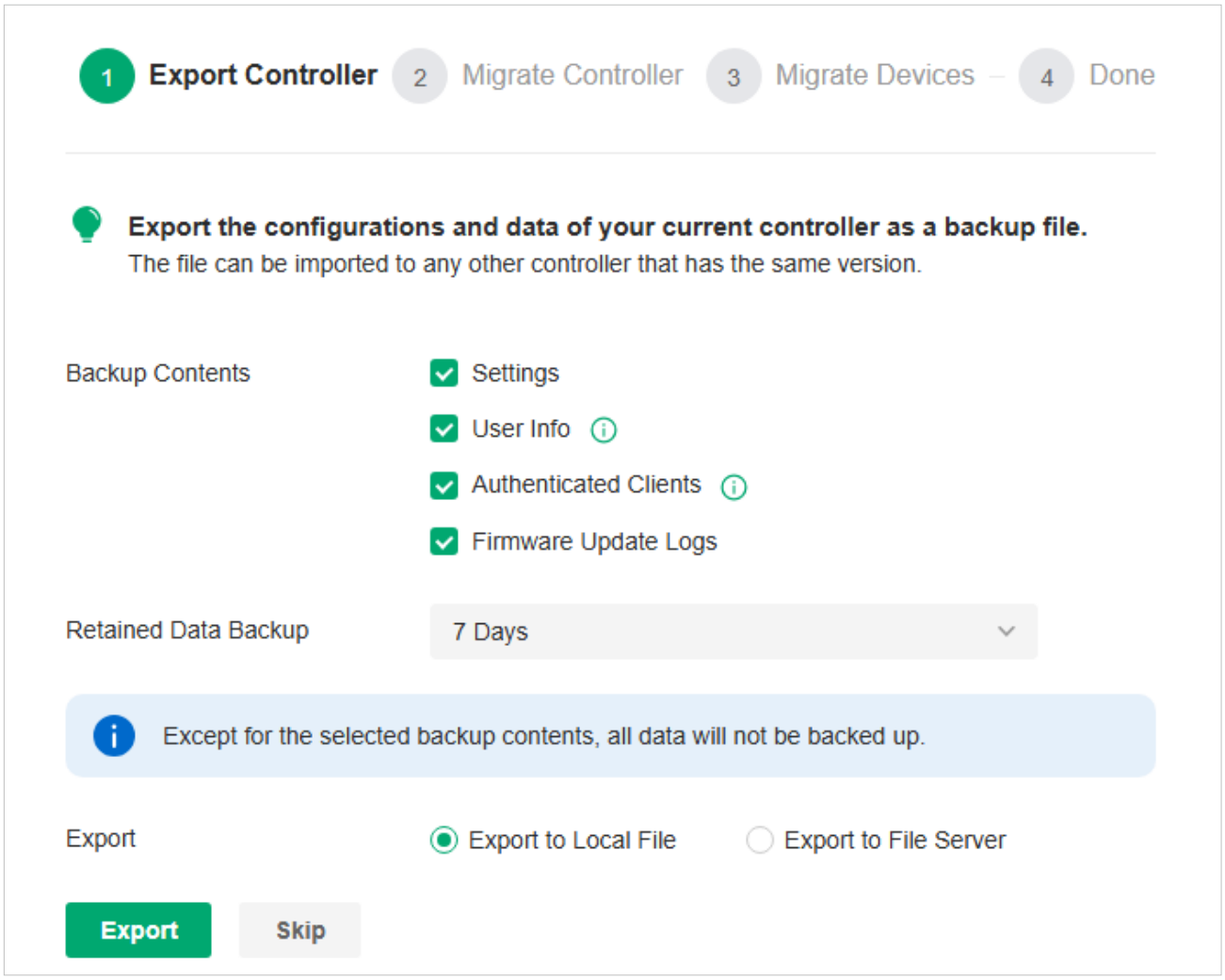
The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Step1: Export Controller

1. Launch the controller and access the Global View. Go to Settings > Migration. On the Controller Migration tab, click the start button on the following page.

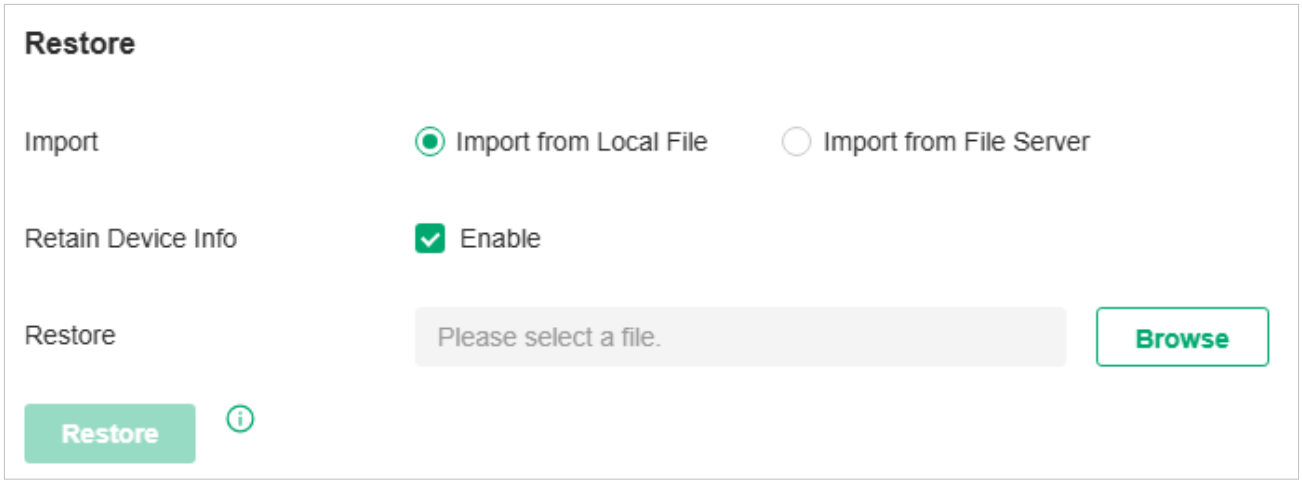


2. Select the length of time in days that data will be backed up in the Retained Data Backup, and where you want to export and save the data. Click Export to export the configurations and data of your current controller as a backup file. If you have backed up the file, click Skip.

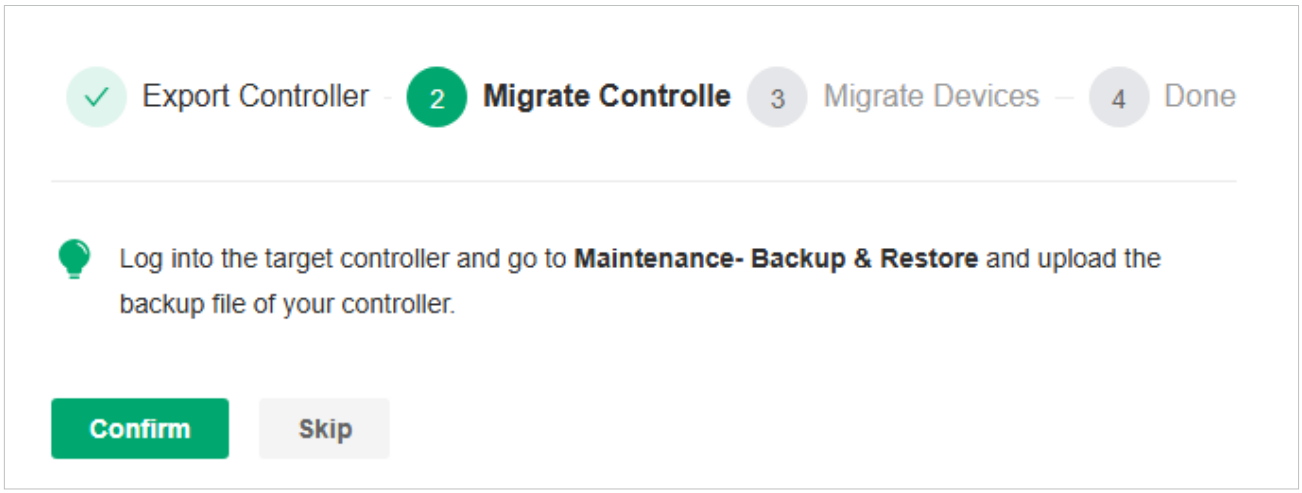


Step2: Migrate Controller

1. Log in to the target controller. Launch the controller and access the Global View. Go to Settings > Maintenance > Restore. Click Browse to locate and choose the backup file of the previous controller. Then click Restore to upload the file.

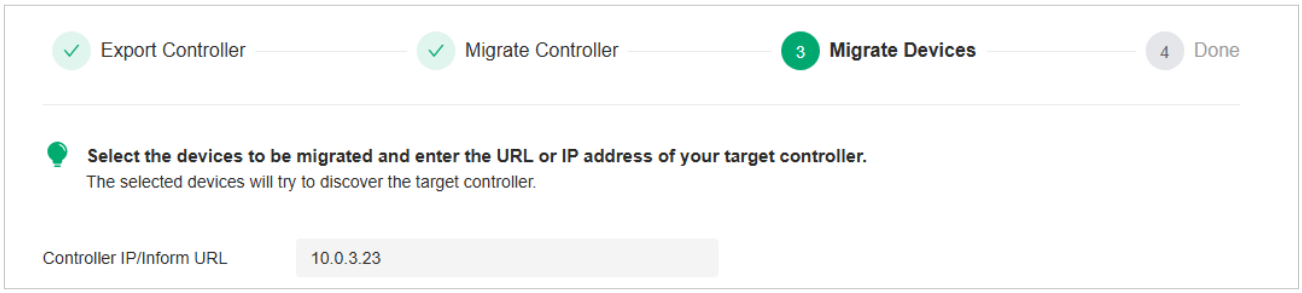


2. After the file has been imported to the target controller, go back to the previous controller and click Confirm.



Step3: Migrate Devices

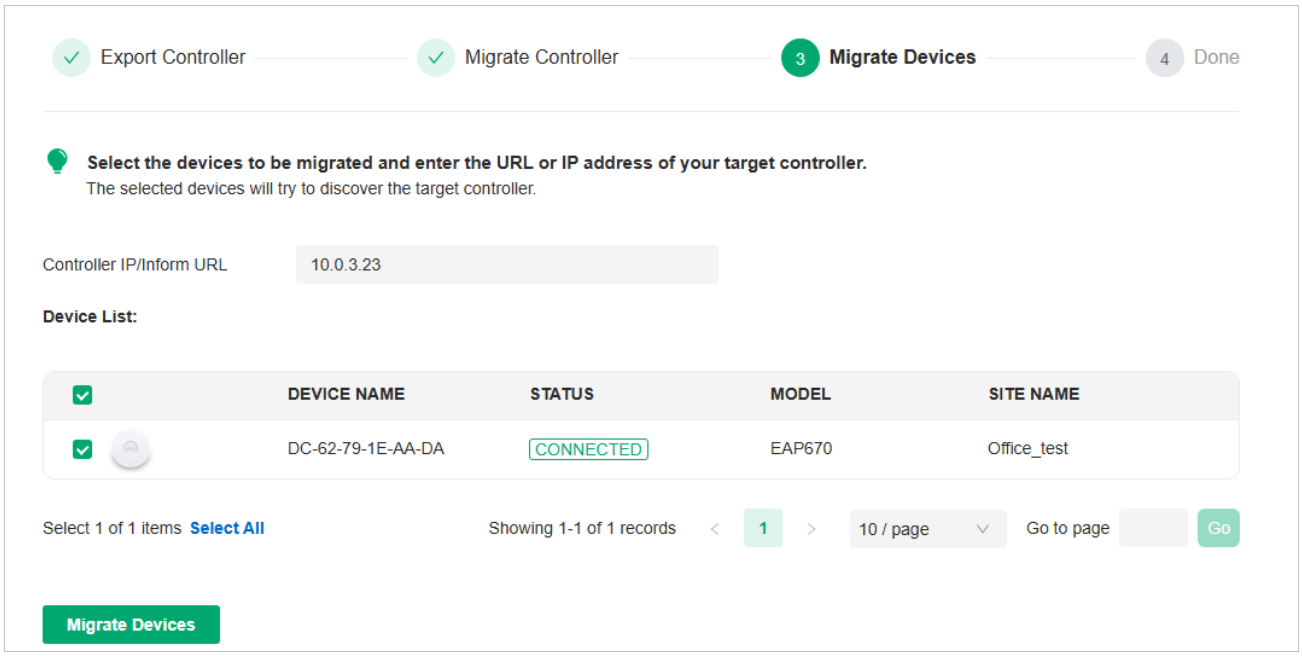
1. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



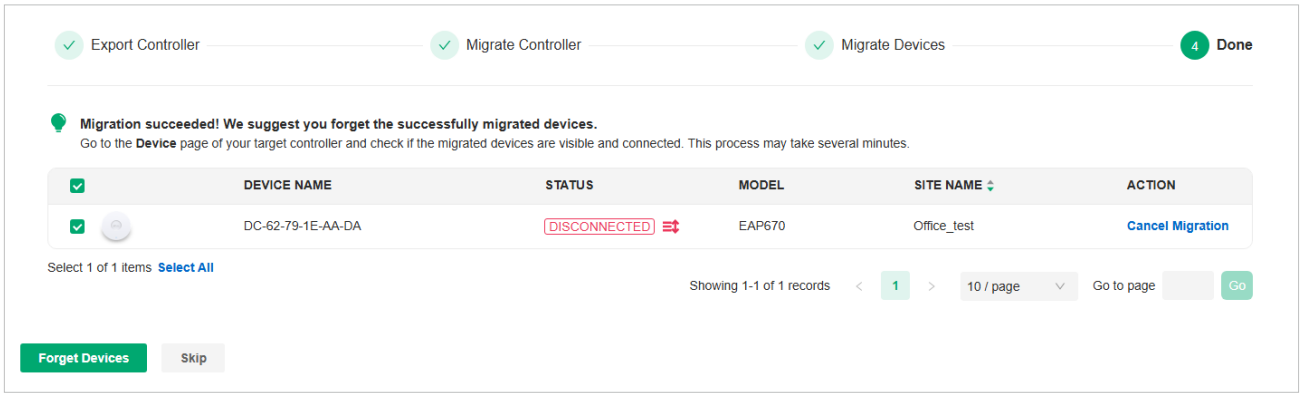
Note:

Make sure that you enter the correct IP address or URL of the target controller to establish the communication between managed devices and your target controller. Otherwise the managed devices cannot be adopted by the target controller.

2. Select the devices that are to be migrated by clicking the box next to each device. By default, all the devices are selected. Click Migrate Devices to migrate the selected devices to the target controller.



3. Verify that all the migrated devices are visible and connected on the target controller. When all the migrated devices are in Connected status on the Device page on the target controller, click Forget Devices to finish the migration process.



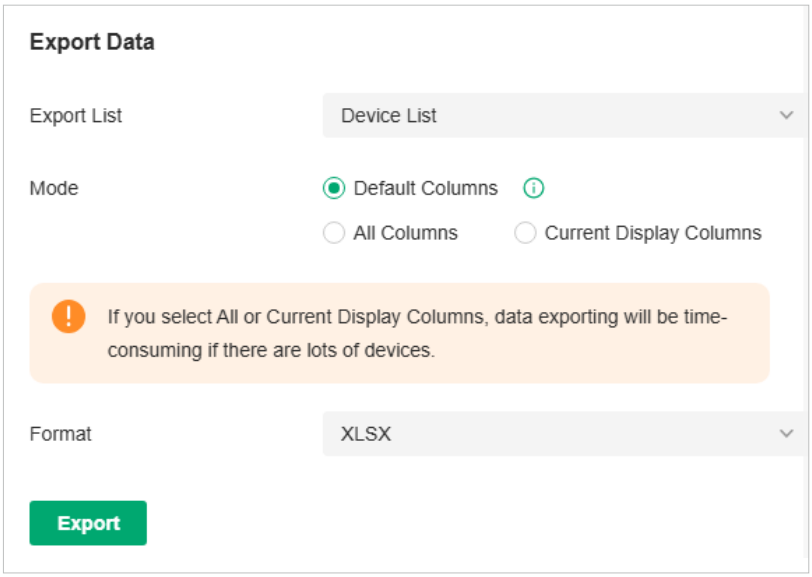
When the migration process is completed, all the configuration and data are migrated to the target controller. You can uninstall the previous controller if necessary.

5. 9 Export Data

5. 9. 1 Export Data

You can export data to monitor or debug your devices.

Launch the controller and access the Global View. Go to Settings > Export Data. Select the type of data from the export list and click Export.

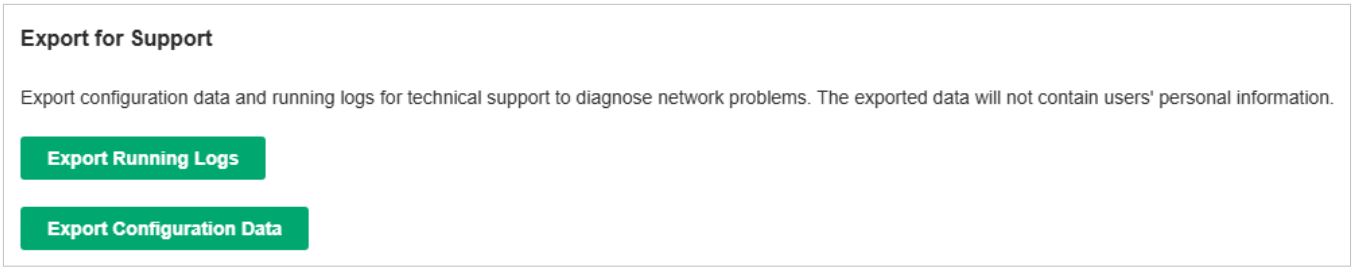


Export List	Device List: Export the list of managed devices. Client List: Export the list of all clients that are connected to the networks. Insight-Rogue AP List: Export the list of the rogue APs scanned before. Log List: Export the list of the logs generated by the controller. Authorized Client List: Export the list of authorized clients. Voucher Codes: Export the list of the voucher codes. Known Clients: Export the list of the known clients. Past Connections: Export the list of the past connections. To export past connections data, you need to first enable Client's History Data in 5.4 History Data Retention.
Mode	Select the columns to export. We recommend selecting Default Columns, which include commonly needed columns such as DEVICE NAME, MAC ADDRESS, MODEL, etc. If you select All Columns or Current Display Columns, data exporting will be time-consuming if there are lots of devices.
Format	The data can be exported to the file in the format of .CSV or .XLSX.

Send Email	If you want to send the exported data via email, enable Send Email and configure the parameters below: Report Name: Specify the report name of the email to send. Occurrence: Specify when to send the email. Send to: Specify the email addresses to send the exported data to.

5. 9. 2 Export for Support

In Export for Support, you can export configuration data and running logs for technical support to diagnose network problems. The exported data will not contain users' personal information.



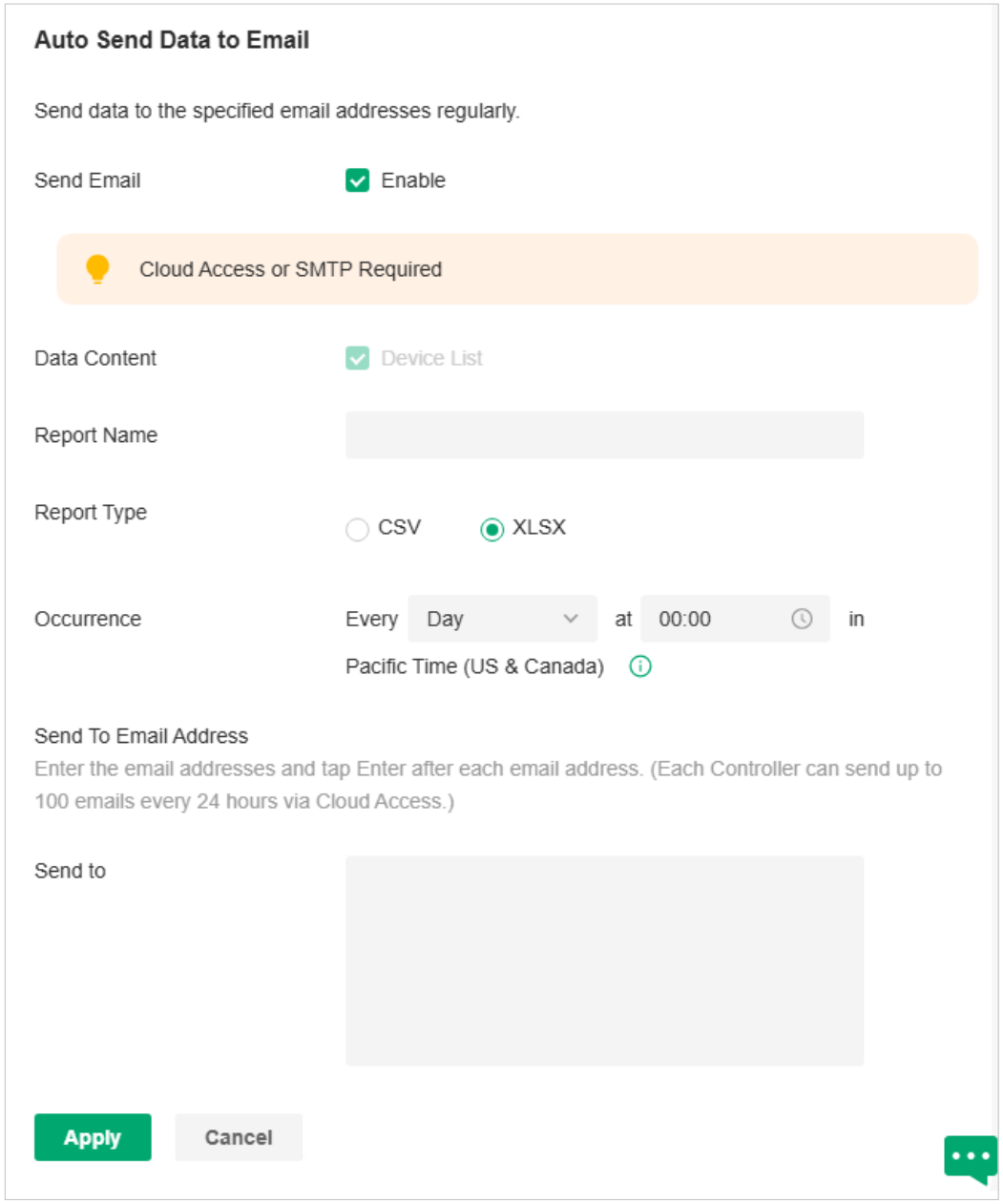
Export Running Logs	Click to export running logs.
Export Configuration Data	Click to export configuration data.

Note:

Configuration data cannot be imported into the controller through restore.

5. 9. 3 Auto Send Data to Email

In Auto Send Data to Email, you can send the data report to the specified email addresses regularly.



Report Name	Specify the name of the data report.
Report Type	Specify the file format of the data report.
Occurrence	Specify the time to send the data report.
Send to	Specify the email to send the data report.

Note:

Cloud Access or SMTP is required to enable the Send Email feature.

5. 10 Cloud Access

Overview

With Cloud Access, it is convenient for you to manage your controller from anywhere, as long as you have access to the internet.

Configuration

To manage your controller from anywhere, follow these steps:

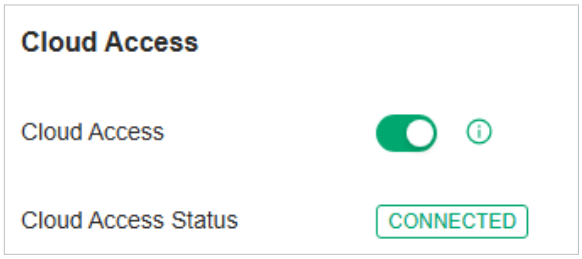
1. Prepare your controller for Cloud Access

■ For Software Controller / Hardware Controller:

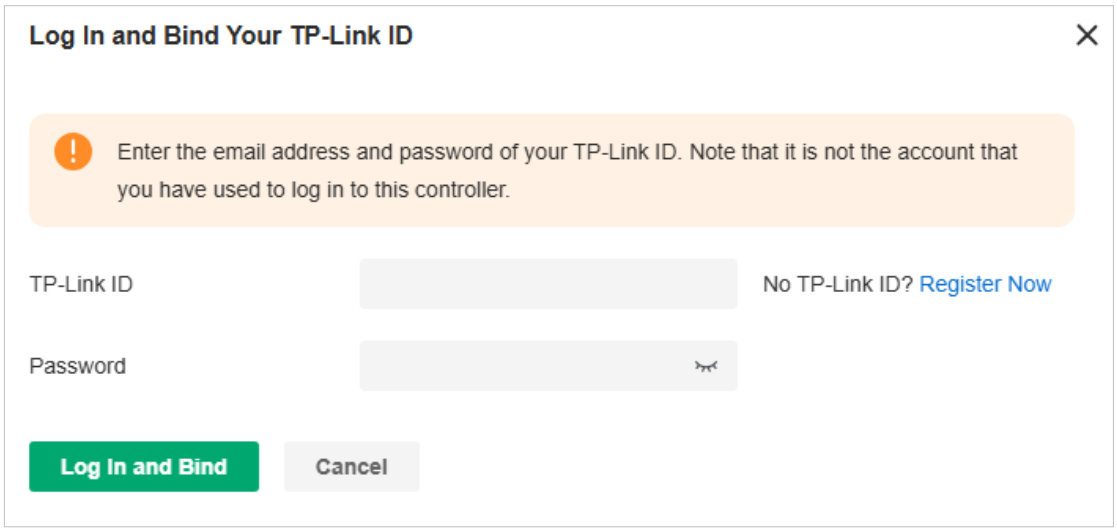
Note:

- Before you start, make sure your Software Controller Host or Hardware Controller has access to the internet.
- If you have enabled cloud access and bound your TP-Link ID in the quick setup wizard, skip this step.

1) Launch the controller and access the Global View. Go to Settings > Cloud Access. Enable Cloud Access.



2) Enter your TP-Link ID and password. Then click Log In and Bind.

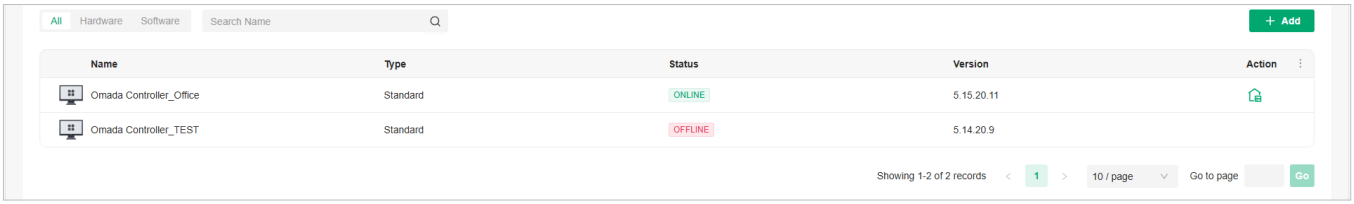


For Cloud-Based Controller

Your Cloud-Based Controller is based on the Cloud, so it is naturally accessible through Cloud Service. No additional preparation is needed.

2. Access your controller through Cloud Service

Go to https://omada.tplinkcloud.com and login with your TP-Link ID and password. A list of controllers that have been bound with your TP-Link ID will appear. Then click the launch icon in the Action column to manage the controller.



Chapter 6

Configure and Monitor Controller-Managed Devices

This chapter guides you on how to configure and monitor controller-managed devices, including gateways, switches and APs. You can configure the devices individually or in batches to modify the configurations of certain devices. The chapter includes the following sections:

- 6. 1 Introduction to the Devices Page
- 6. 2 Configure and Monitor the Gateway
- 6. 3 Configure and Monitor Switches
- 6. 4 Configure and Monitor APs
- 6. 5 Create and Manage Stack Groups
- 6. 6 Create and Manage Bridge Groups

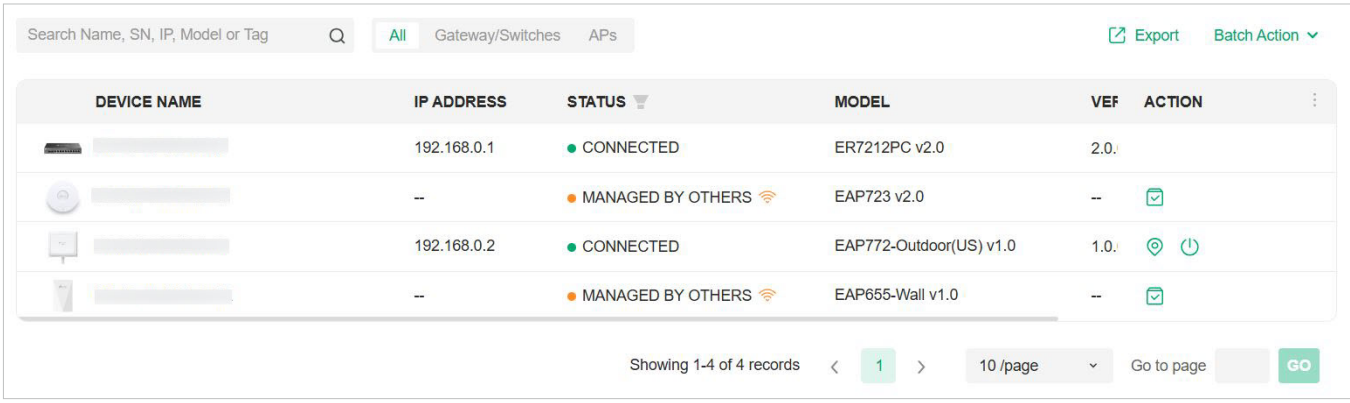
6. 1 Introduction to the Devices Page

The Devices page is further divided into Device List, Device Group, and Configuration Result.

Overview

This page displays all TP-Link devices discovered by the controller and their general information.

For an easy monitoring of the devices, you can customize the column and filter the devices for a better overview of device information. Also, quick operations and Batch Edit are available for configurations.



According the connection status, the devices have the following status: Pending, Isolated, Connected, Managed by Others, Heartbeat Missed, and Disconnected. The icons in the Status column are explained as follows:

PENDING	The device is in Standalone Mode or with factory settings, and has not been adopted by the controller. To adopt the device, click , and the controller will use the default username and password to adopt it. When adopting, its status will change from Adopting, Provisioning, Configuring, to Connected eventually.
ISOLATED	(For APs in the mesh network) The AP once managed by the controller via a wireless connection now cannot reach the gateway. You can rebuild the mesh network by connecting it to an AP in the Connected status, then the isolated AP will turn into a connected one. For detailed configuration, refer to Mesh.
CONNECTED	The device has been adopted by the controller and you can manage it centrally. A connected device will turn into a pending one after you forget it.
MANAGED BY OTHERS	The device has already been managed by another controller. You can reset the device or provide the username and password to unbind it from another controller and adopt it in the current controller.
HEARTBEAT MISSED	A transition status between Connected and Disconnected. Once connected to the controller, the device will send inform packets to the controller in a regular interval to maintain the connection. If the controller does not receive its inform packets in 30 seconds, the device will turn into the Heartbeat Missed status. For a heartbeat-missed device, if the controller receives an inform packet from the device in 5 minutes, its status will become Connected again; otherwise, its status will become Disconnected.

DISCONNECTED	The connected device has lost connection with the controller for more than 5 minutes.
	(For APs in the mesh network) When this icon appears with a status icon, it indicates the AP with mesh function and no wired connection is detected by the controller. You can connect it to an uplink AP through Mesh.
	When this icon appears with a status icon, it indicates the device in the Connected, Heartbeat Missed, Isolated, or Disconnected status is migrating. For more information about Migration, refer to 5. 8 Migration.

Configuration

- **Customize the Column**

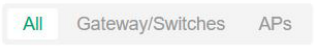
  To customize the columns, click the ellipsis icon next to Action and check the boxes of information type.

  To change the list order, click the upside-down triangle icon next to the column head, which indicates the ascending or descending order.

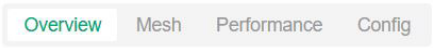
- **Filter the Devices**

  Use the search box and tab bar above the table to filter the devices.

  To search the devices, enter the text in the search box or select a tag from the drop-down list. As for the device tag, refer to the general configuration of switches and APs.

  To filter the devices, a tab bar 

is above the table to filter the devices by device type. You can also filter the devices by their status by clicking the filter icon in the Status column.

  If you select the APs tab, another tab bar 

will be available to change the column quickly.

Overview	Displays the device name, IP address, status, model, firmware version, uptime, channel, and Tx power by default.
Mesh	Displays the information of devices in the mesh network, including the device name, IP address, status, model, uplink device, channel, Tx power, and the number of downlink devices, clients and hops by default.
Performance	Displays the device name, IP address, status, uptime, channel, Tx power, the number of 2.4 GHz and 5 GHz clients, Rx rate, and Tx rate by default.
Config	Displays the device name, status, version, WLAN group, and the radio settings for 2.4 GHz and 5 GHz by default.

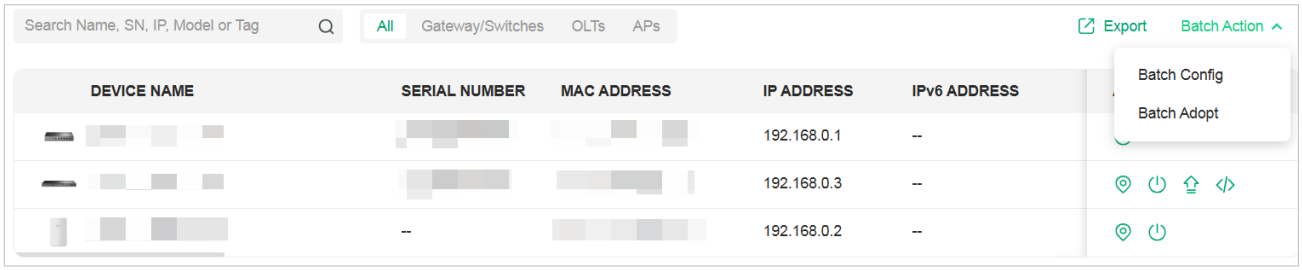
- **Quick Operations**

  Click the icons in the Header or the Action column to quickly adopt, locate, upgrade, or reboot the device.

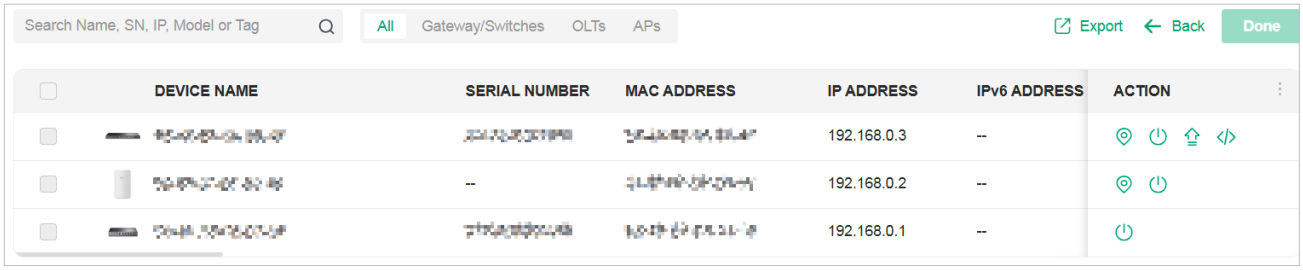
Start Rolling Upgrade	Click to upgrade the managed devices in batches.
	Click to check if there is new firmware for the managed devices.
	(For pending devices) Click to adopt the device.
	(For connected switches and APs) Click this icon and the LEDs of the device will flash to indicate the device's location. The LEDs will keep flashing for 10 minutes, or you can click the icon to stop the flashing.
	(For connected devices) Click to reboot the device.
	Click to upgrade the device's firmware version. This icon appears when the device has a new firmware version.
	Displays the current running configuration. Operators or Administrators or local user group members with execution rights for this command.

- **Batch Edit (for Switches and APs)**

After selecting the Gateway/Switches or APs tab, you can adopt or configure the switches or APs in batches. Batch Config is available only for the devices in Connected/Disconnected/Heartbeat Missed/Isolated status, while Batch Adopt is available for the devices in the Pending/Managed By Others status.



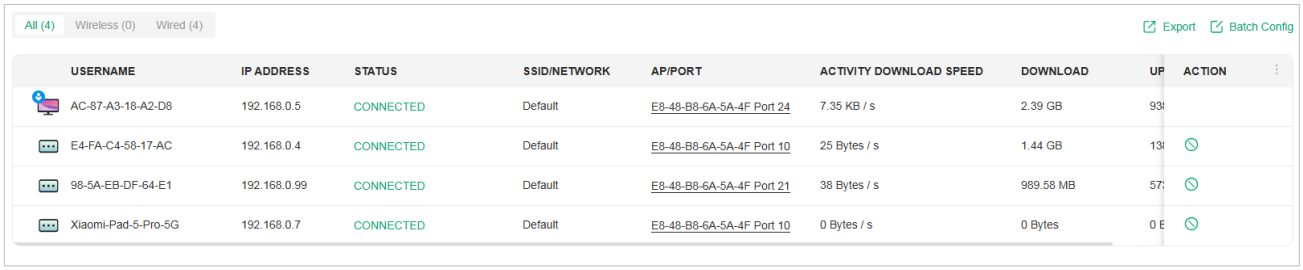
Click Batch Action, select Batch Adopt, click the checkboxes of devices, and click Done. If the selected devices are all in the Pending status, the controller will adopt then with the default username and password. If not, enter the username and password manually to adopt the devices.



Click Batch Action, select Batch Config, click the checkboxes of devices, and click Done. Then the Properties window appears. There are two tabs in the window: Devices and Config.

In Devices, you can click the close icon to remove the device from the current batch configuration.

In Config, all settings are Keep Existing by default. For detailed configurations, refer to the configuration of switches and APs.

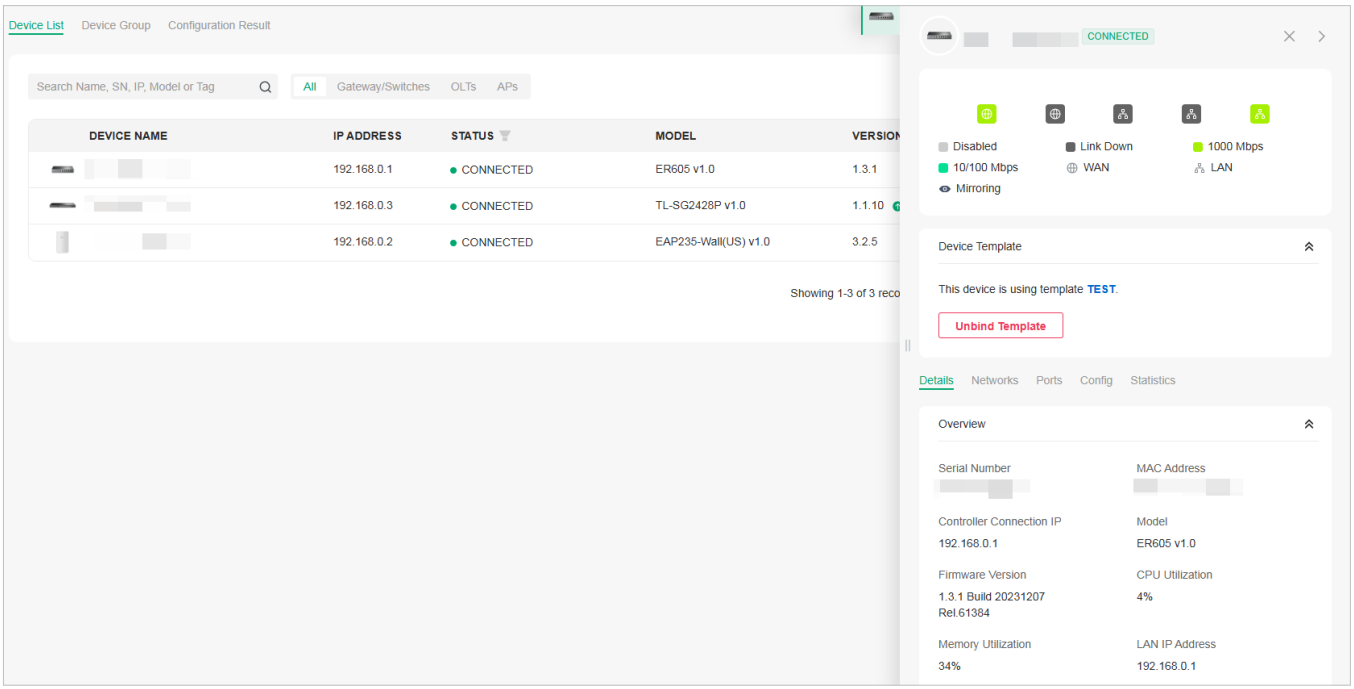


	Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click  .
	Click to maximize the Properties window. You can also use the icon on pages other than the Devices page.
	Click to close the Properties window of the chosen device(s). Note that the unsaved configuration will be lost.
	The number on the lower-right shows the number of devices in the batch configuration.

6. 2 Configure and Monitor the Gateway

In the Properties window, you can configure the gateway managed by the controller and monitor the performance and statistics. By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of a router. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Config tab, such as IP, SNMP, and Hardware Offload, while other tabs are mainly used to monitor the devices.



Note:

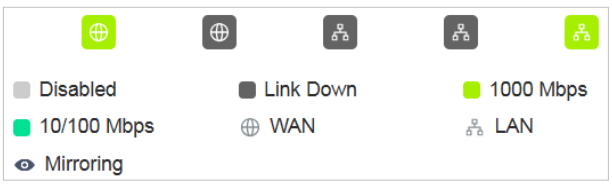
- You can adopt only one router in one site.
- The available functions in the window vary due to the model and status of the device.

6. 2. 1 Configure the Gateway

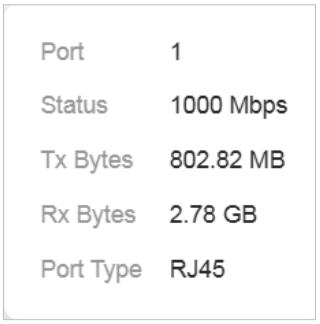
In the Properties window, you can view and configure the ports in Ports, and configure the gateway features in Config.

Monitor Panel

The monitor panel displays the router's ports, and it uses colors and icons to indicate different connection status and port types. When the router is pending or disconnected, all ports are disabled.

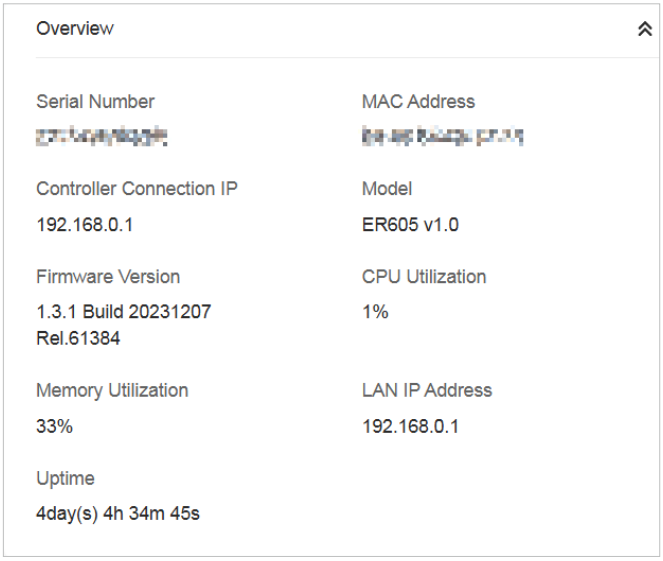


You can hover the cursor over the port icon for more details.



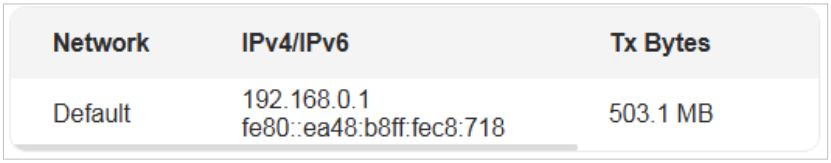
Details

In Details, you can view the basic information of the router and statistics of WAN ports to know the device's running status briefly. The listed information varies with devices.



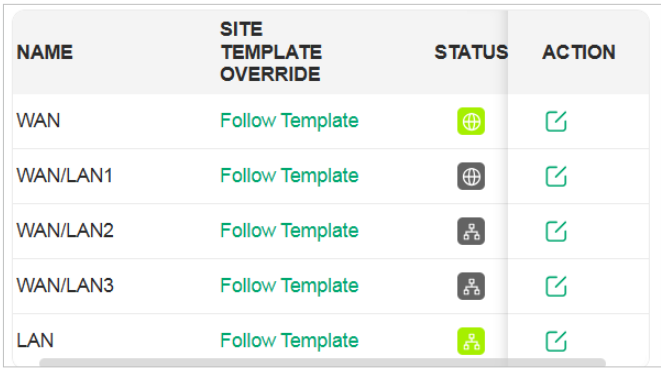
Networks

In Networks, you can view the network information of the router.

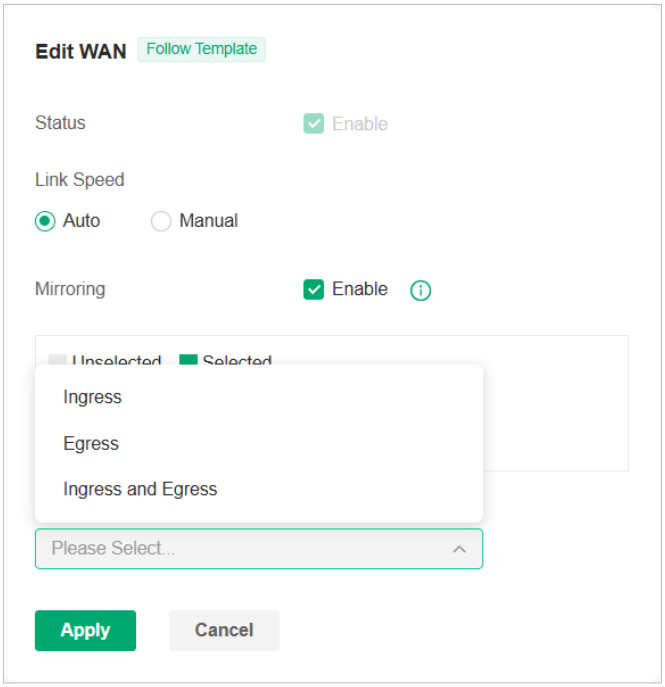


Ports

In Ports, you can view the status and edit settings of the ports.



To configure a port, click the edit icon in the Action column.



Status	Check the box to enable the port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Mirroring	Mirroring is used to analyze network traffic and troubleshoot network problems. Enable this option to set the edited port as the mirroring port, then specify one or multiple mirrored ports. The gateway will sends a copy of traffics passing through the mirrored ports to the mirroring port.

Mirror Mode	Specify the directions of the traffic to be mirrored. Ingress and Egress: Both the incoming and outgoing packets through the mirrored port will be copied to the mirroring port. Ingress: The packets received by the mirrored port will be copied to the mirroring port. Egress: The packets sent by the mirrored port will be copied to the mirroring port.

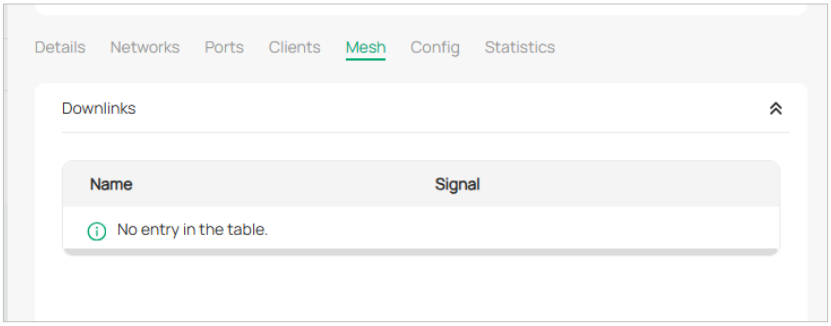
Clients

In Clients, you can view the clients of the router.



Mesh (for wireless routers only)

In Mesh, you can view the mesh downlinks of the router.

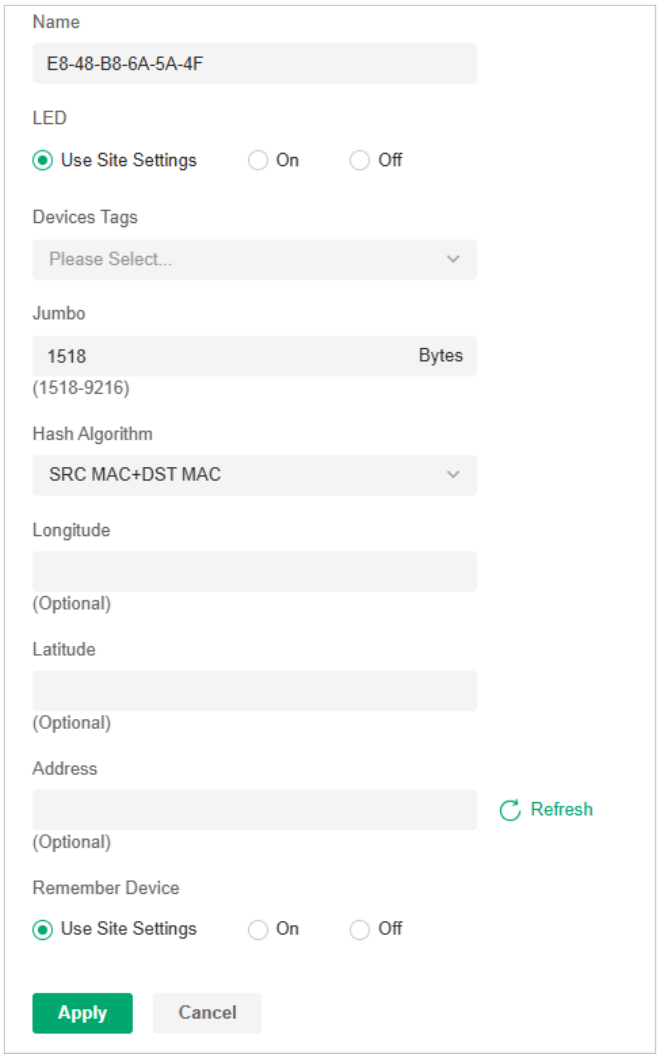


Config

In the Properties window, click Config and then click the sections to configure the features applied to the router.

General

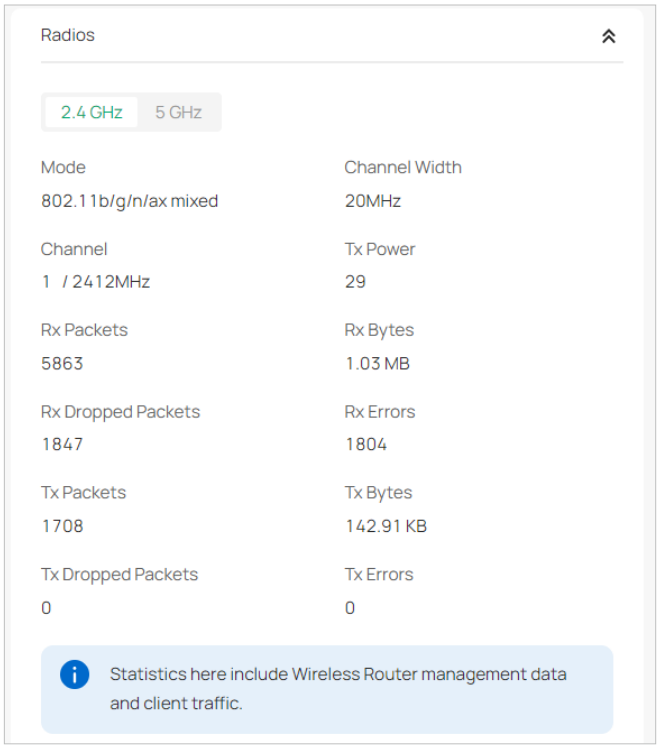
In General, you can specify general settings of the router.



Name	Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.
Remember Device	When enabled, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.

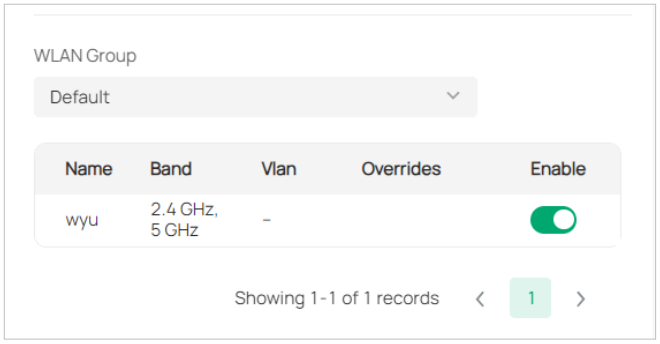
- **Radios (for wireless routers only)**

  In Radios, you can view the statistics of the wireless router management data and client traffic of each band. Different models support different bands.

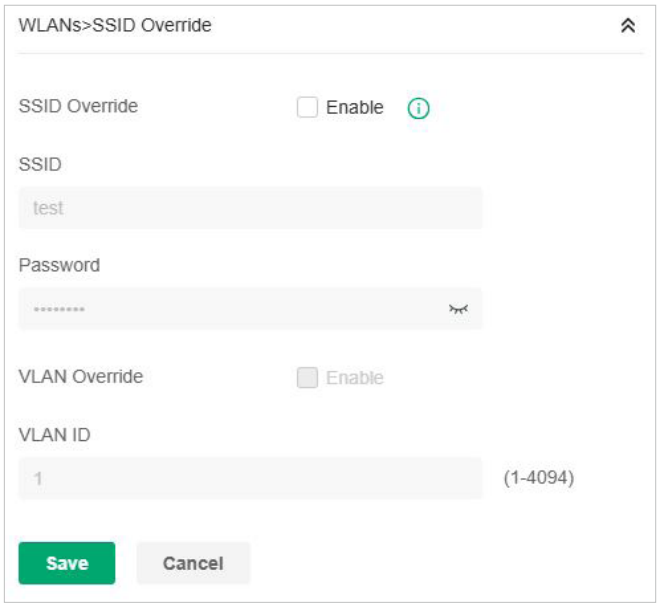


- **WLANs**

  In WLANs, you can apply the WLAN group to the router and specify a different SSID name and password to override the SSID in the WLAN group. After that, clients can only see the new SSID and use the new password to access the network. To create or edit WLAN groups, refer to 4. 3 Configure Wireless Networks.



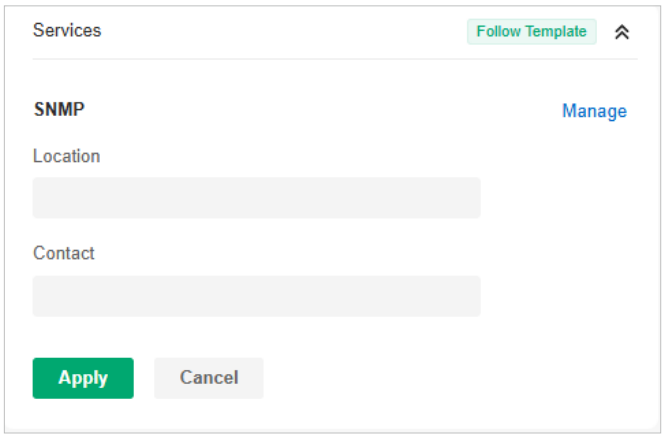
(Only for configuring a single device) To override the SSID, select a WLAN group, click the edit icon in the entry and then the following page appears.



SSID Override	Enable or disable SSID Override on the AP. If SSID Override enabled, specify the new SSID and password to override the current one.
VLAN	Enable or disable VLAN. If VLAN enabled, enter a VLAN ID to add the new SSID to the VLAN.

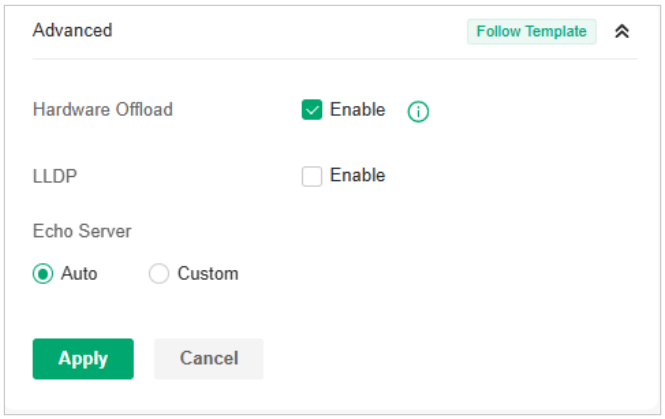
- **Services**

In Services, you can configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP.



Advanced

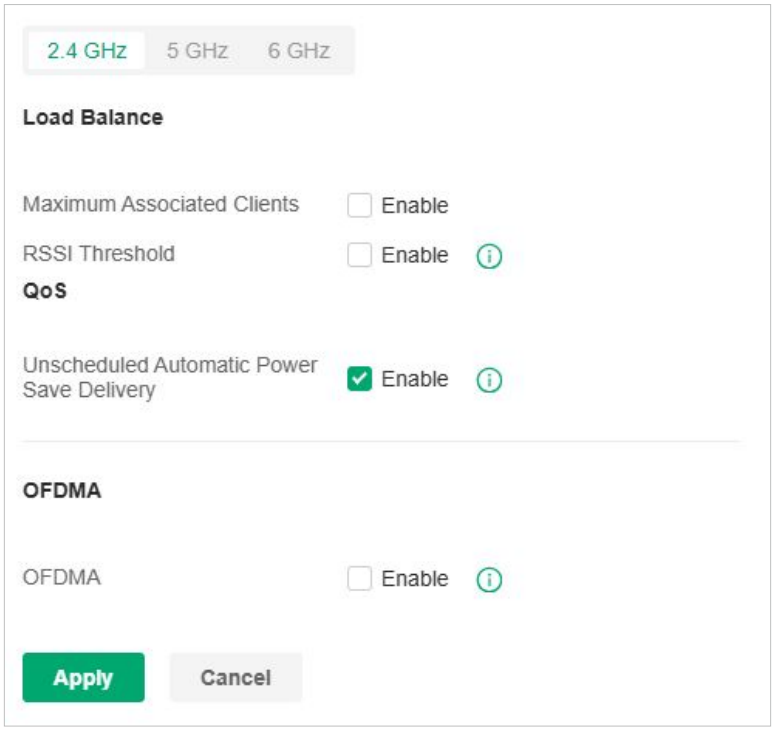
In Advanced, you can configure advanced settings to make better use of network resources.



Hardware Offload	Hardware Offload can improve performance and reduce CPU utilization by using the hardware to offload packet processing. Note that this feature cannot take effect if QoS, Bandwidth Control, or Session Limit is enabled. To configure Bandwidth Control and Session Limit for the router, refer to 4. 5 Transmission.
LLDP	LLDP (Link Layer Discovery Protocol) can help discover devices.
Echo Server	Echo Server is used to test the connectivity and monitor the latency of the network automatically or manually. If you click Custom, enter the IP address or hostname of your custom server.

For a wireless gateway, you can configure Load Balance and QoS to make better use of network resources. Load Balance can control the client number associated to the device, while QoS can optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media.

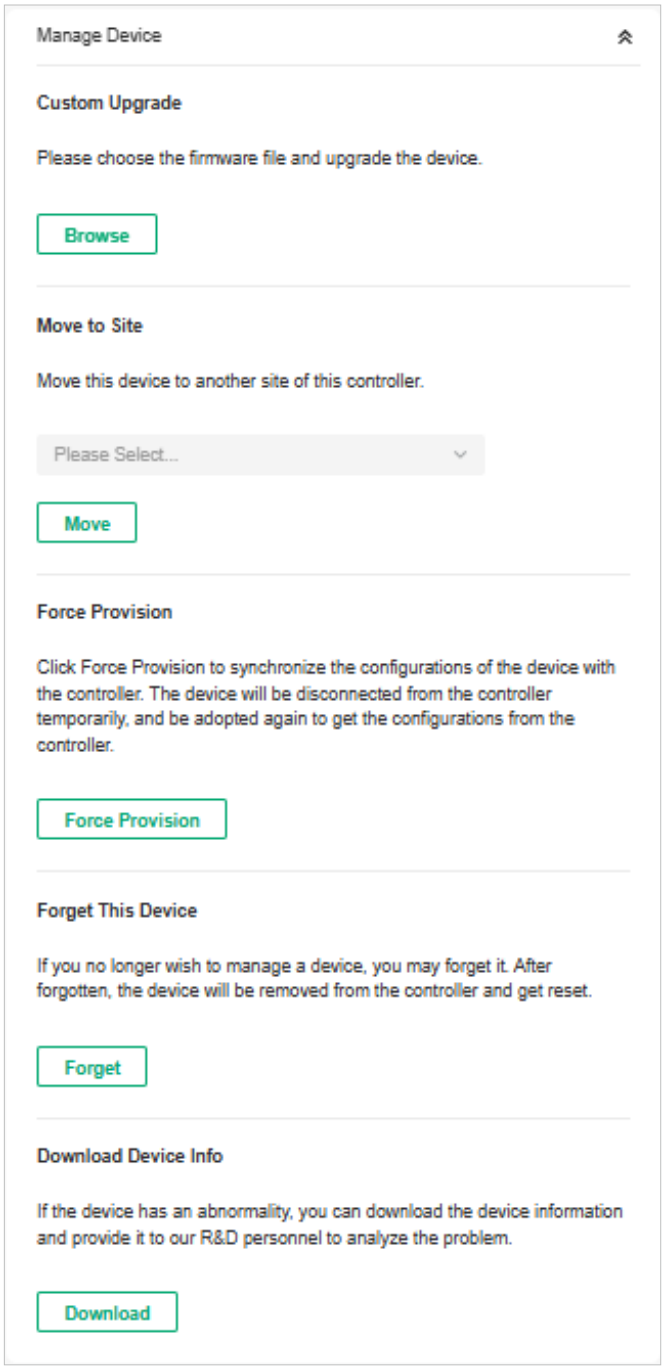
Select each frequency band and configure the following parameters and features.



Max Associated Clients	Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the device will disconnect those with weaker signals to make room for other clients requesting connections.
RSSI Threshold	Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If the client's signal strength is weaker than the threshold, the client will lose connection with the device.
Unscheduled Automatic Power Save Delivery	When enabled, this function can greatly improve the energy-saving capacity of clients.
OFDMA	(Only for AP supporting 802.11 ax or later standards) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improves speed and efficiency. Note that the benefits of OFDMA can be fully enjoyed only when the clients support OFDMA.

Manage Device

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller, and forget the router.

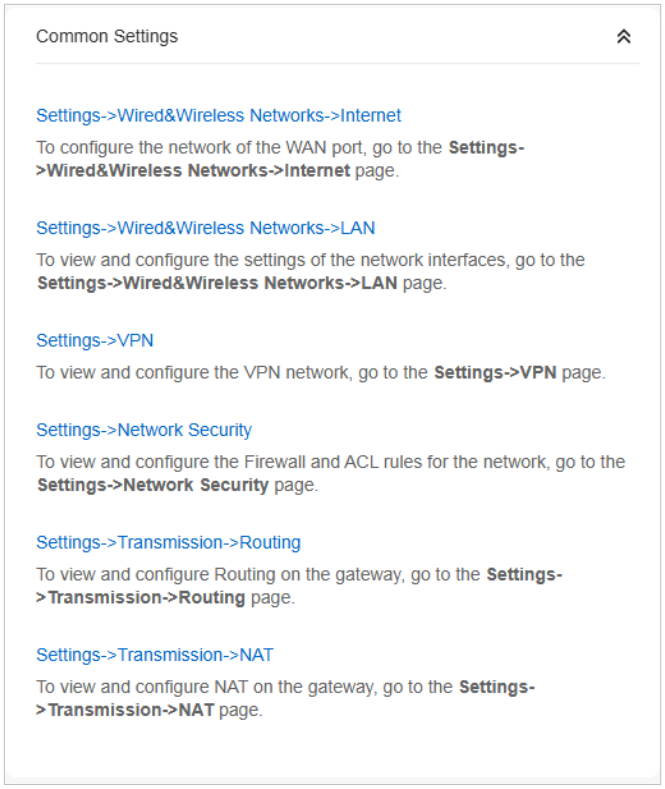


Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.

Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.

- **Common Settings**

  In Common Settings, you can click the path to jump to corresponding modules quickly.

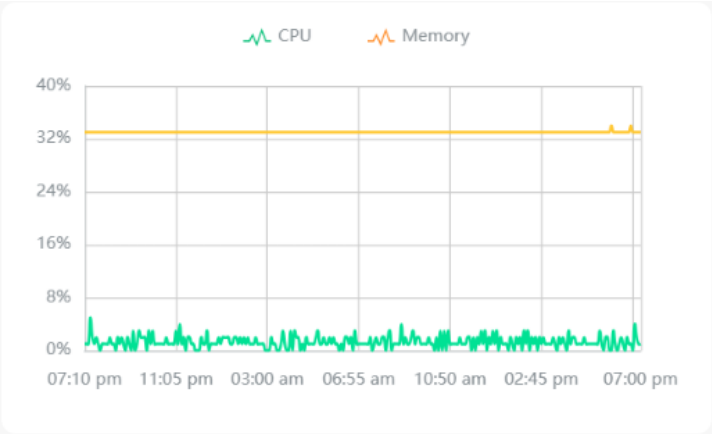


6. 2. 2 Monitor the Gateway

One panel and three tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Networks, and Statistics.

Statistics

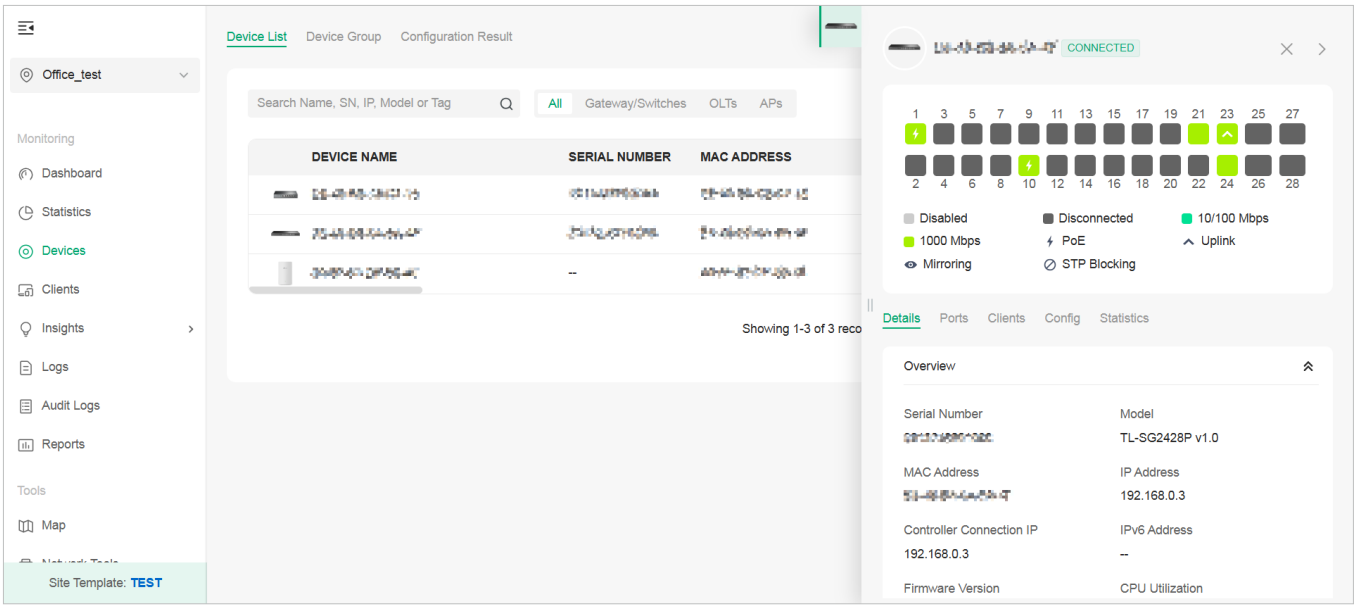
In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in a certain period, click the chart.



6. 3 Configure and Monitor Switches

In the Properties window, you can configure one or some switches connected to the controller and monitor the performance and statistics. Configurations changed in the Properties window will be applied only to the selected switch(es). By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of a switch, or click Batch Action, and then Batch Config to select switches for batch configuration. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Ports and Config tab, such as the port mirroring, IP address, and Management VLAN, while other tabs are mainly used to monitor the devices.



Note:

- The available functions in the window vary due to the model and status of the device.
- In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.

6. 3. 1 Configure Switches

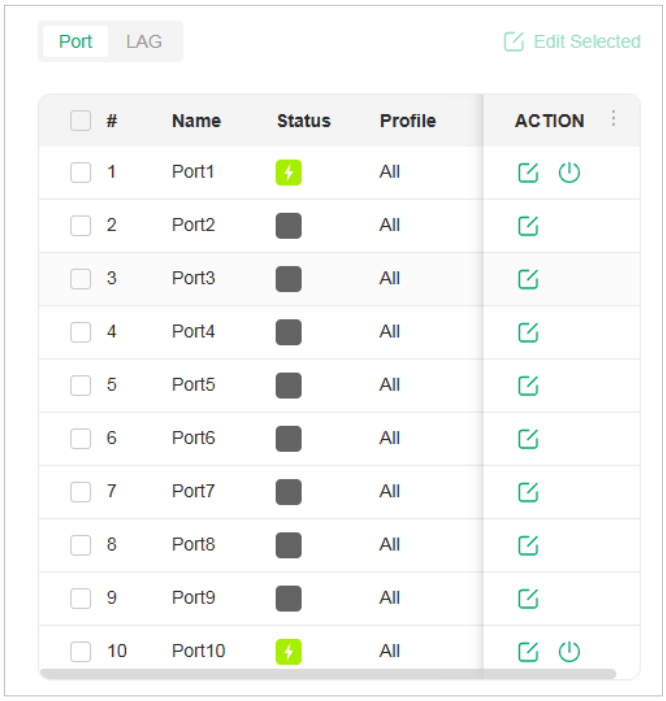
In the Properties window, you can view and configure the profiles applied to ports in Ports, and in Config, you can configure the switch features.

Ports

Port and LAG are two tabs designed for physical ports and LAGs (Link Aggregation Groups), respectively. Under the Port tag, all ports are listed but you can configure physical ports only, including overriding the applied profiles, configuring Port Mirroring, and specifying ports as LAGs. Under the LAG tag, all LAGs are listed and you can view and modify the configurations of existing LAGs.

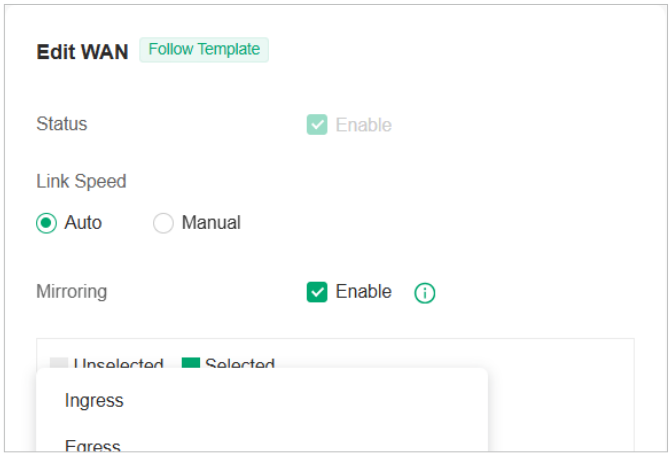
Ports

In Ports, you can view and configure all ports' names and applied profiles.



Status	Displays the port status in different colors. : The port profile is Disabled. To enable it, click the edit icon to change the profile. : The port is enabled, but no device or client is connected to it. : The port is running at 1000 Mbps. : The port is running at 10/100 Mbps.
Profile	Displays the profile applied to the port.
Action	: Click to edit the port name and configure the profile applied to the port. : (For PoE ports) Click to reboot the connected powered devices (PDs).

To configure a single port, click in the table. To configure ports in batches, click the checkboxes and then click Edit Selected. Then you can configure the port name and profile. By default, all settings are Keep Existing for batch configuration.

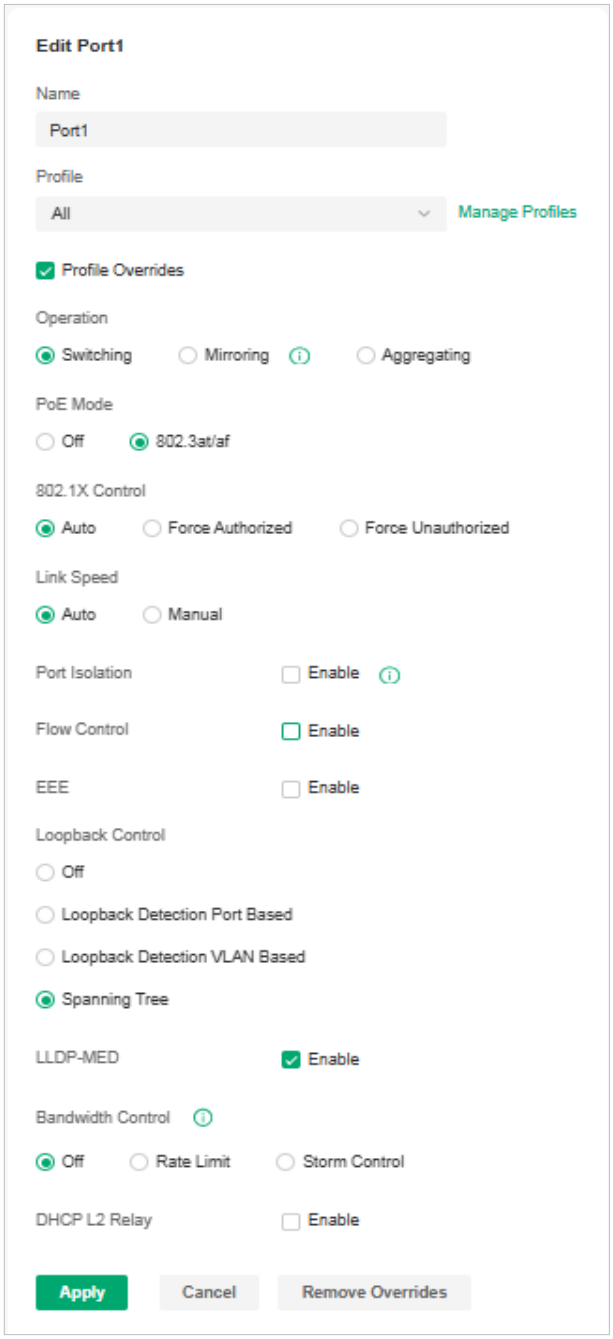


Name	Enter the port name.
Profile	Select the profile applied to the port from the drop-down list. Click Manage Profiles to jump to view and manage profiles. For details, refer to 4. 2 Configure Wired Networks.
Profile Overrides	Click the checkbox to override the applied profile. The parameters to be configured vary in Operation modes,

With Profile Overrides enabled, select an operation mode and configure the following parameters to override the applied profile, configure a mirroring port, or configure a LAG.

- Override the Applied Profile

  If you select Switching for Operation, configure the following parameters and click Apply to override the applied profile. To discard the modifications, click Remove Overrides and all profile configurations will become the same as the applied profile.



PoE Mode	(Only for PoE ports) Select the PoE (Power over Ethernet) mode for the port. Off: Disable PoE function on the PoE port. 802.3at/af: Enable PoE function on the PoE port.

802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Settings > Authentication > 802.1X. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, and the client connected to the port cannot authenticate with any means. The switch cannot provide authentication services to the client through the port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the current port will be removed from the VLAN. Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP (Voice over Internet Protocol) devices.

Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and specify traffic threshold on each port to make good use of network bandwidth. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Action	When Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network, which takes the Layer 2 DHCP communications (Discover, Request, etc.) and forwards them to a specified IP address (your DHCP server).
Format	Select the format of option 82 sub-option value field. Normal: The format of sub-option value field is TLV (type-length-value). Private: The format of sub-option value field is just value.

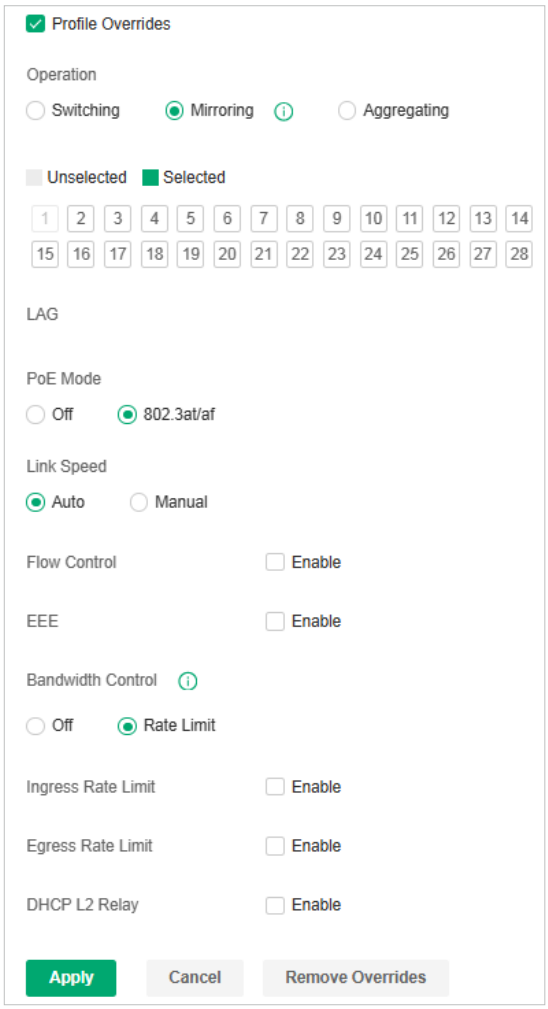
Circuit ID	(Optional) Enter the customized circuit ID. The circuit ID configurations of the switch and the DHCP server should be compatible with each other. If it is not specified, the switch will use the default circuit ID when inserting Option 82 to DHCP packets.
Remote ID	(Optional) Enter the customized remote ID. The remote ID configurations of the switch and the DHCP server should be compatible with each other. If it is not specified, the switch will use its own MAC address as the remote ID.

- Configure a Mirroring Port

  If you select Mirroring as Operation, the edited port can be configured as a mirroring port. Specify other ports as the mirrored port, and the switch sends a copy of traffics passing through the mirrored port to the mirroring port. You can use mirroring to analyze network traffic and troubleshoot network problems.

  To configure Mirroring, select the mirrored port or LAG, specify the following parameters, and click Apply. To discard the modifications, click Remove Overrides and all profile configurations become the same as the applied profile.

Note that the mirroring ports and the member ports of LAG cannot be selected as mirrored ports.



PoE Mode	(Only for PoE ports) Select the PoE mode for the port. Off: Disable PoE on the PoE port. 802.3at/af: Enable PoE on the PoE port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Bandwidth Control	Bandwidth control optimizes network performance by limiting the bandwidth of specific sources. Off: Disable bandwidth control on the port. Rate Limit: Enable bandwidth control on the port, and you need to specify the ingress and/or egress rate limit.

Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.
Egress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.

- Configure a LAG

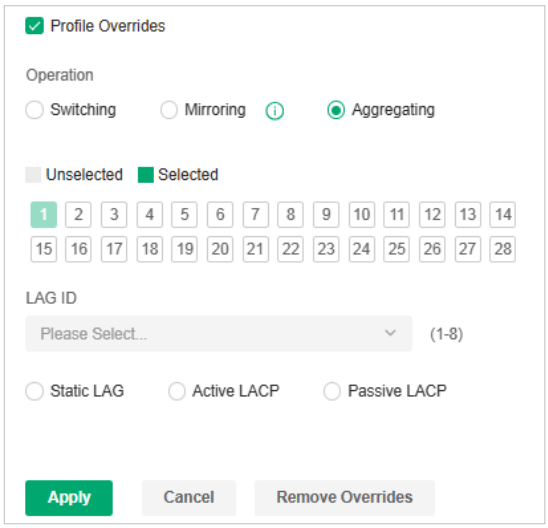
  If you select Aggregating as Operation, you can aggregate multiple physical ports into a logical interface, which can increase link bandwidth and enhance the connection reliability.

  Configuration Guidelines:

  - Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should also be set as LACP mode.
  - Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo and flow control mode.
  - A port cannot be added to more than one LAG at the same time.
  - LACP does not support half-duplex links.
  - One static LAG supports up to eight member ports. All the member ports share the bandwidth evenly. If an active link fails, the other active links share the bandwidth evenly.
  - One LACP LAG supports multiple member ports, but at most eight of them can work simultaneously, and the other member ports are backups. Using LACP protocol, the switches negotiate parameters and determine the working ports. When a working port fails, the backup port with the highest priority will replace the faulty port and start to forward data.
  - The member port of an LAG follows the configuration of the LAG but not its own. Once removed, the LAG member will be configured as the default All profile and Switching operation.
  - The port enabled with Port Security, Port Mirror, MAC Address Filtering or 802.1X cannot be added to an LAG, and the member port of an LAG cannot be enabled with these functions.

  To configure a new LAG, select other ports to be added to the LAG, specify the LAG ID, and choose a LAG type. Click Apply. To discard the modifications, click Remove Overrides and all

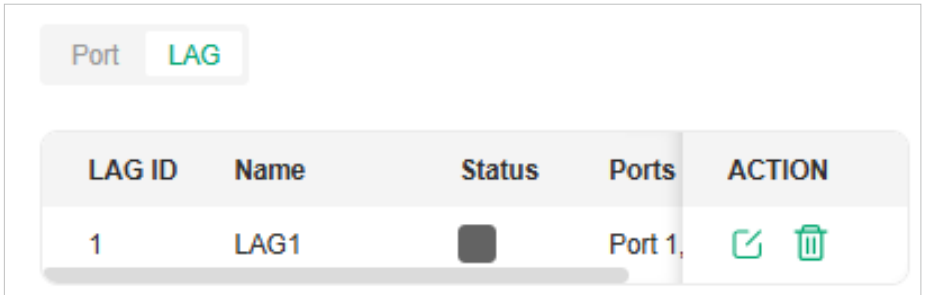
profile configurations become the same as the applied profile. For other parameters, configure them under the LAG tab.



LAG ID	Specify the LAG ID of the LAG. Note that the LAG ID should be unique. The valid value of the LAG ID is determined by the maximum number of LAGs supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value ranges from 1 to 14.
Static LAG	In Static LAG mode, the member ports are added to the LAG manually.
Active LACP/ Passive LACP	LACP extends the flexibility of the LAG configurations. In LACP, the switch uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. Active LACP: In this mode, the port will take the initiative to send LACPDU. Passive LACP: In this mode, the port will not send LACPDU before receiving the LACPDU from the peer end.

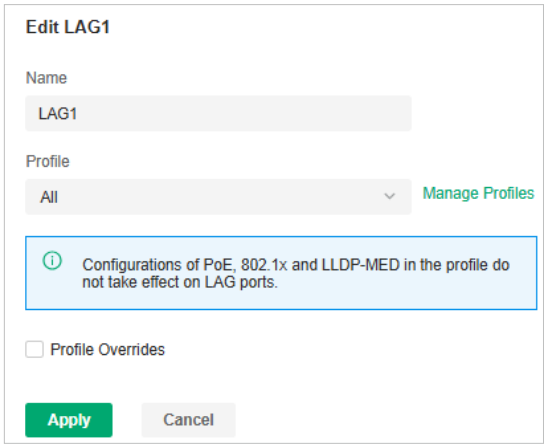
- **LAG**

LAGs (Link Aggregation Groups) are logical interfaces aggregated, which can increase link bandwidth and enhance the connection reliability. You can view and edit the LAGs under the LAG tab. To configure physical ports as a LAG, refer to Configure a LAG.



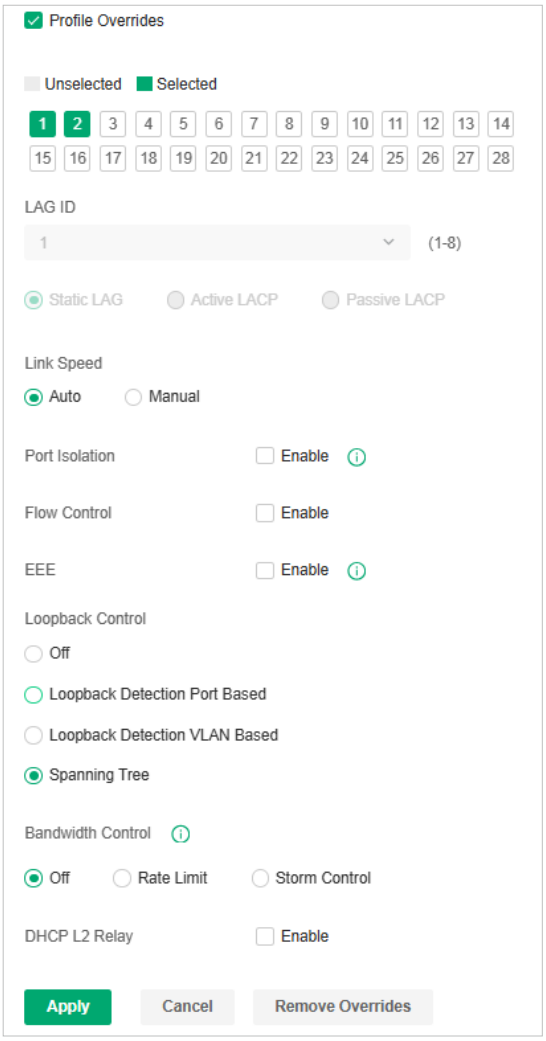
Status	Displays the status in different colors. : The LAG profile is Disable. To enable it, click the edit icon to change the profile. : The port is enabled, but no device or client is connected to it. : The LAG ports are running at 1000 Mbps. : The LAG port are running at 10/100 Mbps.
Ports	Displays the port number of LAG ports.
Profile	Displays the profile applied to the port.
Action	: Click to edit the port name and configure the profile applied to the port. : Click to delete the LAG. Once deleted, the ports will be configured as the default All profile and Switching operation. You can configure the ports under the Port tab.

Click the edit icon to configure the LAG name and the applied profile.



Name	Enter the port name.
Profile	Select the profile applied to the port from the drop-down list. Click Manage Profiles to jump to view and manage profiles. For details, refer to 4. 2 Configure Wired Networks.
Profile Overrides	Click the checkbox to override the applied profile. The parameters to be configured vary in Operation modes.

With Profile Overrides enabled, you can reselect the LAG members and configure the following parameters.



Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.

Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the current port will be removed from the VLAN. Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.

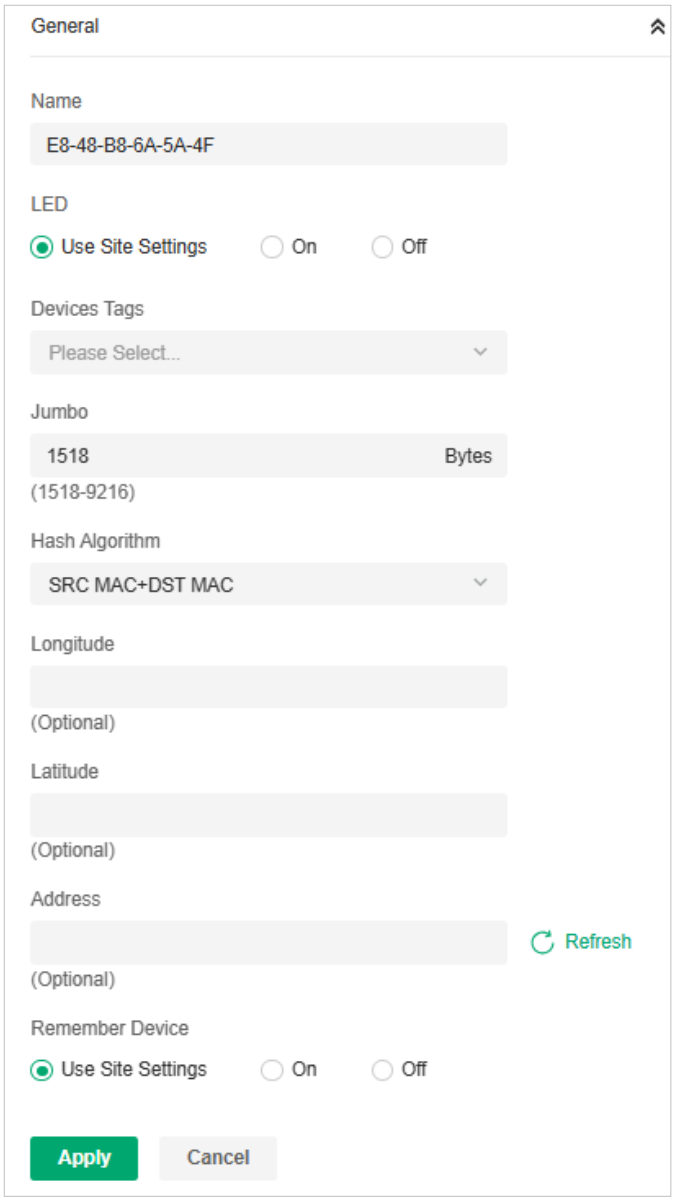
Action	With Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.

Config

In Config, click the sections to configure the features applied to the selected switch(es), including the general settings, services, and networks.

General

In General, you can specify general settings of the switch.

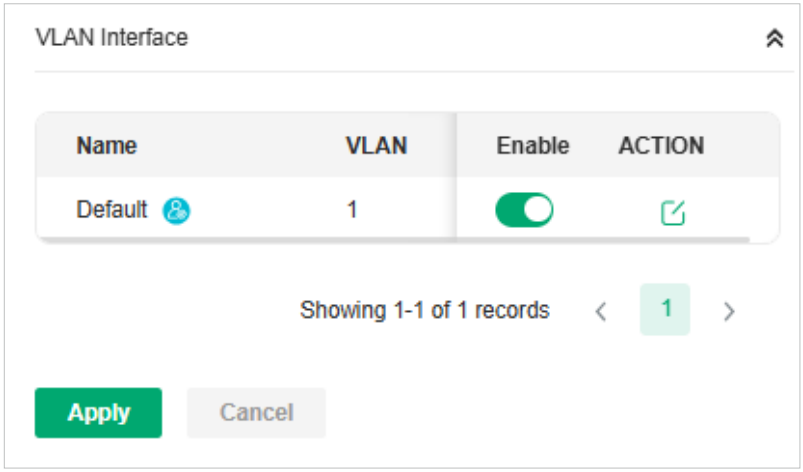


Name	(Only for configuring a single device) Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.
Jumbo	Configure the size of jumbo frames. By default, it is 1518 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.

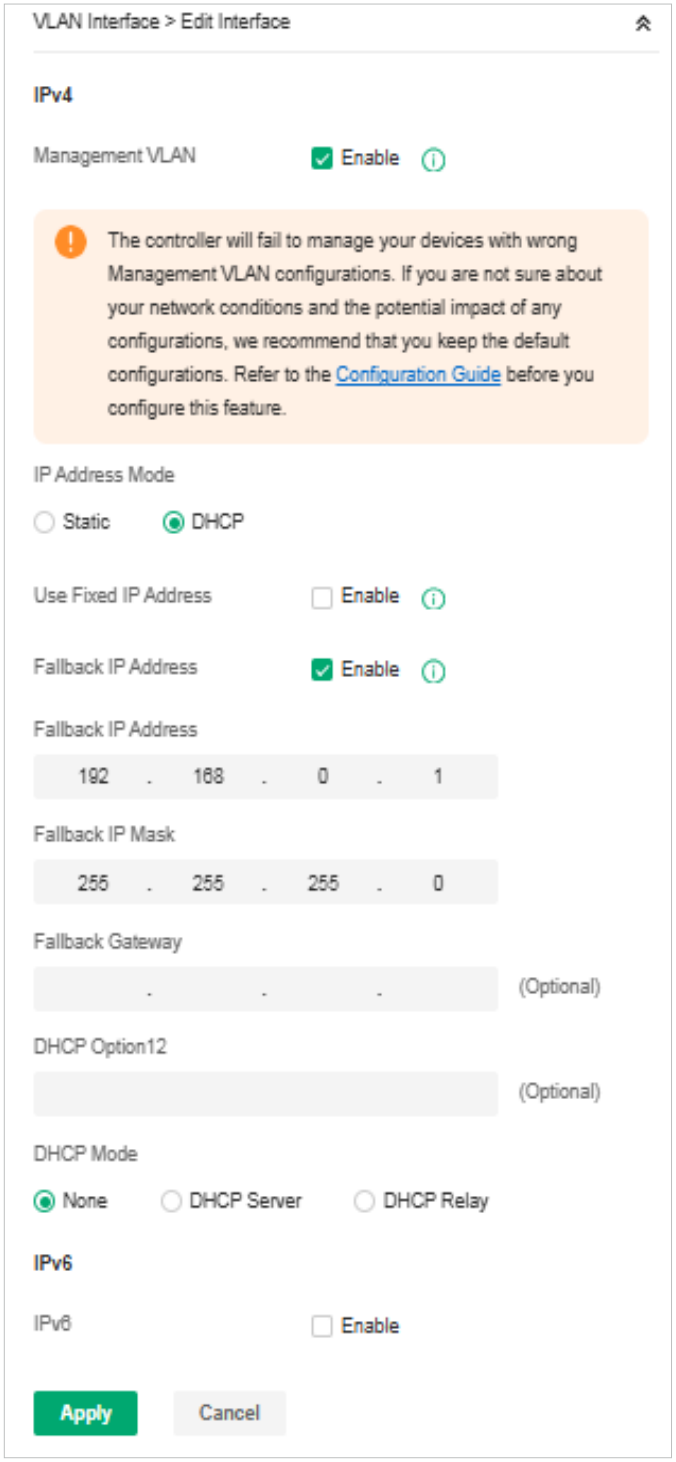
Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to forward the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. SRC MAC: The computation is based on the source MAC addresses of the packets. DST MAC: The computation is based on the destination MAC addresses of the packets. SRC MAC+DST MAC: The computation is based on the source and destination MAC addresses of the packets. SRC IP: The computation is based on the source IP addresses of the packets. DST IP: The computation is based on the destination IP addresses of the packets. SRC IP+DST IP: The computation is based on the source and destination IP addresses of the packets.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.
Remember Device	When enabled, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.

- **VLAN Interface**

In VLAN Interface, you can configure Management VLAN and different VLAN interface for the switch. The general information of the existing VLAN interface are displayed in the table.



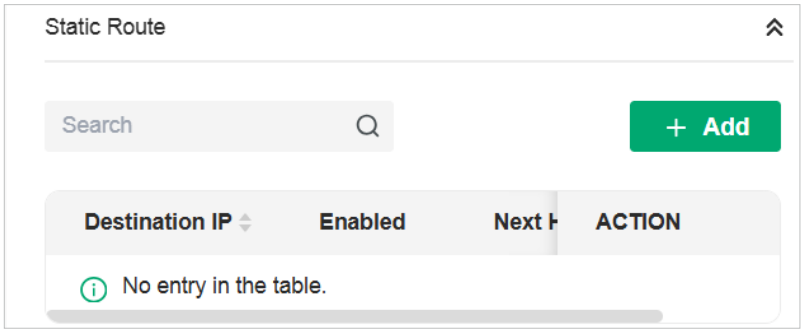
To configure a single VLAN interface, hover the mouse on the entry and click to edit the settings.



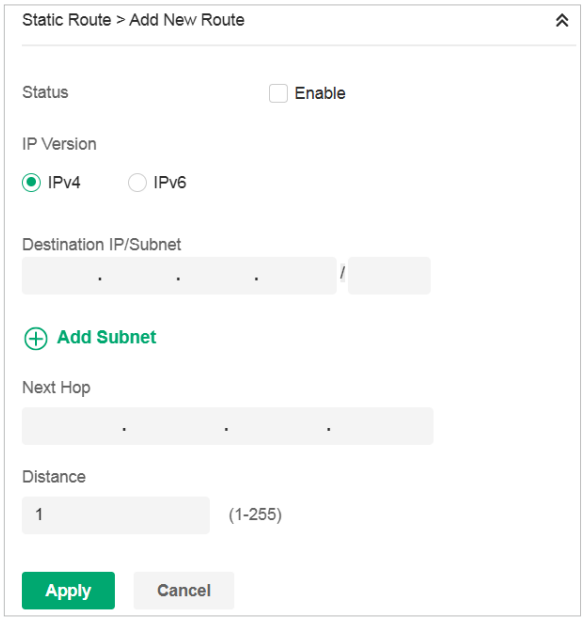
Management VLAN	Click the checkbox if you want to use the VLAN interface as Management VLAN. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
IP Address Mode (when Management VLAN enabled)	Select a mode for the interface to obtain its IP address, and the VLAN will communicate with other networks including VLANs with the IP address. Static: Assign an IP address to the interface manually, specify the IP Address and Subnet Mask for the interface. When the VLAN interface is set as the Management VLAN, it is optional for you to specify the Default Gateway and Primary/Secondary DNS for the interface. DHCP: Assign an IP address to the interface through a DHCP server. When you want to let device use a fixed IP address, enable Use Fixed IP Address and specify the Network and IP Address based on needs. When the VLAN interface is set as the Management VLAN, you can further enable Fallback IP Address, and specify the Fallback IP Address, Fallback IP Mask, and Fallback Gateway (optional). If the VLAN interface fails to get an IP address from the DHCP server, the fallback IP address will be used for the interface.
DHCP Option 12	When DHCP is selected as the IP Address Mode, you can specify the hostname of the DHCP client in the field. The DHCP client will use option 12 to tell the DHCP server their hostname.
DHCP Mode	Select a mode for the clients in the VLAN to obtain their IP address. None: Do not use DHCP to assign IP addresses. DHCP Server: Assign an IP address to the clients through a DHCP server. When DHCP Server is selected, you can specify the DHCP Range, and the IP addresses in the range can be assigned to the clients in the VLAN. Also, it is optional for you to specify the DHCP Option 138, Primary/Seconday DNS, Default Gateway, and Lease Time. DHCP Option 138 informs the DHCP client of the controller's IP address when the client sends a request to the DHCP server, and specify Option 138 as the controller's IP address here. Lease Time decides how long the client can use the assigned IP address. DHCP Relay: It allows clients in the VLAN to obtain IP addresses from a DHCP server ion different subnet. When DHCP Relay is selected, specify the IP address of the DHCP server in Server Address.

Static Route

In Static Route, you can configure entries of static route for the switch. The general information of the existing static route entries are displayed in the table. For an existing static route, click the edit button to modify the settings, and click the delete button to remove it.



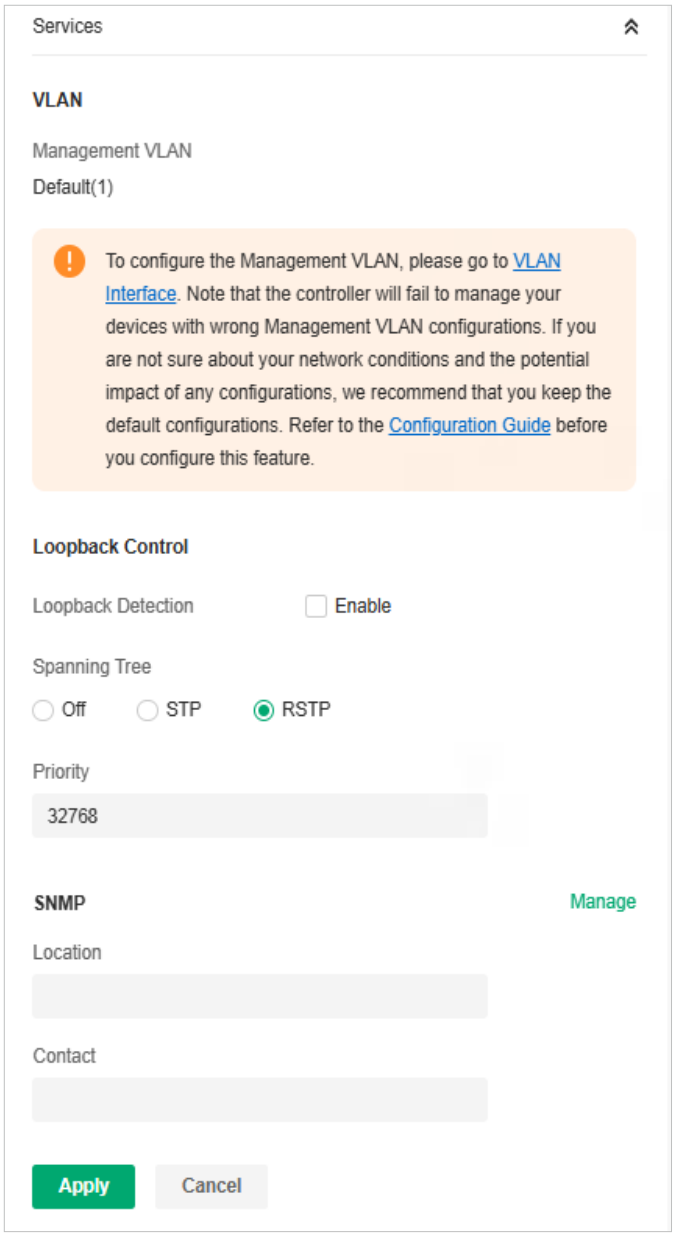
To add a new static route entry, click + Add and configure the parameters.



Status	Click the checkbox to enable or disable the static route.
IP Version	Select IPv4 or IPv6.
Destination IP/Subnet / Destination IP/Prefix Length	When IP Version is IPv4, specify Destination IP/Subnet. When IP Version is IPv6, specify Destination IP/Prefix Length. They identify the network traffic which the Static Route entry controls. You can click + Add Subnet to specify multiple entries or click the trash bin icon to delete them.
Next Hop	Specify the IP address for your devices to forward the corresponding network traffic.
Distance	Specify the priority of a static route. It is used to decide the priority among routes to the same destination. Among routes to the same destination, the route with the lowest distance value will be recorded into the routing table.

Services

In Services, you can configure Management VLAN, Loopback Control and SNMP.

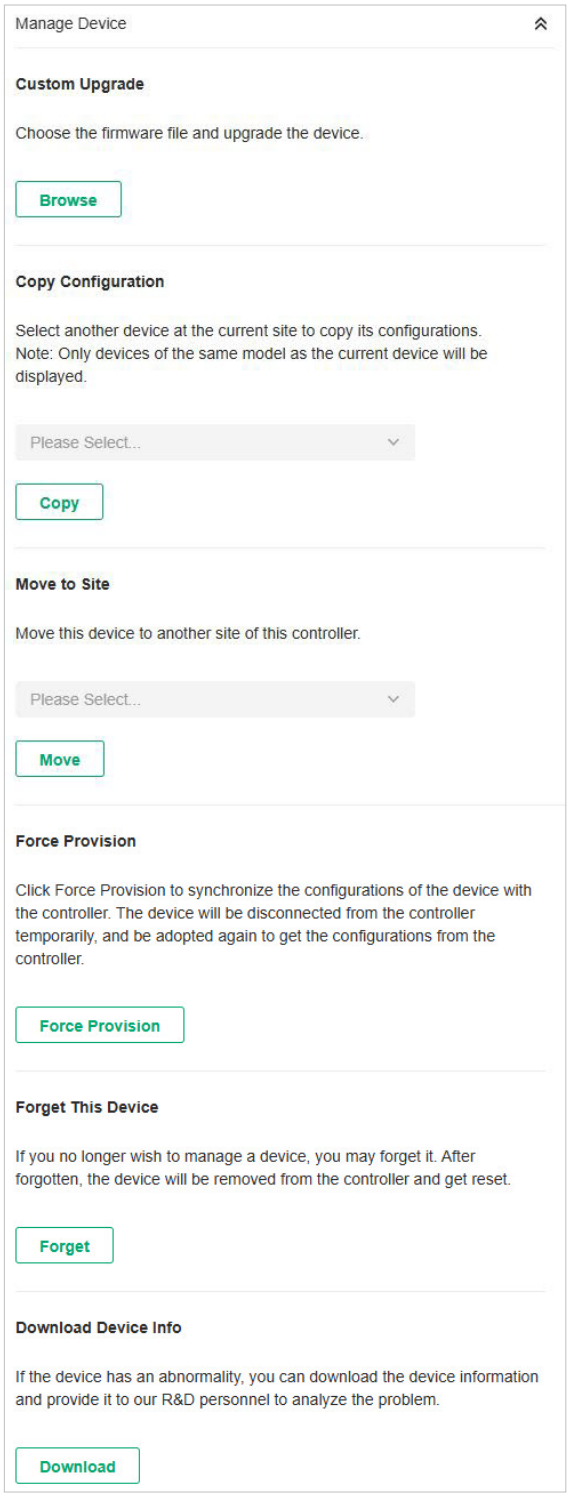


Management VLAN	Display the name of the current Management VLAN. To configure the Management VLAN, please go to Config > VLAN Interface. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.

Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Note that Lopback Detection and Spanning Tree are not available at the same time.
Spanning Tree	Select a mode for Spanning tree. This feature is available only when Loopback Detection is disabled. Off: Disable Spanning Tree on the switch. STP: Enable STP (Spanning Tree Protocal) to prevent loops in the network. STP helps to block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP: Enable RSTP (Rapid Spanning Tree Protocal) to prevent loops in the network. RSTP provides the same features as STP with faster spanning ree convergence. Priority: When STP/RSTP enabled, specify the priority for the swith in Spanning Tree. In STP/RSTP, the switch with the highest priority will be selected as the root of the spanning tree. The switch with the lower value has the higher priority.
SNMP	(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP.

Manage Device

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller and forget the switch.



Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.

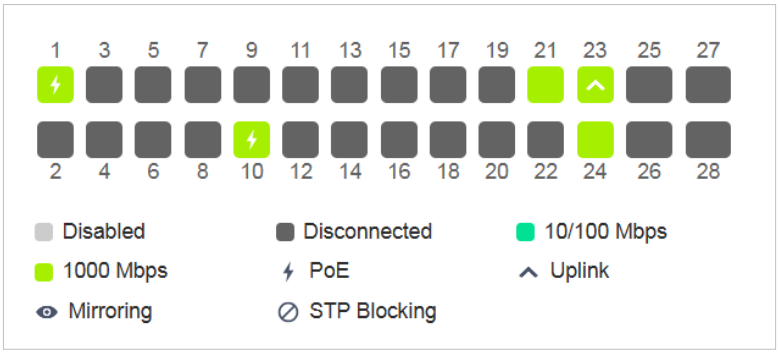
Copy Configuration	Select another device at the current site to copy its configurations.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.

6. 3. 2 Monitor Switches

One panel and four tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Clients, and Statistics.

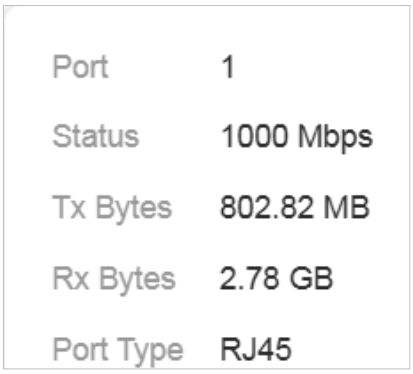
Monitor Panel

The monitor panel displays the switch's ports and uses colors and icons to indicate the connection status and port type. When the switch is pending or disconnected, all ports are disabled.



PoE	A PoE port connected to a powered device (PD).
Uplink	An uplink port connected to WAN.
Mirroring	A mirroring port that is mirroring another switch port.
STP Blocking	A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.

You can hover the cursor over the port icon (except disabled ports) for more details. The displayed information varies due to connection status and port type.



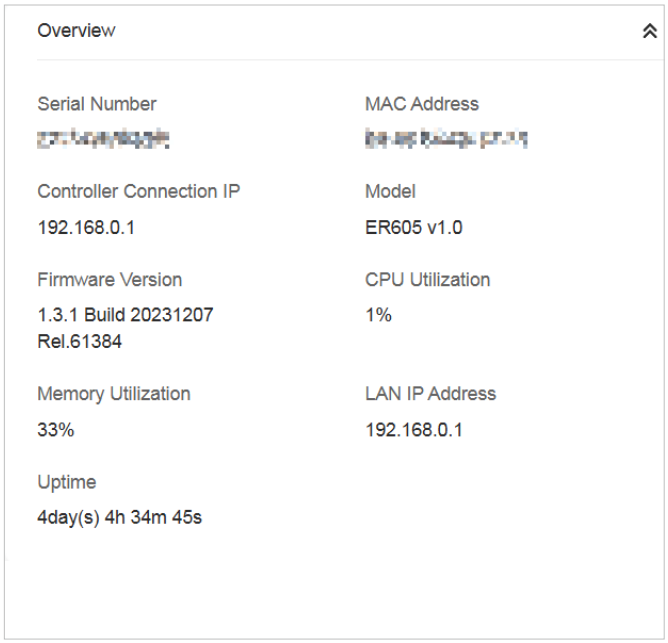
Status	Displays the negotiation speed of the port.
Tx Bytes	Displays the amount of data transmitted as bytes.
Rx Bytes	Displays the amount of data received as bytes.
Profile	Displays the name of profile applied to the port, which defines how the packets in both ingress and egress directions are handled. For detailed configuration, refer to 4. 7 Create Profiles.
PoE Power	Displays the PoE power supply for the PD device.
Uplink	Displays the name of device connected to the uplink port.
Mirroring From	Displays the name of port that is mirrorred.
LAG ID	Displays the name of ports that are aggregated into a logical interface.

Details

In Details, you can view the basic information, traffic information, and radio information of the device to know the device's running status.

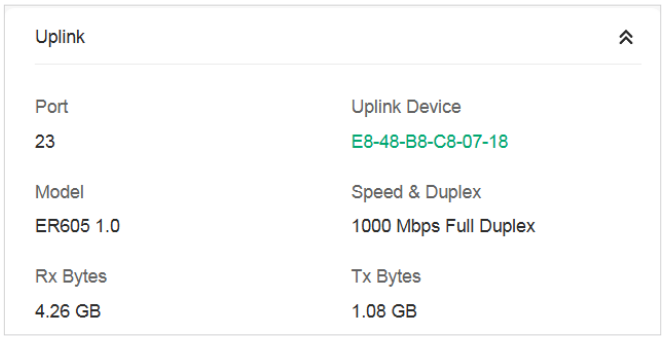
- **Overview**

  In Overview, you can view the basic information of the device. The listed information will be varied due to the device's model and status.



- **Uplink (Only for the switch connected to a controller-managed router/switch in Connected status)**

  Click Uplink to view the uplink information, including the uplink port, the uplink device, the negotiation speed, and transmission rate.



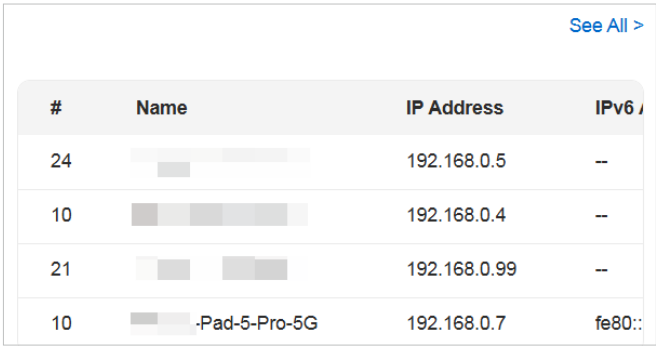
- **Downlink (Only for the switch connected to controller-managed devices in Connected status)**

  Click Downlink to view the downlink information, including the downlink ports, devices name and model as well as negotiation speed.



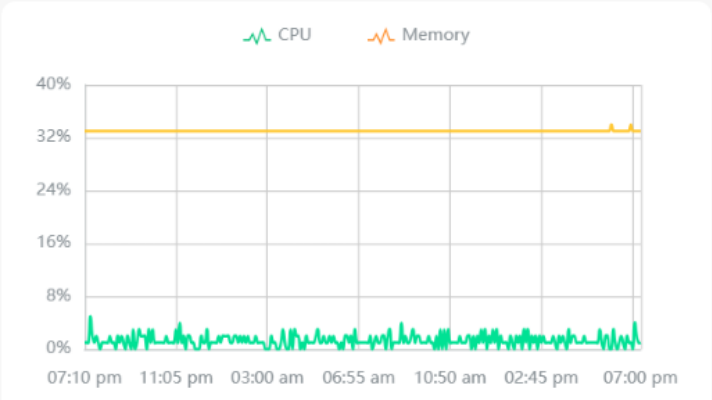
Clients

In Clients, you can view the information of clients connected to the switch, including the client name, IP address and the connected port. You can click the client name to open its Properties window.



Statistics

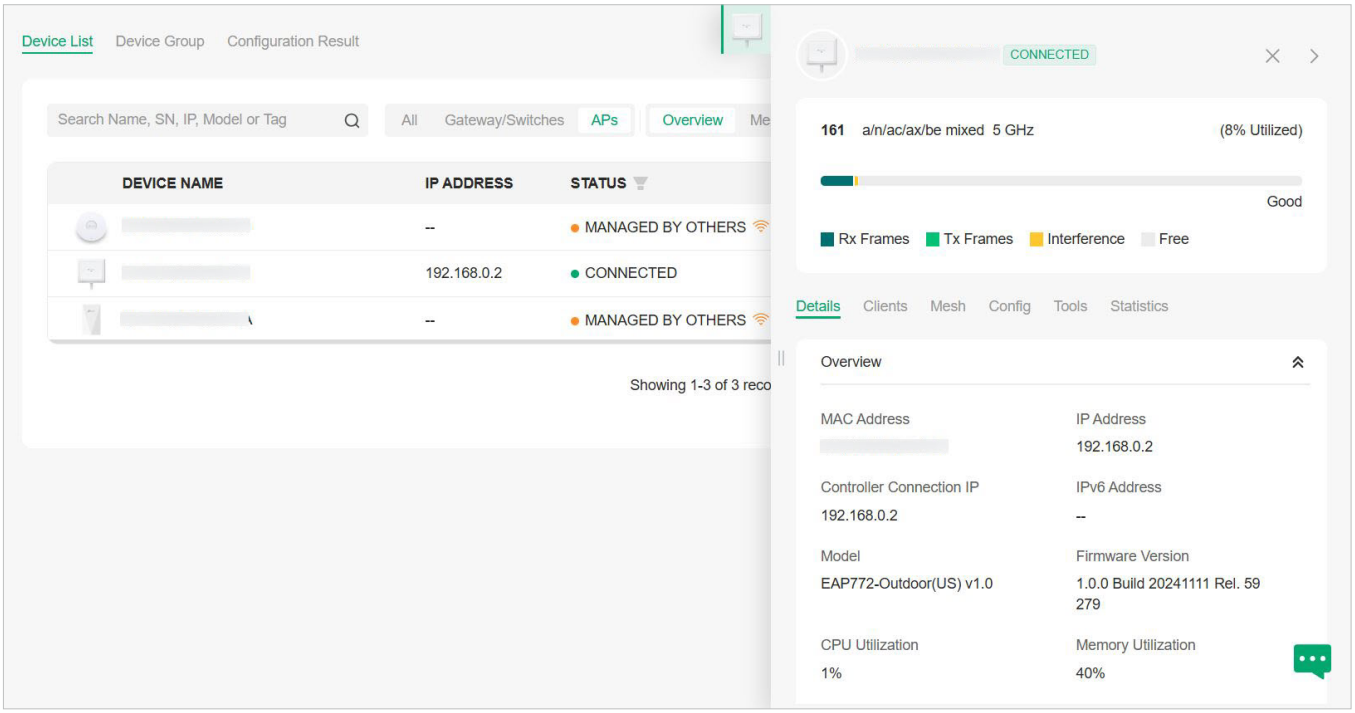
In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in certain period, click the chart to jump to 8. 2 View the Statistics of the Network.



6. 4 Configure and Monitor APs

In the Properties window, you can configure one or some APs connected to the controller and monitor the performance and statistics. Configurations changed in the Properties window will be applied only to the selected AP(s). By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of an AP, or click Batch Action, and then Batch Config to select APs for batch configuration. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Config tab, such as IP, radios, SSID, and VLAN, while other tabs are mainly used to monitor the device.



Note:

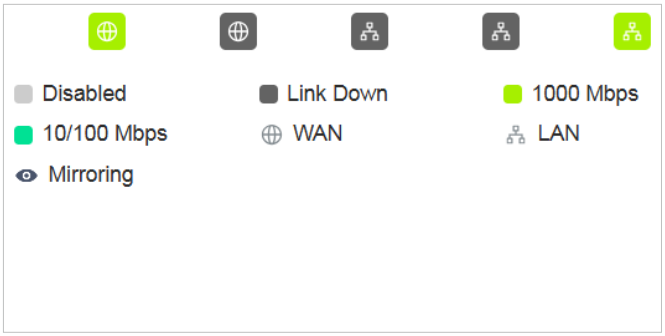
- The available functions in the window vary due to the model and status of the device.
- In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.
- In Batch Config, if some functions, such as the 5 GHz band, are available only on some selected APs, the corresponding configurations will not take effect. To configure them successfully, check the model of selected devices first.

6. 4. 1 Configure APs

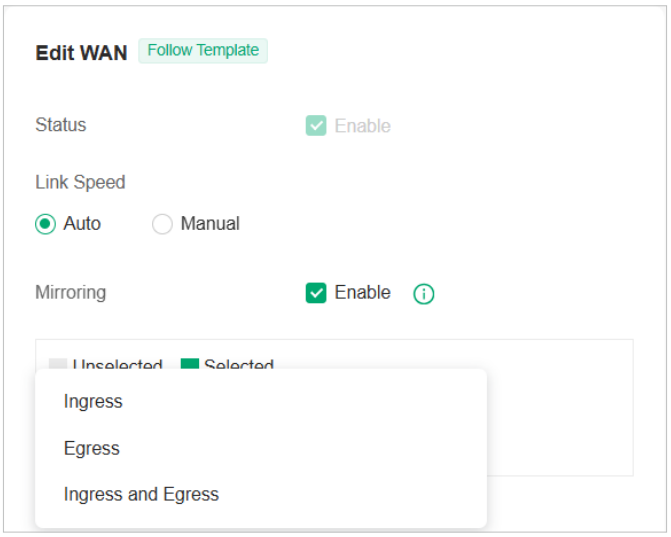
In the Properties window, you can view and configure the ports (only for EAPs with multiple LAN ports) in Ports, and configure the gateway features in Config.

Ports (Only for EAPs with multiple LAN ports)

In Ports, you can view the status and edit settings of the ports.



To configure a port, click the edit button in the Action column.



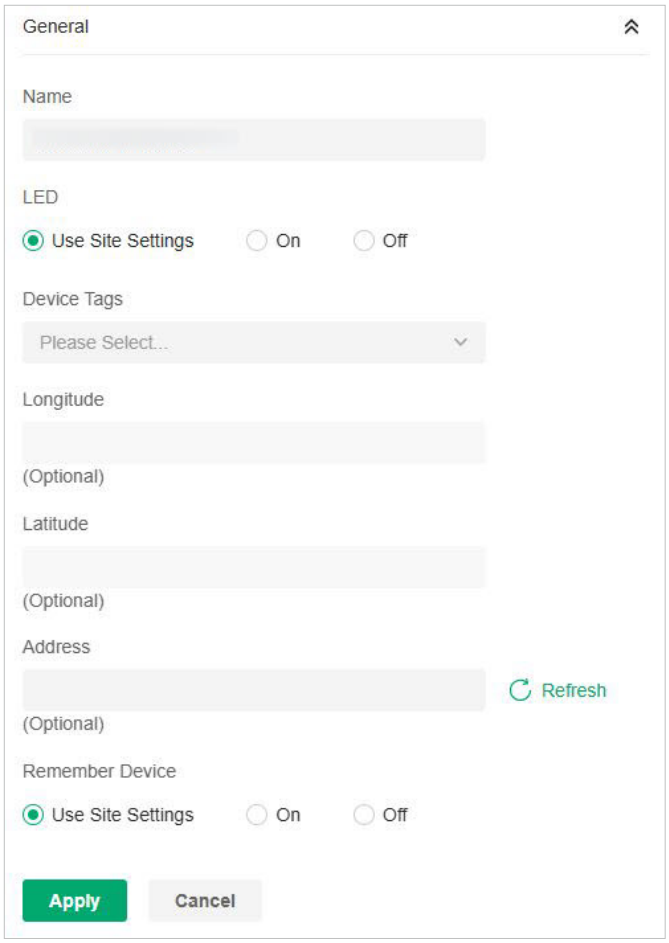
Name	Specify the name of the port.
Status	Click the box to enable or disable the port.
VLAN	Configure the uplink port VLAN corresponding to the SSID. Default: Using untagged transmission. Custom: Enter the PVID (Port VLAN Identifier). When a port receives an untagged frame, the EAP inserts a VLAN tag to the frame based on the PVID before forwarding it.
PoE Out	(Only for APs with the PoE out port) Enable this function to supply power to the connected device on this port.

Config

In the Properties window, click Config and then click the sections to configure the features applied to the selected AP(s).

General

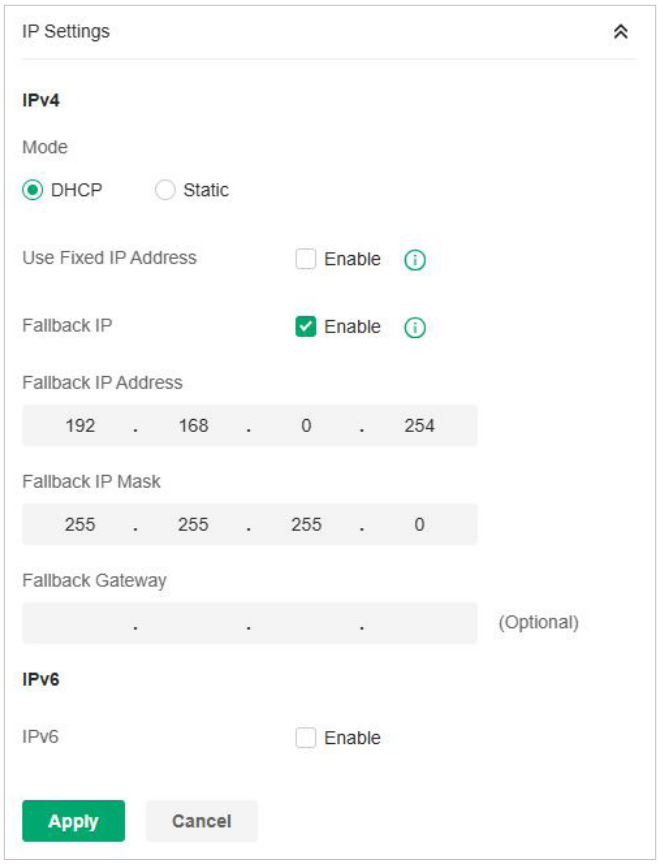
In General, you can specify general settings of the AP.



Name	(Only for configuring a single device) Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to 4. 1. 2 General Config. On/Off: The device's LED will keep on/off.
Wi-Fi Control	(Only for Certain APs) Enable Wi-Fi Control, and it will take effect only when the LED feature is enabled. After enabling Wi-Fi Control, you can press the LED button on the AP to turn on/off the Wi-Fi and LED at the same time.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.
Remember Device	When enabled, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.

- **IP Settings (Only for configuring a single device)**

  In IP Settings, select an IP mode and configure the parameters for the device.



  If you select DHCP as the mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. If you want to let the device use a fixed IP address, you can enable Use Fixed IP Address, and set the network and IP address based on needs. Also, you can set a fallback IP address to hold an IP address in reserve for the situation in which the device fails to get a dynamic IP address. Enable Fallback IP and then set the IP address, IP mask and gateway.

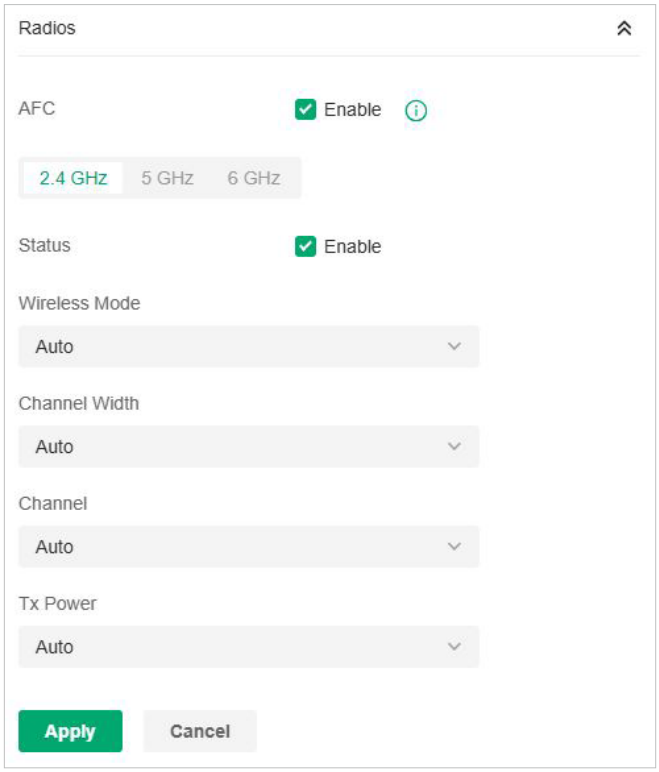
  If you select Static as the mode, set the IP address, IP mask, gateway, and DNS server for the static address.

- **Radios**

  In Radios, you can control how and what type of radio signals the AP emits. Select each frequency band and configure the parameters. Different models support different bands.

Note:

The 6 GHz band is only available for certain devices.



AFC	(For Wi-Fi 7 APs of US version) Enable this feature to use the 6GHz band. The AFC (Automated Frequency Coordination) feature adjusts the transmission power of the 6 GHz band according to your geographic location to meet regulatory requirements.
Status	If you disable the frequency band, the radio on it will turn off.
Wireless Mode	Specify the wireless mode of the band. Different bands have different available options. We recommend using the default value.
Channel Width	Specify the channel width of the band. Different bands have different available options. We recommend using the default value.
Channel	Specify the operation channel of the AP to improve wireless performance. If you select Auto for the channel setting, the AP scans available channels and selects the channel where the least amount of traffic is detected.

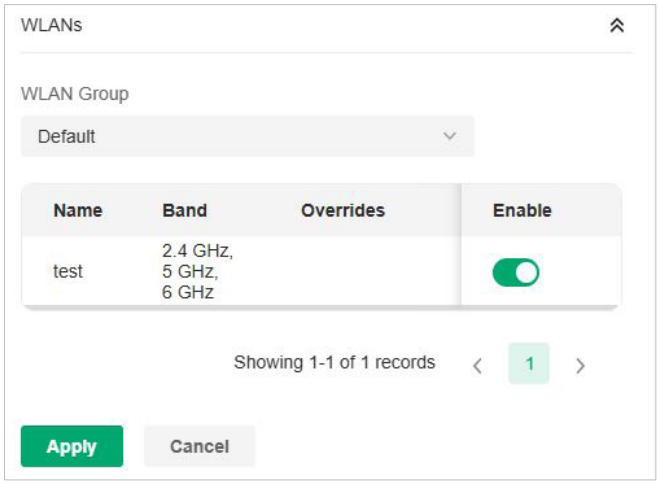
Tx Power	Specify the Tx Power (Transmit Power) in the 4 options: Low, Medium, High and Custom. The actual power of Low, Medium and High are based on the minimum transmit power (Min. Txpower) and maximum transmit power (Max. TxPower), which may vary in different countries and regions. Low: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (round off the value) Medium: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (round off the value) High: Max. TxPower Custom: Specify the value manually.

- **WLANs**

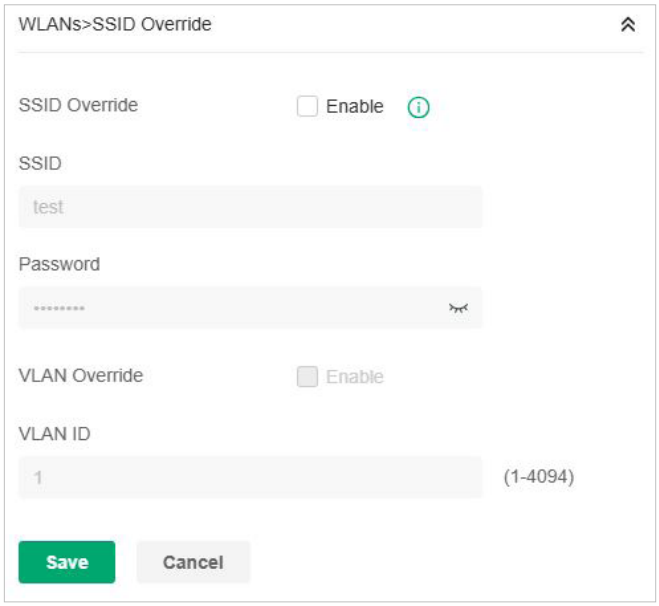
In WLANs, you can apply the WLAN group to the AP and specify a different SSID name and password to override the SSID in the WLAN group. After that, clients can only see the new SSID and use the new password to access the network. To create or edit WLAN groups, refer to 4. 3 Configure Wireless Networks.

Note:

The 6 GHz band is only available for certain devices.



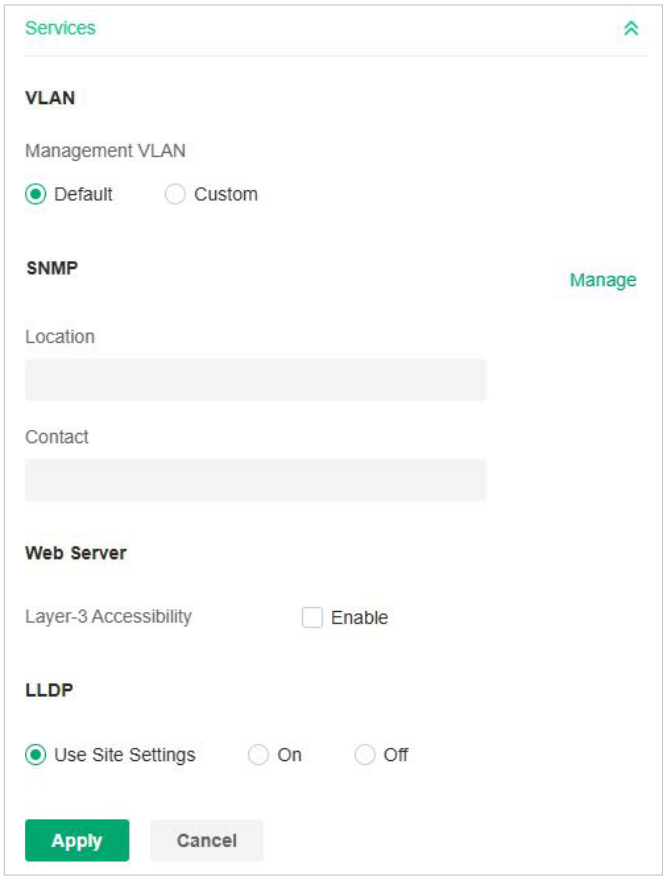
(Only for configuring a single device) To override the SSID, select a WLAN group, click in the entry and then the following page appears.



SSID Override	Enable or disable SSID Override on the AP. If SSID Override enabled, specify the new SSID and password to override the current one.
VLAN	Enable or disable VLAN. If VLAN enabled, enter a VLAN ID to add the new SSID to the VLAN.

Services

In Services, you can enable Management VLAN to protect your network and configure SNMP and web server parameters.

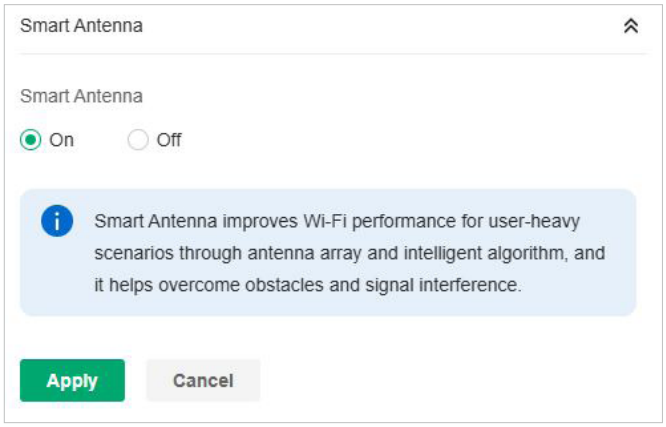


Management VLAN	To configure Management VLAN, create a network in LAN first, and then select it as the management VLAN on this page. For details, refer to 4. 2 Configure Wired Networks. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
SNMP	(Only for configuring a single device) Configure SNMP to write down the Location and Contact detail. You can also click Manage to jump to Settings > Services > SNMP.
Loopback Control	(Only for EAPs with multiple LAN ports) Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or enable Loopback Detection to help detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked.
Layer-3 Accessibility	With this feature enabled, devices from a different subnet can access controller-managed devices.

LLDP	LLDP (Link Layer Discovery Protocol) can help discover devices.

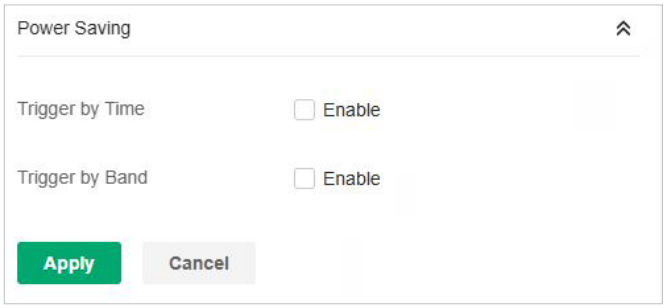
- **Smart Antenna (Only for certain models)**

  In Smart Antenna, you can turn on the function to improve Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm. This help overcome obstacles and signal interference.



- **Power Saving (Only for certain models)**

  In Power Saving, you can trigger the power saving mode reduce the AP's power usage.

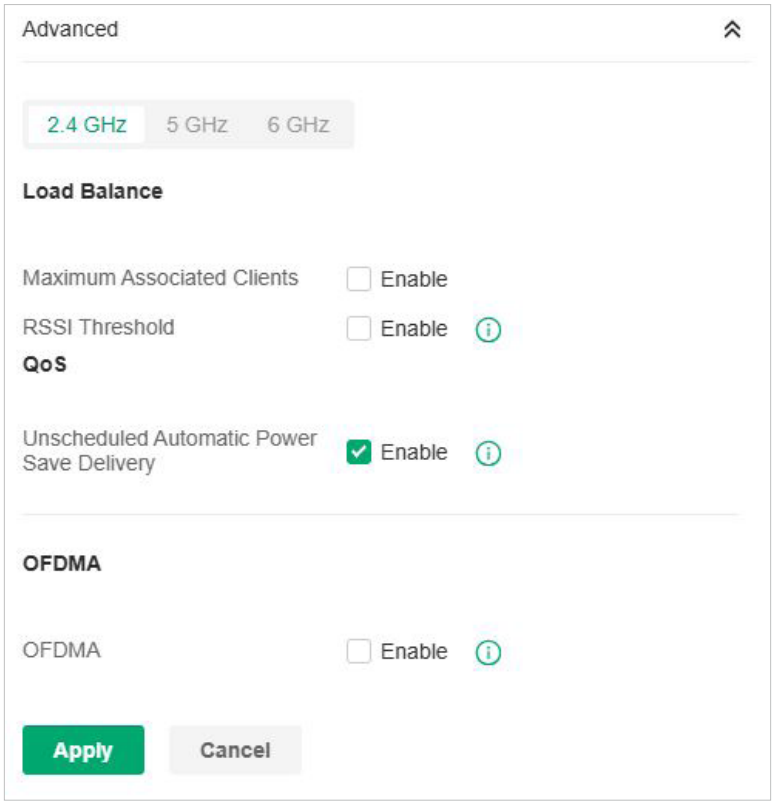


Trigger by Time	With this option enabled, you can specify the start and end time to enable power saving every day within the time period.
Trigger by Band	With this option enabled, you can specify the bands and idle duration to enable power saving when there are no connections for the specified duration on the bands.

- **Advanced**

  In Advanced, configure Load Balance and QoS to make better use of network resources. Load Balance can control the client number associated to the AP, while QoS can optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media.

Select each frequency band and configure the following parameters and features.

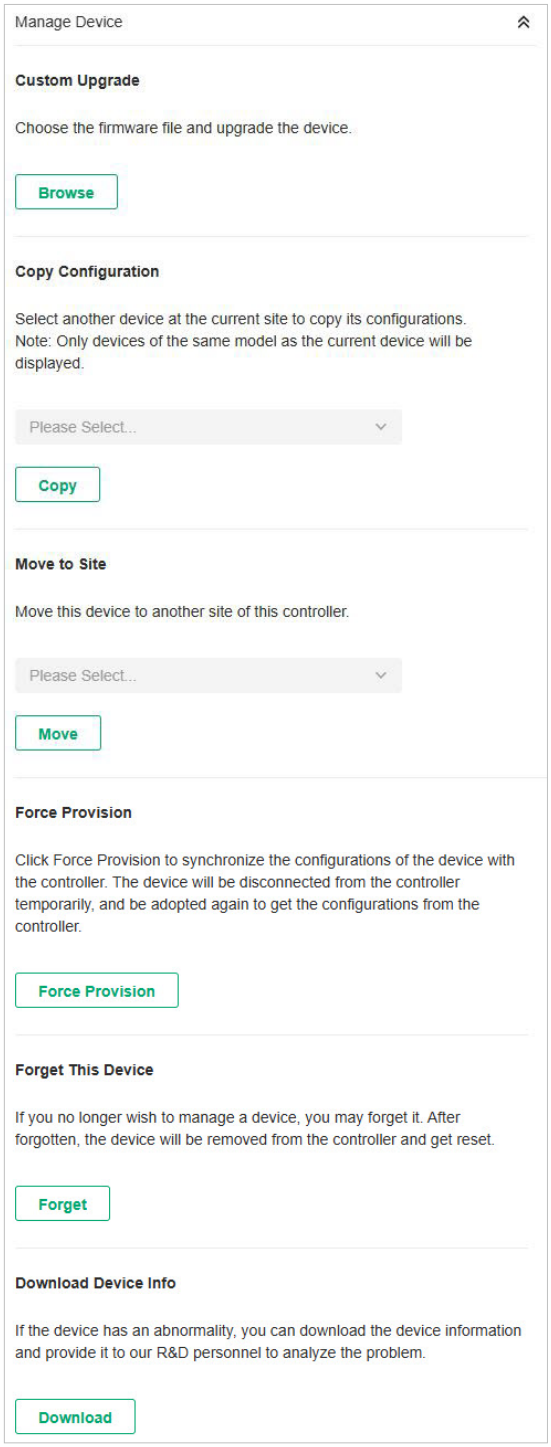


Max Associated Clients	Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the AP will disconnect those with weaker signals to make room for other clients requesting connections.
RSSI Threshold	Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If the client's signal strength is weaker than the threshold, the client will lose connection with the AP.
ETH VLAN/ETH2 VLAN/ ETH3 VLAN	(Only for APs with multiple LAN ports) Enable this function and add the corresponding AP's LAN port to the VLAN specified here. Then the hosts connected to this AP can only communicate with the devices in this VLAN.
ETH3 PoE Out	(Only for APs with the PoE out port) Enable this function to supply power to the connected device on this port.
Wi-Fi Multimedia (WMM)	With WMM enabled, the AP maintains the priority of audio and video packets for better media performance.
No Acknowledgment	Enable this function to specify that the APs will not acknowledge frames with QoS No Ack. Enabling No Acknowledgment can bring more efficient throughput, but it may increase error rates in a noisy Radio Frequency (RF) environment.
Unscheduled Automatic Power Save Delivery	When enabled, this function can greatly improve the energy-saving capacity of clients.
Non-PSC Channels	(Only for AP supporting 6GHz band) When enabled, the AP can use both non-PSC channels and PSC channels. Note that some clients may not discover 6GHz networks using non-PSC channels.

OFDMA	(Only for AP supporting 802.11 ax or later standards) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improves speed and efficiency. Note that the benefits of OFDMA can be fully enjoyed only when the clients support OFDMA.

Manage Device

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller and forget the AP.



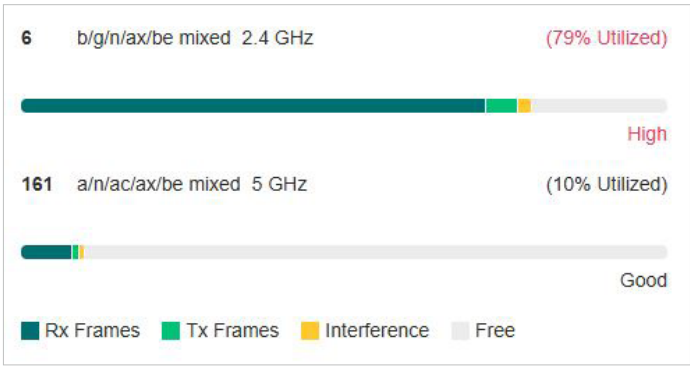
Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.
Copy Configuration	Select another device at the current site to copy its configurations.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget this AP	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.

6. 4. 2 Monitor APs

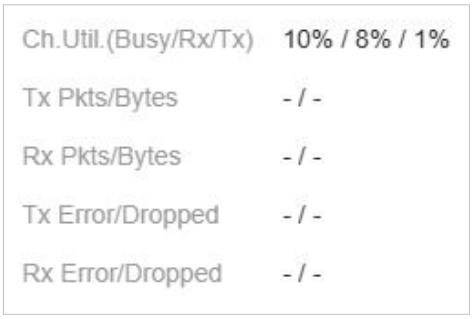
One panel and four tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Clients, Mesh, Tools, and Statistics.

Monitor Panel

The monitor panel illustrates the active channel information on each radio band, including the AP's operation channel, radio mode and channel utilization. Four colors are used to indicate the percentage of Rx Frames (blue), Tx Frames (green), Interference (orange), and Free bandwidth (gray).



You can hover the cursor over the channel bar for more details.



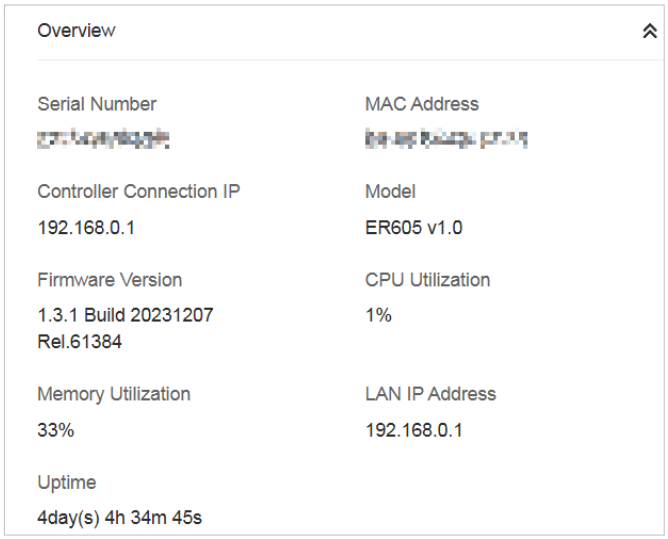
Ch.Util.(Busy/Rx/Tx)	Displays channel utilization statistics. **Busy**: Displays the sum of Tx, Rx, and also non-WiFi interference, which indicates how busy the channel is. **Rx**: Indicates how often the radio is in active receive mode. **Tx**: Indicates how often the radio is in active transmit mode.
Tx Pkts/Bytes	Displays the amount of data transmitted as packets and bytes.
Rx Pkts/Bytes	Displays the amount of data received as packets and bytes.
Tx Error/Dropped	Displays the percentage of transmit packets that have errors and the percentage of packets that were dropped.
Rx Error/Dropped	Displays the percentage of receive packets that have errors and the percentage of packets that were dropped.

Details

In Details, you can view the basic information, traffic information, and radio information of the device to know the device's running status.

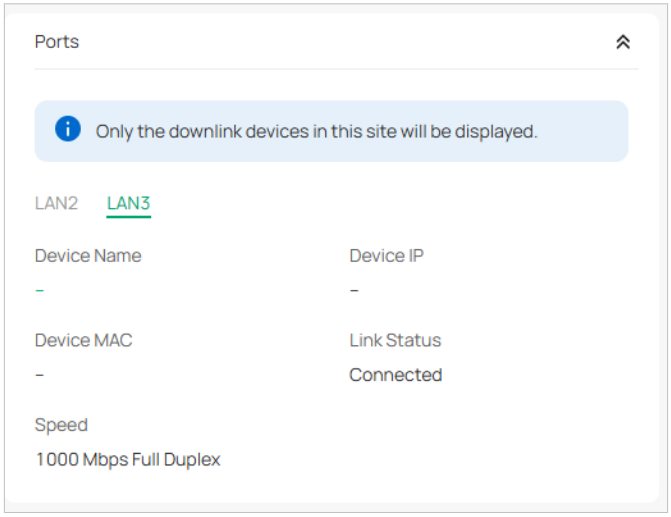
- **Overview**

  In Overview, you can view the basic information of the device. The listed information varies due to the device's status.



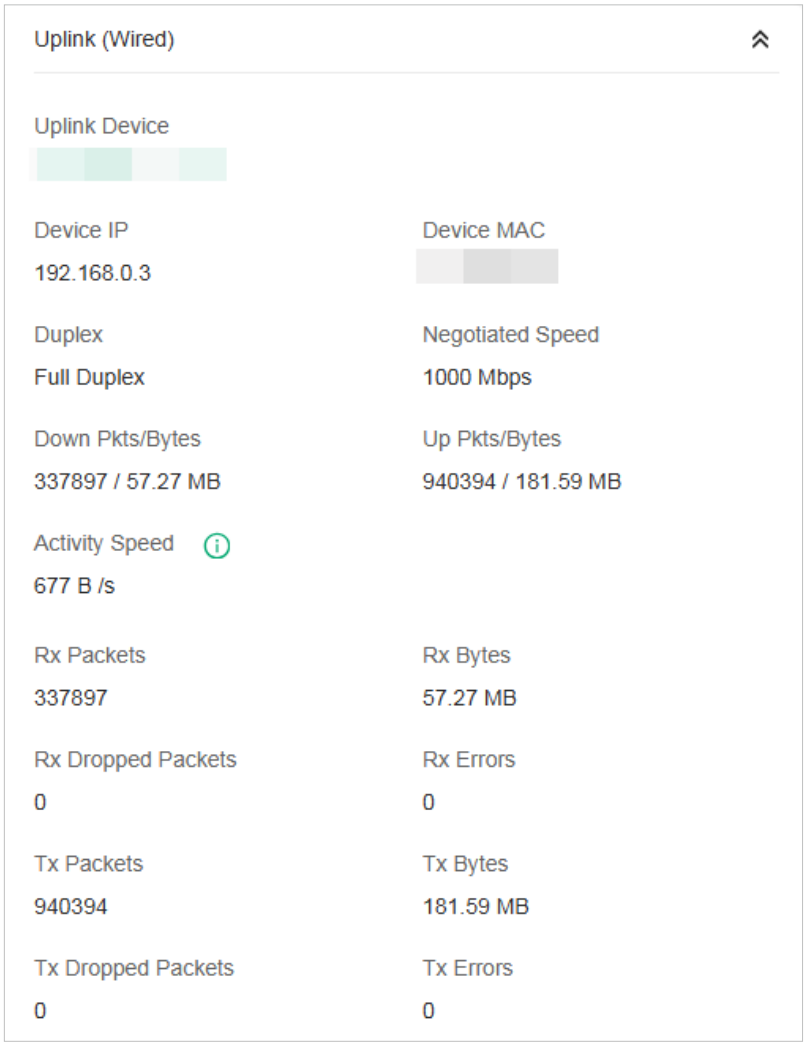
- **LAN (Only for devices in the Connected status)**

  Click LAN to view the traffic information of the LAN port, including the total number of packets, the total size of data, the total number of packets loss, and the total size of error data in the process of receiving and transmitting data.



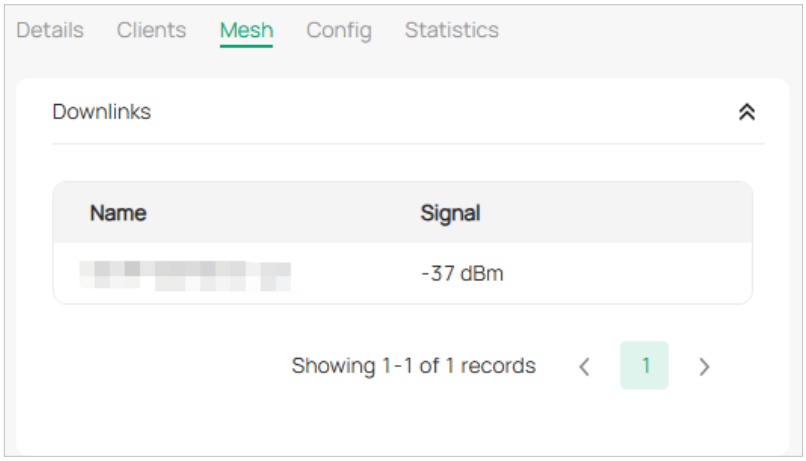
- **Uplink (Only for devices in the Connected status)**

  Click Uplink to view the traffic information related to the uplink device.



- **Downlink (Only for devices in the Connected status)**

  Click Downlink to view the information related to the downlink devices.

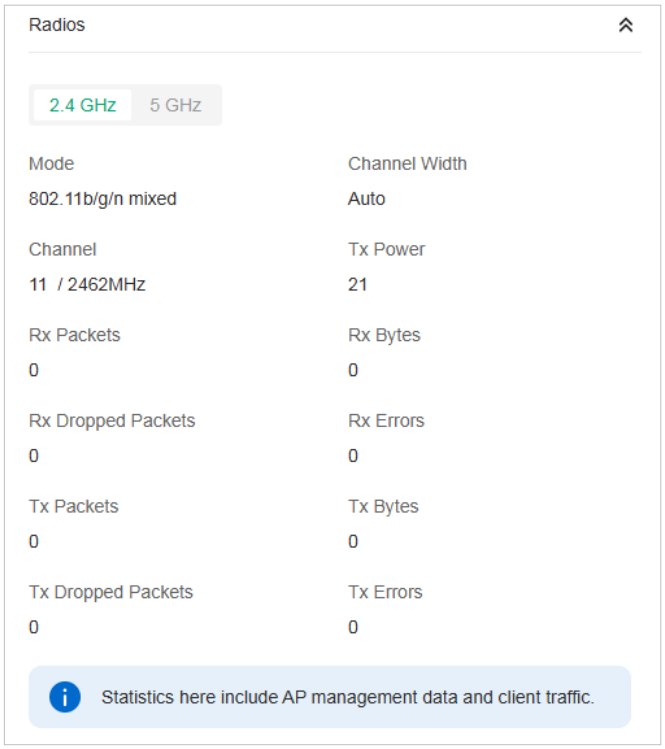


- **Radios (Only for devices in the Connected status)**

  Click Radio to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. You can also view parameters of receiving/transmitting data on each radio band.

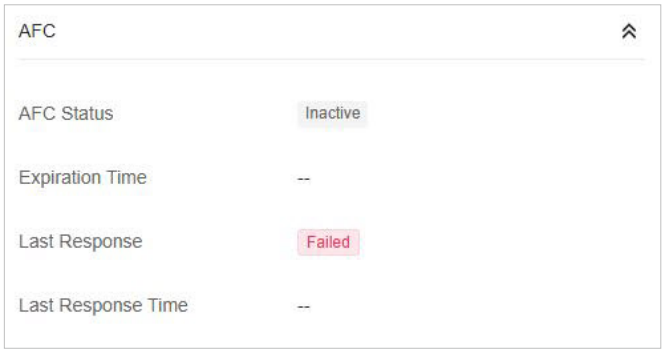
  Note:

  The 6 GHz band is only available for certain devices.



- **AFC (Only for Wi-Fi 7 APs of US version)**

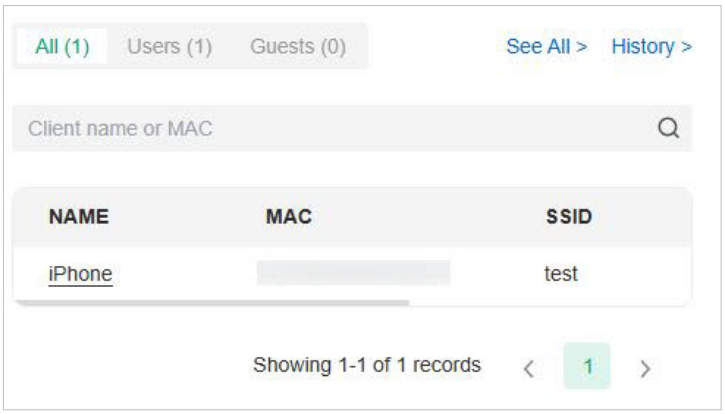
  Click AFC to view the AFC information, including the AFC status, expiration time, last response, and last response time.



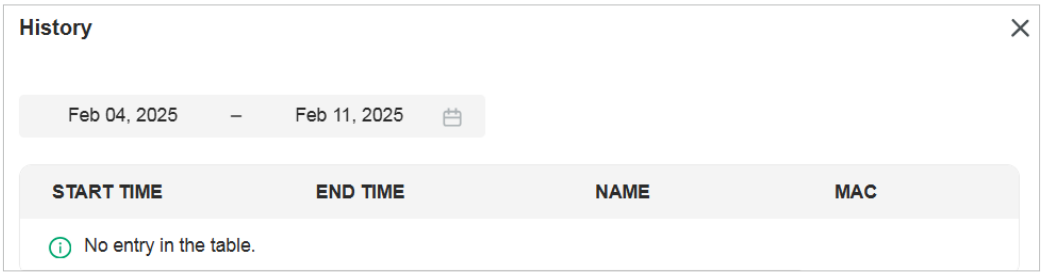
Clients

In Clients, you can view the information of users and guests connecting to the AP, including client name, MAC address and the connected SSID. Users are clients connected to the AP's SSID with Guest

Network disabled, while Guests are clients connected to that with Guest Network enabled. You can click the client name to open its Properties window.



Click History to view the client history. In the History page, you can specify the date or time period to view the clients connected during specific time, and click Export to download the list of clients.



Mesh (Only for pending/connected/isolated devices supporting Mesh)

Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5 GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the APs can be configured and managed in the controller in the same way as wired APs. Meanwhile, because of the ability to self-organize and self-configure, mesh also can efficiently reduce the configuration.

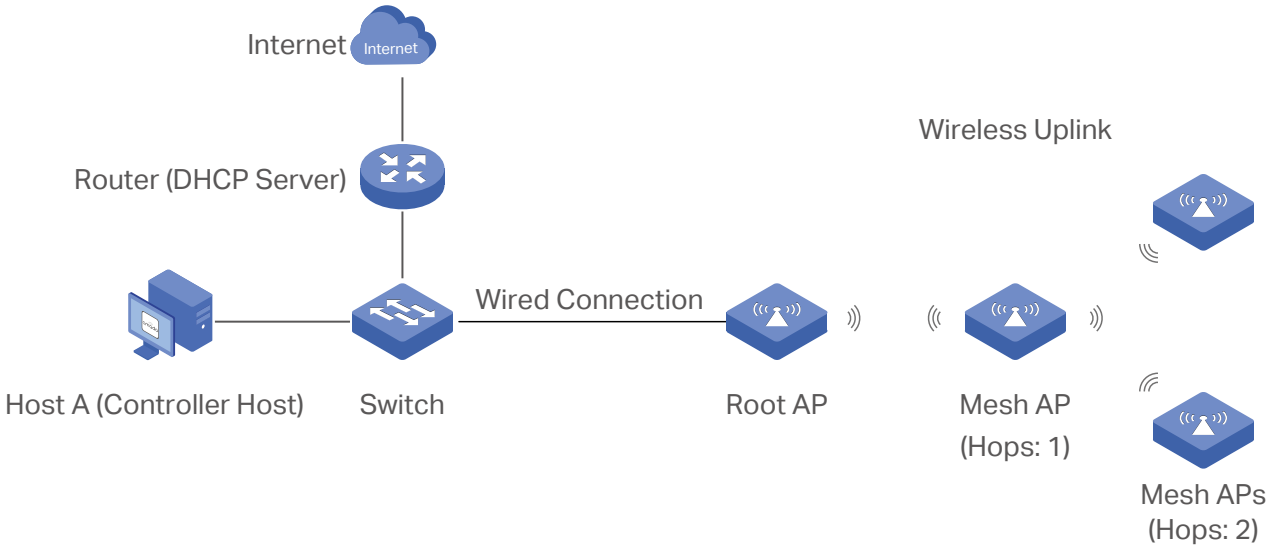
Note that only certain AP models support Mesh, and the APs should be in the same site to establish a Mesh network.

To understand how mesh can be used, the following terms used in the Controller will be introduced:

Root AP	The AP is managed by the Controller with a wired data connection that can be configured to relay data to and from mesh APs (downlink AP).
Isolated AP	When the AP which has been managed by the Controller before connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.
Mesh AP	An isolated AP will become a mesh AP after establishing a wireless connection to the AP with network access.

Uplink AP/Downlink AP	Among mesh APs, the AP that offers the wireless connection for other APs is called uplink AP. A Root AP or an intermediate AP can be the uplink AP. And the AP that connects to the uplink AP is called downlink AP. An uplink AP can offer direct wireless connection for 4 downlink APs at most.
Wireless Uplink	The action that a downlink AP connects to the uplink AP.
Hops	In a deployment that uses a root AP and more than one level of wireless uplink with intermediate APs, the uplink tiers can be referred to by root, first hop, second hop and so on. The hops should be no more than 3.

A common mesh network is shown as below. Only the root AP is connected by an Ethernet cable, while other APs have no wired data connection. Mesh allows the isolated APs to communicate with pre-configured root AP on the network. Once powered up, factory default or unadopted APs can detect the AP in range and make itself available for adoption in the controller.



After all the APs are adopted, a mesh network is established. The APs connected to the network via wireless connection also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

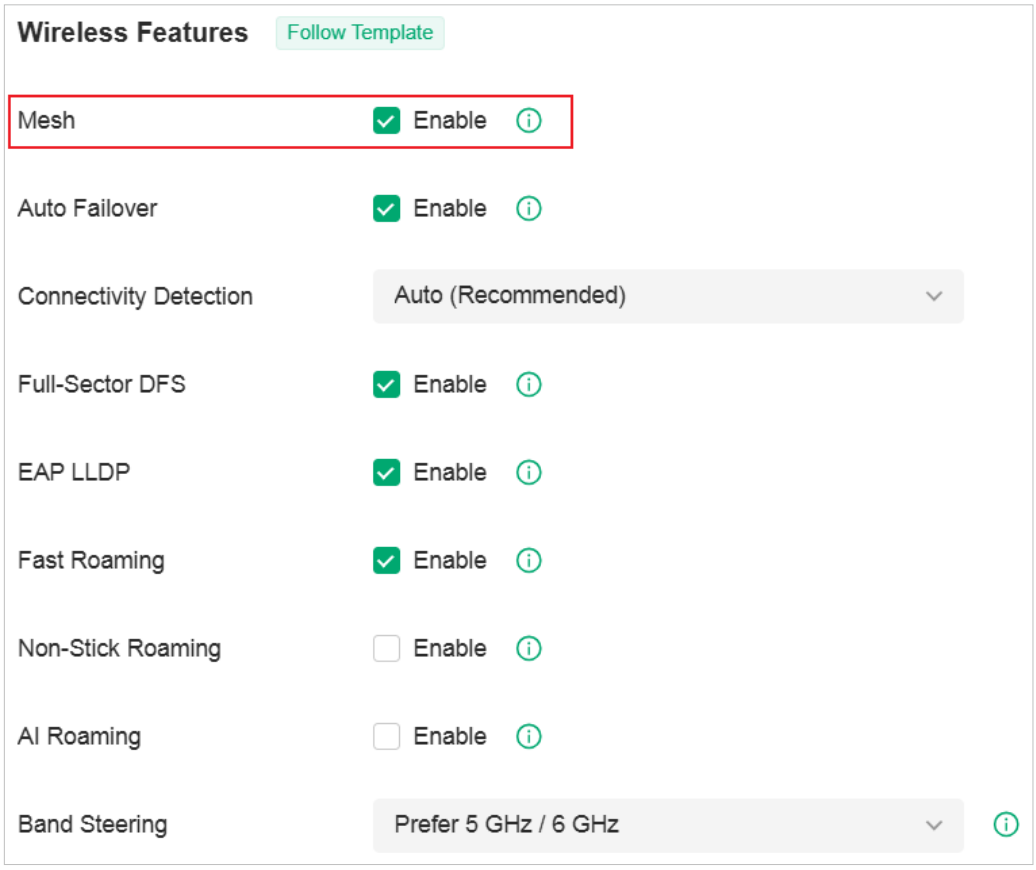
To build a mesh network, follow the steps below:

1) Enable Mesh function.

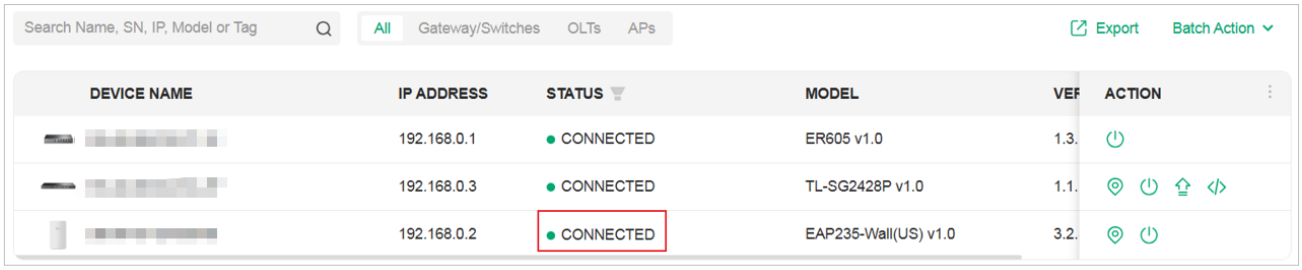
2) Adopt the Root AP.

3) Set up wireless uplink by adopting APs in Pending(Wireless) or Isolated status.

1. Go to Settings > Site Settings to make sure Mesh is enabled.

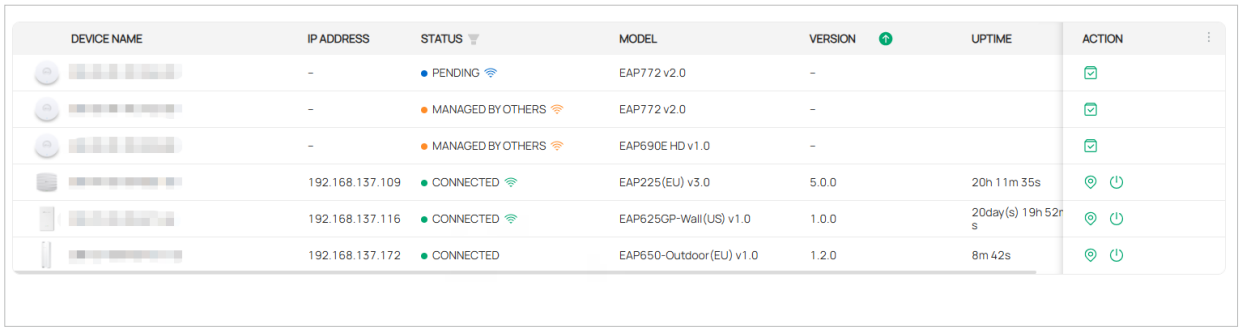


2. Go to Devices to make sure that the Root AP has been adopted by the controller. The status of the Root AP is Connected.



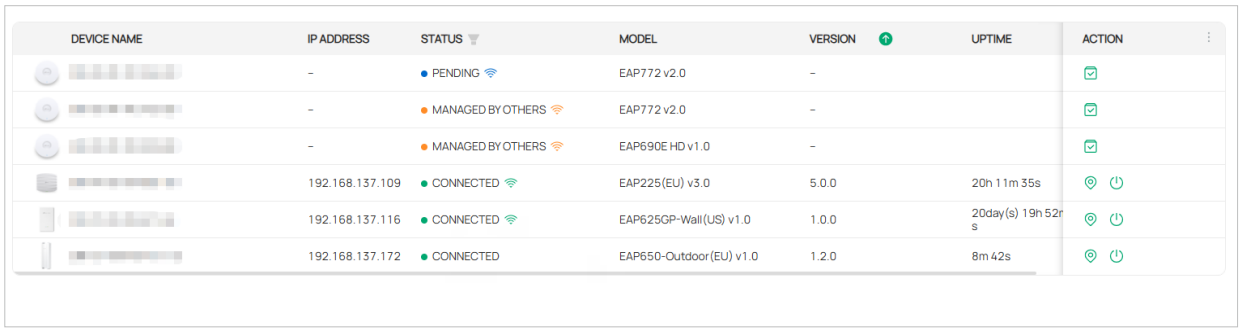
3. Install the AP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The APs that is waiting for Wireless Uplink includes two cases: factory default APs and APs that has been managed by the controller before. Go to Devices to adopt an AP in Pending (Wireless) status or link an isolated AP.

1) For the factory default AP, after powering on the device, the AP will be in Pending (Wireless) status in the Devices list of the controller. Click the adopt icon in the Action column to adopt the AP.

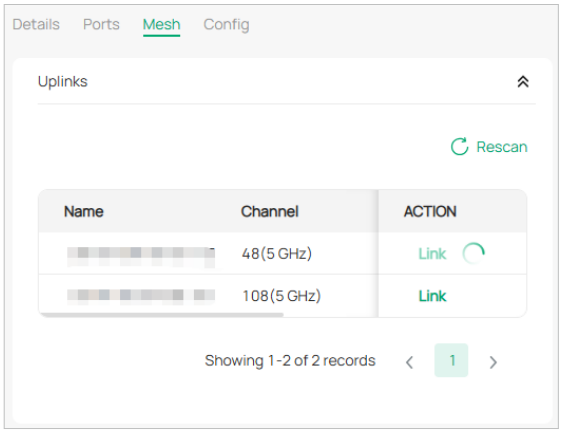


After adoption begins, the status of Pending (Wireless) AP will become Adopting (Wireless) and then Connected (Wireless). It should take roughly 2 minutes to show up Connected (Wireless) on your controller.

2) For the AP that has been managed by the Controller before and cannot reach the gateway, it goes into Isolated status in the Devices list when it is discovered by controller again. Click the adopt icon in the Action column to connect the Uplink AP.

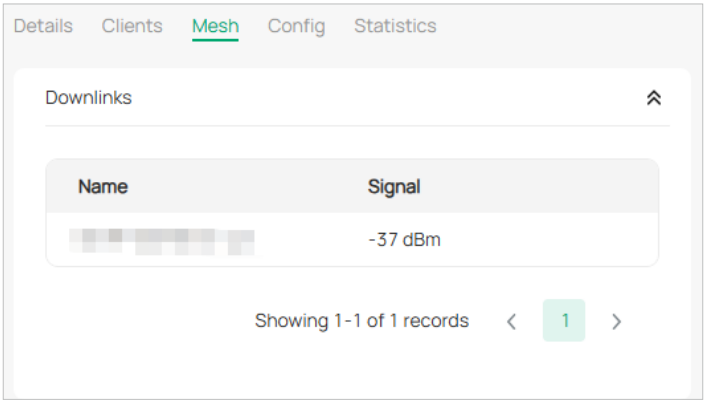


The following page will be shown as below, click Link to connect the Uplink AP.

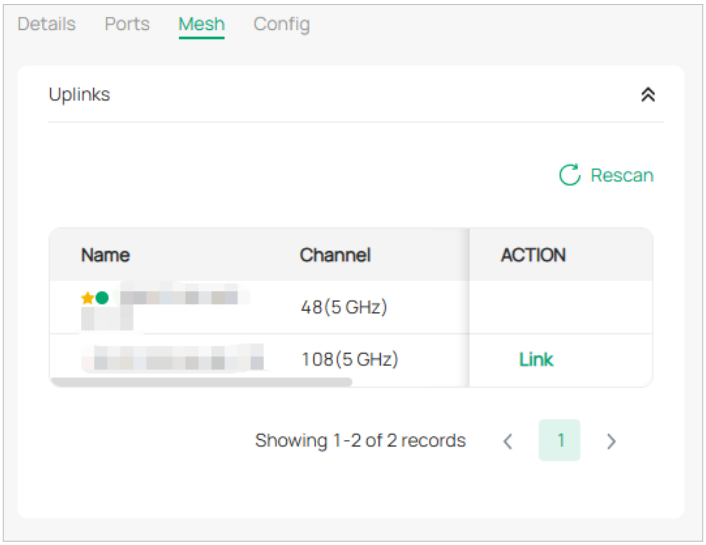


Once mesh network has been established, the AP can be managed by the controller in the same way as a wired AP. You can click the AP's name in the Devices list, and click Mesh to view and configure the mesh parameters of the AP in the Properties window.

In Mesh, if the selected AP is an uplink AP, this page lists all downlink APs connected to the AP.



If the selected AP is a downlink AP, this page lists all available uplink APs and their channel, signal strength, hop, and the number of downlink APs. You can click Rescan to search the available uplink APs and refresh the list, and click Link to connect the uplink AP and build up a mesh network.



★	The icon appears before the priority uplink AP of the downlink AP. If you want to set another AP as the priority AP, click Link in Action column.
●	The icon appears before the current uplink AP of the downlink AP.

Tips:

- You can manually select the priority uplink AP that you want to connect in the uplink AP list. To build a mesh network with better performance, we recommend that you select the uplink AP with the strongest signal, least hop and least downlink AP.
- Auto Failover is enabled by default, and it allows the controller automatically select an uplink AP for the isolated AP to establish Wireless Uplink. And the controller will automatically select a new uplink AP for the mesh APs when the original uplink fails. For more details about Mesh global configurations, refer to the Mesh feature in 4. 1. 2 General Config.

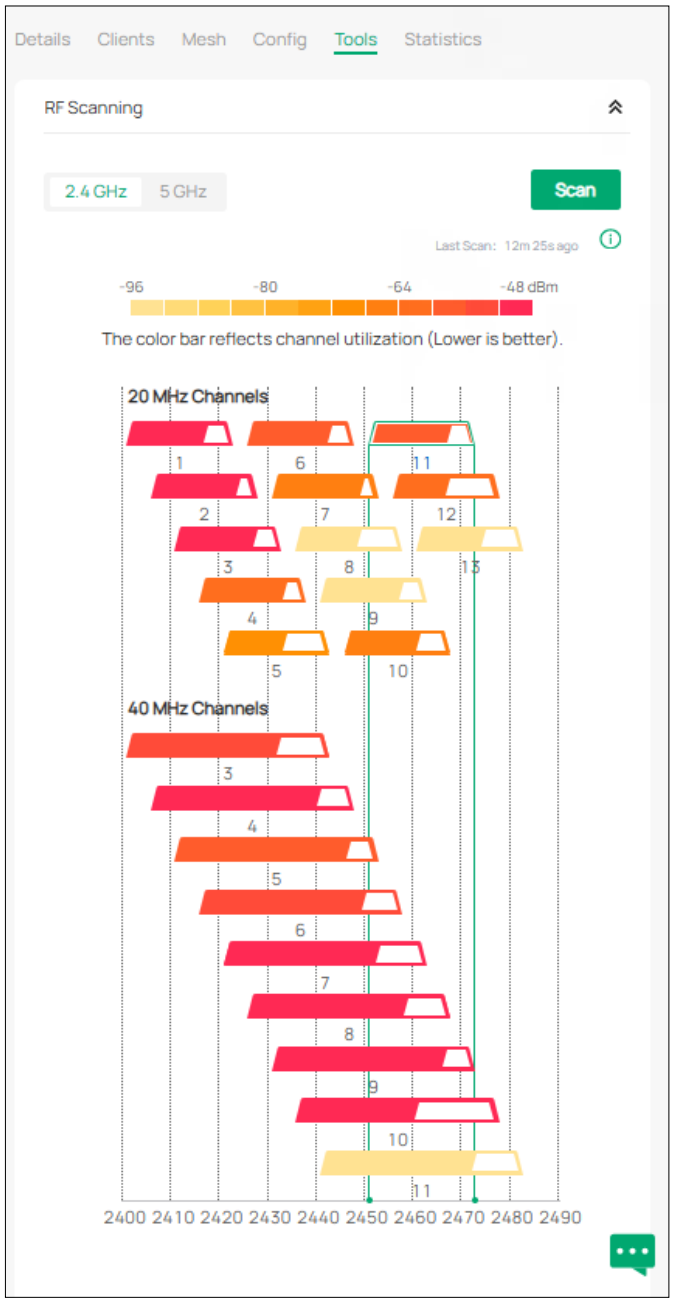
Tools

In Tools, you can enable RF Scanning to scan the RF (Radio Frequency) environments around the AP, which is useful for spectral analysis in channel selection and planning.

Note:

- The RF scanning may take several minutes. During the scanning, all clients using this AP will be disconnected, and the AP will be offline. You should select a spare time of network to start scanning.
- The APs in the mesh network do not support RF Scanning.

Select each frequency band to view and analyze the scan results.



Each colored bar graph displays the information about channel utilization and interference on a channel. The filling area of the bar represents the channel utilization. And the larger filling area means the higher

utilization, which indicates the channel is busier in transmitting data. The color shade represents the level of interference. And the legend is displayed at the top.

The results of different bands are displayed in different channel widths.

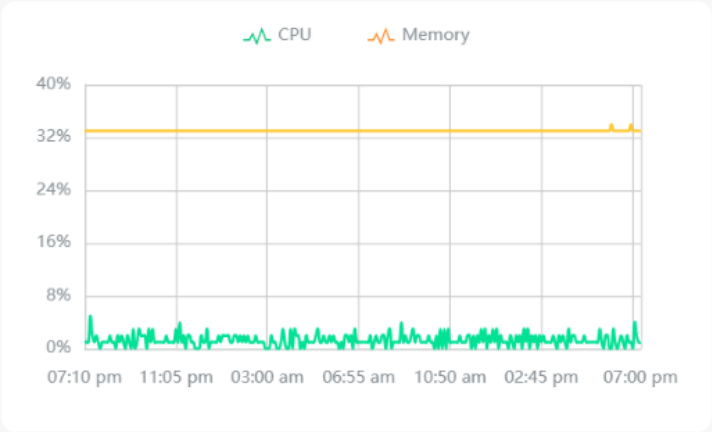
The number below the bar graph displays the corresponding channel number for each channel width option. For example, channels 1, 6 and 11 are three of the 20 MHz channels. And the channel outline in color is in use currently.

You can hover the cursor over a channel option for more details.

Radio	Displays the radio that the AP uses.
Channel Width	Displays the width of the channel.
Used Channels	Displays the channels in use.
Frequency Range	Displays the range of frequencies.
Utilization	Displays the percentage of the frequency range already in use.
Interference	Displays the level of interference.
Interference Type	Displays the type of interface, including MWO (Microwave Oven), CW (Continuous Wave), WLAN (Wi-Fi signals) and FHSS (Frequency Hopping Spread Spectrum).

Statistics

In Statistics, you can monitor the utilization of the device in last 24 hours via charts, including CPU/Memory Monitor, Channel Utilization, Dropped Packets, and Retried Packets. To view statistics of the device in certain period, click the chart to jump to 8. 2 View the Statistics of the Network.



6. 5 Create and Manage Stack Groups

6. 5. 1 Introduction to Stack

Stack is a device virtualization technology that connects two and above switches supporting stack features via Ethernet cables through their stack ports, which logically virtualize them to one device as a whole to forward data in the network. Through this feature, switches can be stacked to improve reliability, expand port numbers, increase bandwidth, simplify networking, and etc.

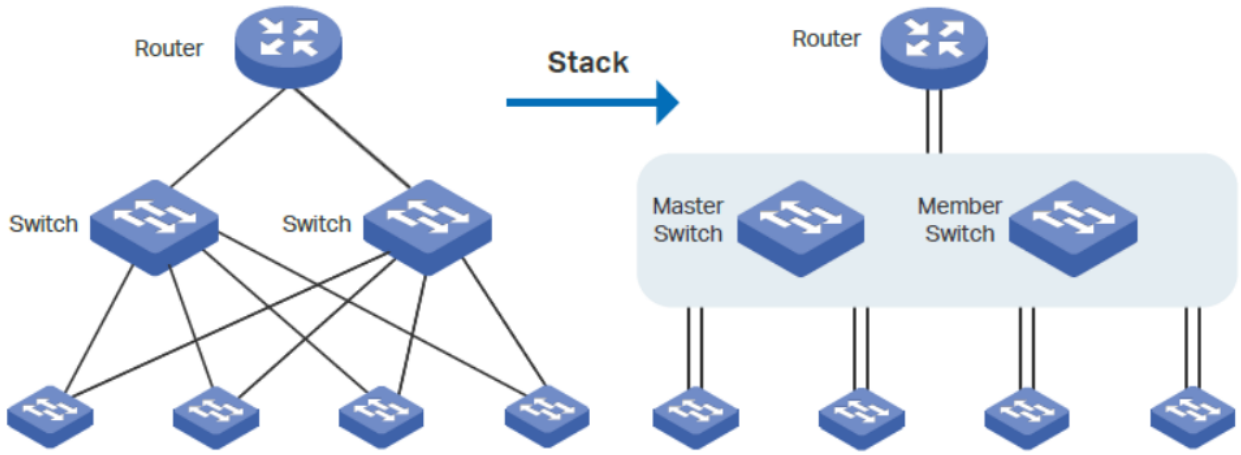
In a stack system, the switches can be categorized mainly into two roles:

- Master Switch

  A stack system has only one master switch. It manages and controls devices in the whole stack system.

- Member Switch

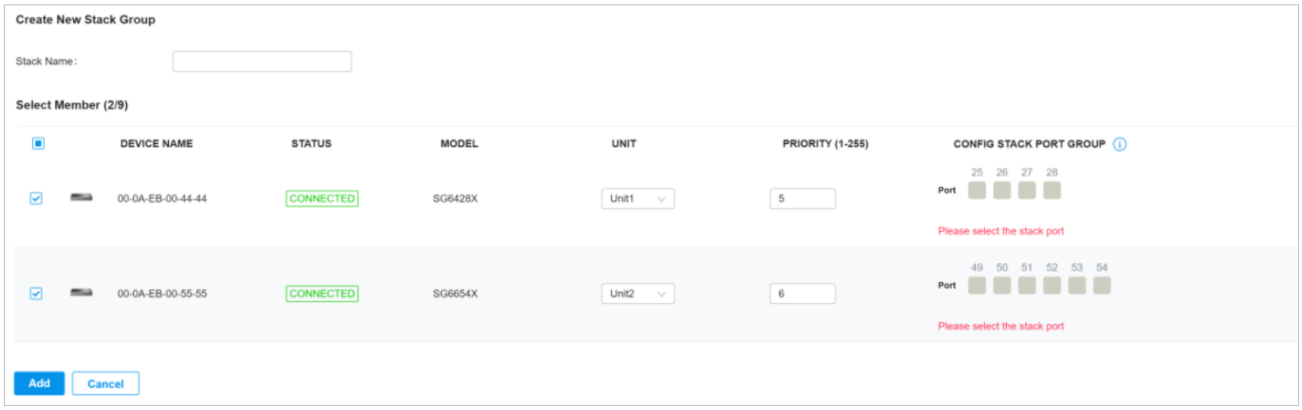
  A stack system may have one or several member switches. They only forward data as standby devices of the master switch. When the master switch fails, a member switch will be re-elected as the new master switch.



6. 5. 2 Create a Stack Group

1. In the Site interface, go to Devices > Device Group > Stack Group.

2. Click Create New Stack. Configure the parameters.



Stack Name	Enter a name to identify the stack group.
Select Member	Select the switches to be stacked, and configure the following parameters: Unit: Specify the unit ID of the switch. Each switch in the stack has a unique unit ID for device management. Priority: Specify the stack priority of the switch. The higher the stack priority, the more likely the switch is to be elected as the Master Switch. A smaller value means a higher priority. Config Stack Port Group: Click the port to be stacked and choose the group ID. A port can join only one group. **Note:** To change the stacking mode of a port, please link down it first. After a port is switched to stacking mode, it can no longer be used as a service port.

3. Apply the settings. Now you can connect the stack ports configured with the same group ID via Ethernet cables to stack the switches.

Note:

- Do not connect a stack port to a non-stack port. Otherwise, device operation may be affected.
- Connect stack ports only when they are set to the same group ID.

6. 5. 3 Configure and Monitor the Stack Group

The stack group logically virtualizes switches to one device as a whole. You can configure and monitor stack groups in the same way as configuring and monitoring switches. For details, refer to 6. 3 Configure and Monitor Switches.

6. 6 Create and Manage Bridge Groups

6. 6. 1 Introduction to Bridge

Outdoor Bridge easily builds point-to-point and point-to-multi-point long range wireless connections. In practical application, it can help users to conveniently deploy APs over long range.

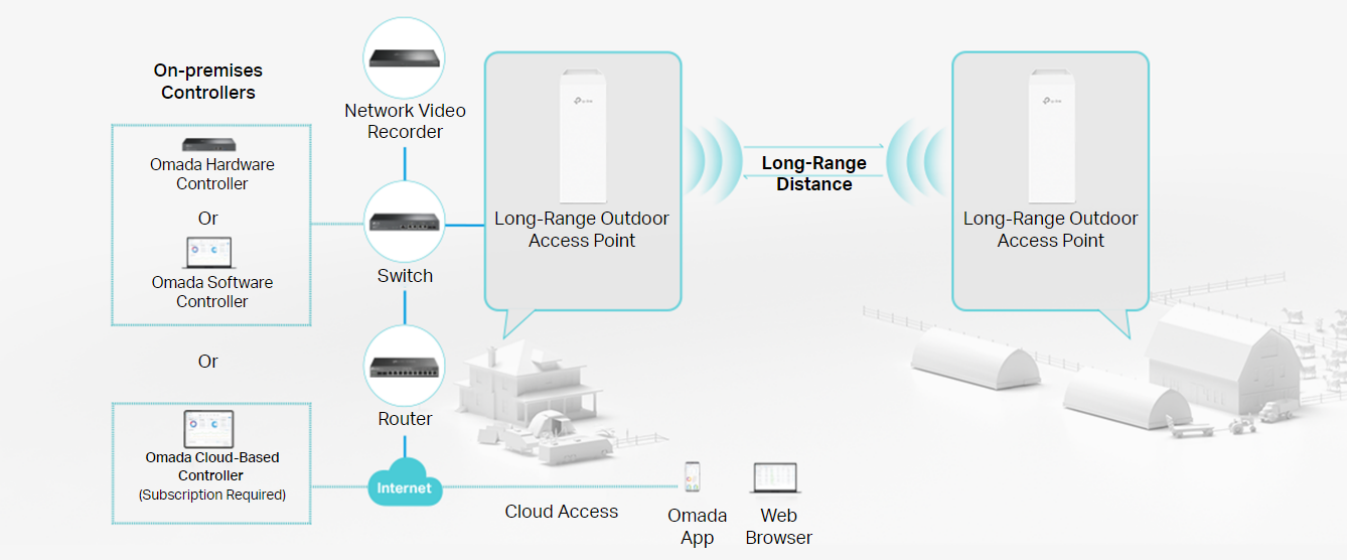
In a bridge system, the APs can be categorized mainly into two roles:

- Main AP

  The Main AP connects to your gateway/router for network access. A bridge system generally has only one Main AP.

- Sub-AP

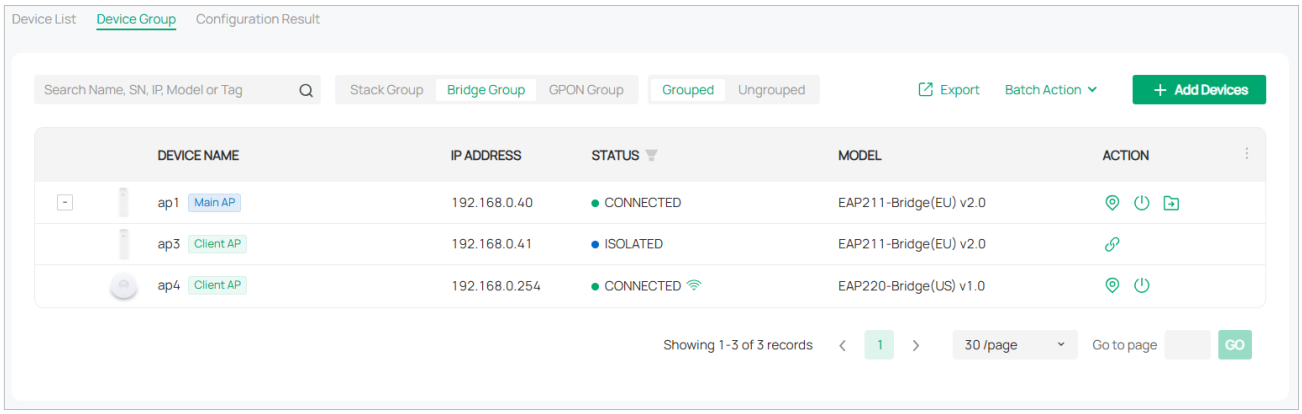
  Sub-APs connect to the Main AP via wireless bridge. A bridge system may have one or several Sub-APs.



6. 6. 2 Create a Bridge Group

1. Obtain a bridge kit product, connect an AP to your gateway/router for network access, and power on all the APs in the kit. The AP with network access will work as the Main AP, and the other AP(s) will automatically connect to the Main AP via wireless bridge.
2. Launch your controller and access a site.

3. Go to Devices > Device Group > Bridge Group. The controller will detect the bridge kit APs and show them in the list.



6. 6. 3 Configure and Monitor the Bridge Group

You can configure and monitor bridge groups in the same way as configuring and monitoring APs. For details, refer to 6. 4 Configure and Monitor APs.

Chapter 7

Monitor and Manage the Clients

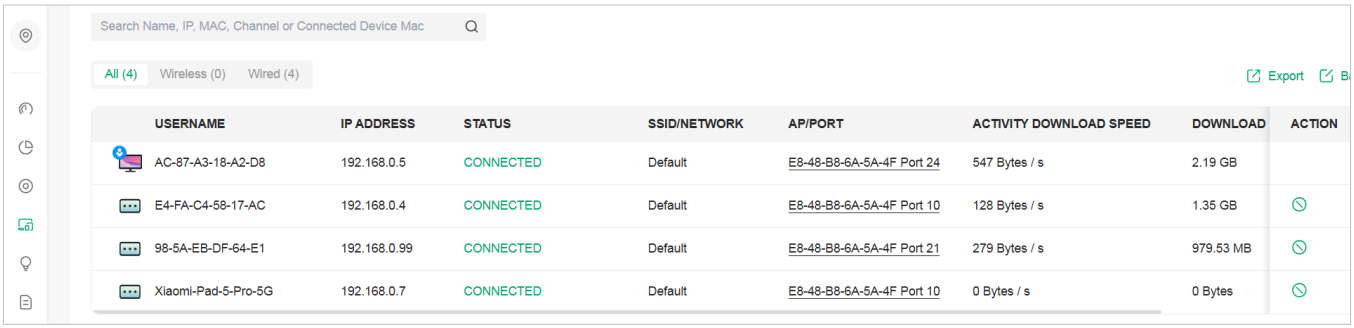
This chapter guides you on how to monitor and manage the clients through the Clients page using the clients table and the properties window and the Hotspot system. To view clients that have connected to the network in the past, refer to View the Statistics During the Specified Period with Insight. This chapter includes the following sections:

- 7. 1 Manage Wired and Wireless Clients in Clients Page
- 7. 2 Manage Client Authentication in Hotspot

7. 1 Manage Wired and Wireless Clients in Clients Page

7. 1. 1 Introduction to Clients Page

The Clients page offers a straight-forward way to manage and monitor clients. It displays all connected wired and wireless clients in the chosen site and their general information. You can also open the Properties window for detailed information and configurations.



PENDING	The client has not passed the portal authentication and it is not connected to the internet.
AUTHORIZED	The client has been authorized and is connected to the internet.
CONNECTED	The client is connected to internet via non-portal network.
AUTHENTICATION-FREE	The client does not need to be authorized and it is connected to the internet.

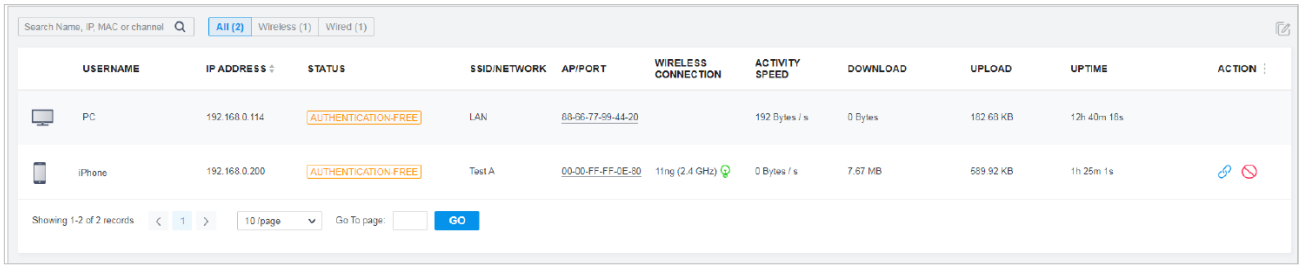
7. 1. 2 Using the Clients Table to Monitor and Manage the Clients

To quickly monitor and manage the clients, you can customize the columns and filter the clients for a better overview of their information. Also, quick operations and batch configuration are available.

- **Customize the Information Columns**

  Click the ellipse icon next to the Action column and you have three choices: Default Columns, All Columns, and Customize Columns. To customize the information shown in the table, click the checkboxes of information type.

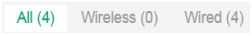
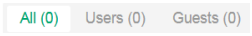
  To change the list order, click the column head and the ascending and descending icon appears for you to choose the display order.



When this icon appears in the Wireless Connection column, it indicates the client is in the power-saving mode.

Filter the Clients

To search specific client(s), use the search box above the table. To filter the clients by their connection type, use the tab bars above the table. For wireless clients, you can further filter them by the frequency band and the type of connected wireless network.

	Filter clients using the search box based on username, IP address, MAC address or channel.
	Filter clients based on their connection type.
	(For wireless clients) Filter wireless clients based on the frequency band they are using.
	(For wireless clients) Filter wireless clients based on the type of connected wireless network. Guests are clients connected to the guest network, which you can set during the Quick Setup, creating wireless networks, etc.

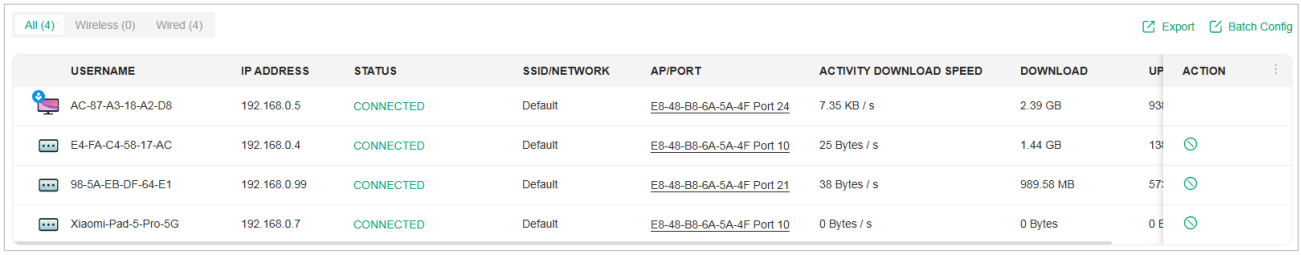
Quick Operations

For quick operations on a single client, click the icons in the Action column. The available icons vary according to the client status and connection type.

	Click to block the client in the chosen site. You can view blocked clients in 8. 5. 2 Known Clients.
	(With portal authentication enabled) Click to manually authorize the client that has not passed the portal authentication.
	(With portal authentication enabled) Click to unauthorize the client that has passed the portal authentication.
	(For wireless clients) Click to reconnect the wireless client to the wireless network.

Multiple Select for Batch Configuration

To select multiple clients and add them to the Properties window, click Batch Config on the upper-right and then check the boxes. When you finish choosing the clients, click Done and the chosen client(s) will be added to the Properties window for batch client configuration.



7. 1. 3 Using the Properties Window to Monitor and Manage the Clients

In Properties window, you can view more detailed information about the connected client(s) and manage them. To open the Properties window, click the entry of a single client, or click the edit icon to select multiple clients for batch configuration. Use the following icons for the Properties window.

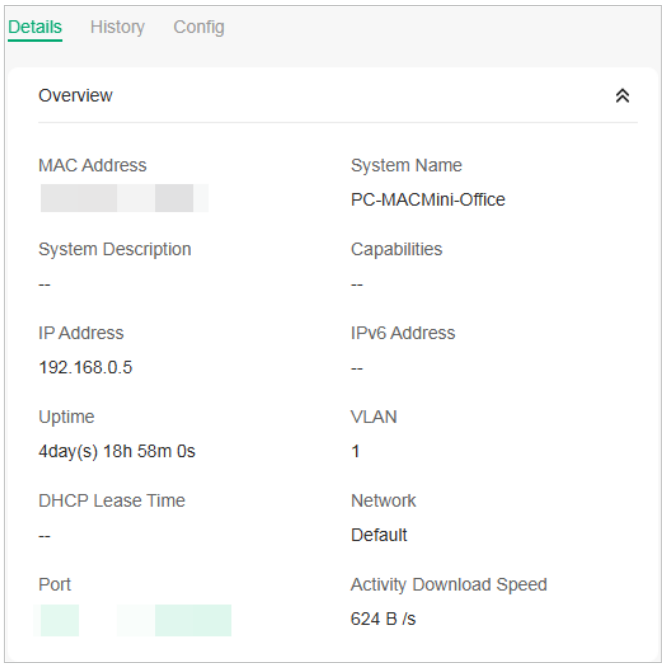
	Click to select multiple clients and add them to the Properties window for batch monitoring and management.
	Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click  .
	Click to maximize the Properties window. You can also use the icon on pages other than the Clients page.
	Click to close the Properties window of the chosen client(s). Note that the unsaved configuration for the client(s) will be lost.
	The number on the lower-right shows the number of clients in the batch client configuration.

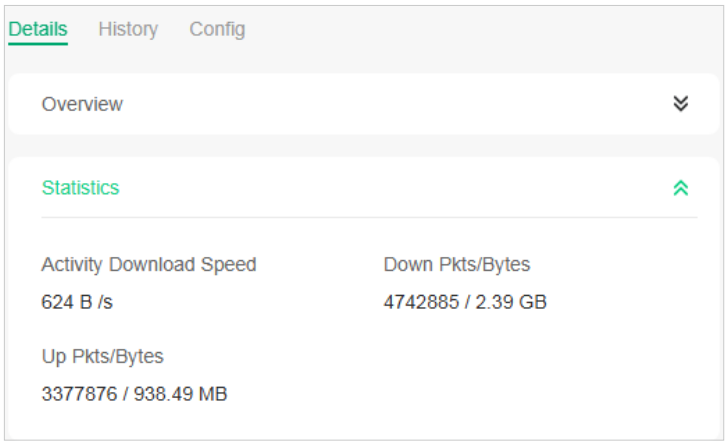
Monitor and Manage a Single Client

- **Monitor a Single Client**

  After opening the Properties window of a single client, you can view the basic information, traffic statistics, and connection history under the Details and History tabs.

  Under the Details tab, Overview and Statistics displays the basic information and traffic statistics of the client, respectively. The listed information varies due to the client's status and connection type.



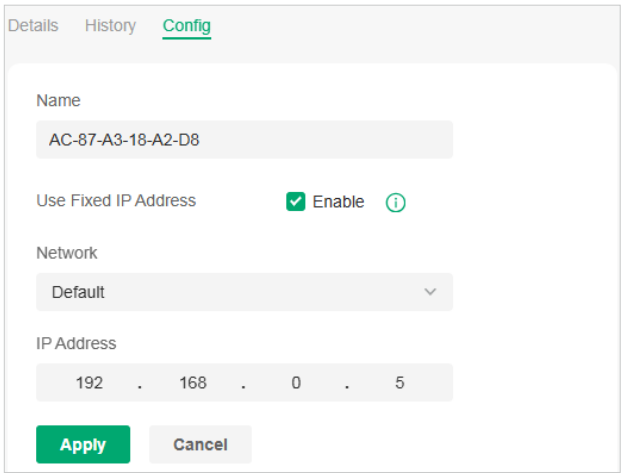


Under the History tab, you can view the connection history of the client.



■ Manage a Single Client

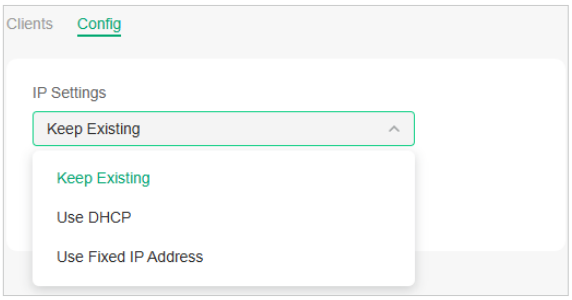
In Config, you can configure the following parameters:



Name	Specify the client's name to better identify different clients, and the name is used as the client's username in the table on the Clients page.
Use Fixed IP Address	Click the checkbox to configure a fixed IP address for the client. With this function enabled, select a network and specify an IP address for the client. To view and configure networks, refer to 4. 2 Configure Wired Networks. Note: A gateway is required for this function. Otherwise, you cannot set a fixed IP address for the client.

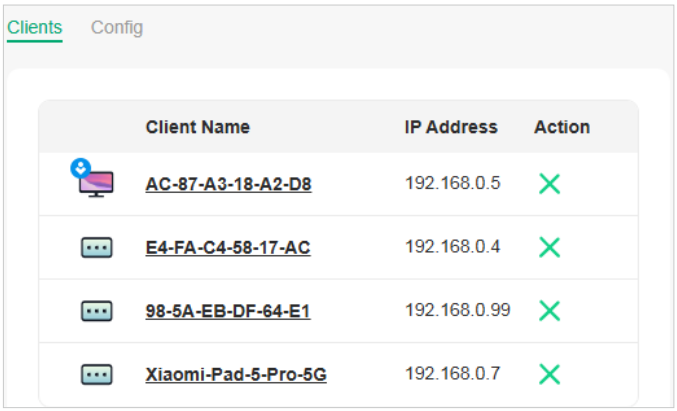
Monitor and Manage Multiple Clients

To manage multiple clients at the same time, click the edit button, select multiple clients, and click Done. Then you can configure the following parameters under the Config tab.



IP Setting	Keeping Existing: The IP setting of the chosen clients remains their current settings. Use DHCP: The IP addresses of the clients is automatically assigned by the DHCP server, such as the Layer 3 switch and the gateway. Use Fixed IP Address: Select a network and assign fixed IP addresses to the chosen clients manually. To view and configure networks, refer to 4. 2 Configure Wired Networks. Note that a gateway is required for this function. Otherwise, you cannot set fixed IP addresses for the chosen clients.

You can view their names and IP addresses in the Clients tab and remove client(s) from Batch Client Configuration by clicking the block icon in the Action column.



7. 2 Manage Client Authentication in Hotspot

Hotspot is a portal management system for centrally monitoring and managing the clients authorized by portal authentication. The following four tabs are provided in the system for a easy and direct management.

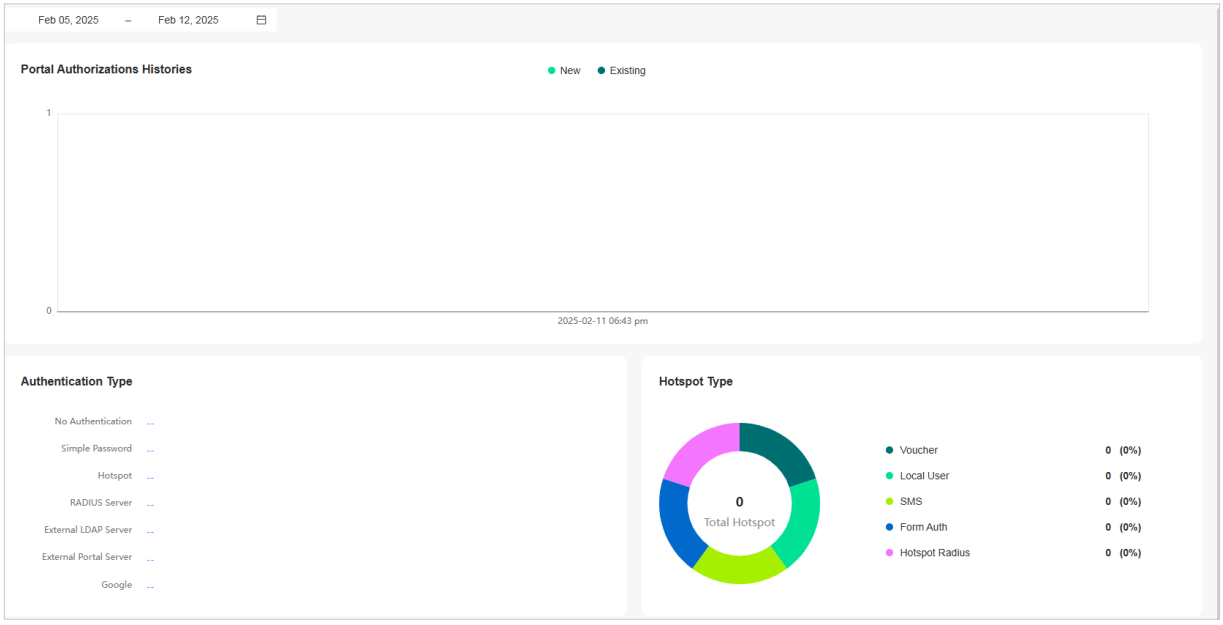
Dashboard	Monitor portal authorizations at a glance through different visualizations.
Authorized Clients	View the records of the connected and expired portal clients.
Vouchers	Create vouchers for Portal authentication, and view and manage the related information.
Local Users	Create local user accounts for Portal authentication, view their information, and manage them.
Form Auth Data	Customize your survey contents and publish it to collect data.
Operators	Create operator accounts for Hotspot management, view their information, and manage them.

To access the system, click Hotspot in the sidebar of the Site interface.

7. 2. 1 Dashboard

In the dashboard, you can monitor portal authorizations at a glance through different visualizations.

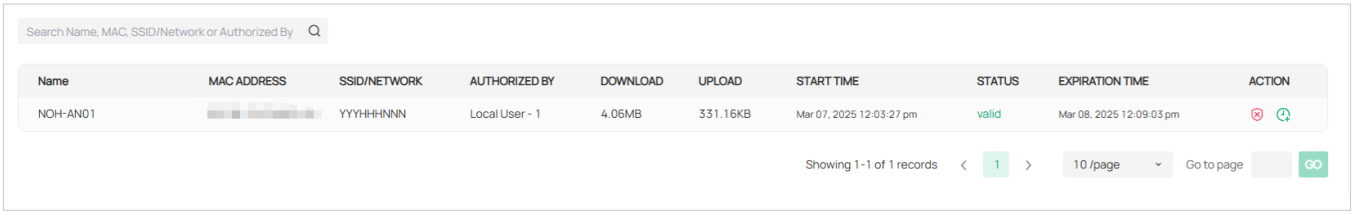
To open the dashboard, click Hotspot in the sidebar of the Site interface and click Dashboard. Specify the time period to view portal authorization histories.



7. 2. 2 Authorized Clients

The Authorized Clients tab is used to view and manage the clients authorized by portal system, including the expired clients and the clients within the valid period.

To open the list of Authorized Clients, click Hotspot in the sidebar of the Site interface and click Authorized Clients. You can search certain clients using the search box, view their detailed information in the table, and manage them using the action column.



	Click to extend the valid period of the authorized client. You can choose the preset time length or set a customized period based on needs.
	Click to disconnect the authorized client(s). If you disconnect an authorized client, the client needs to be re-authenticated for the next connection.
	Click to delete the expired client from the list.

7. 2. 3 Vouchers

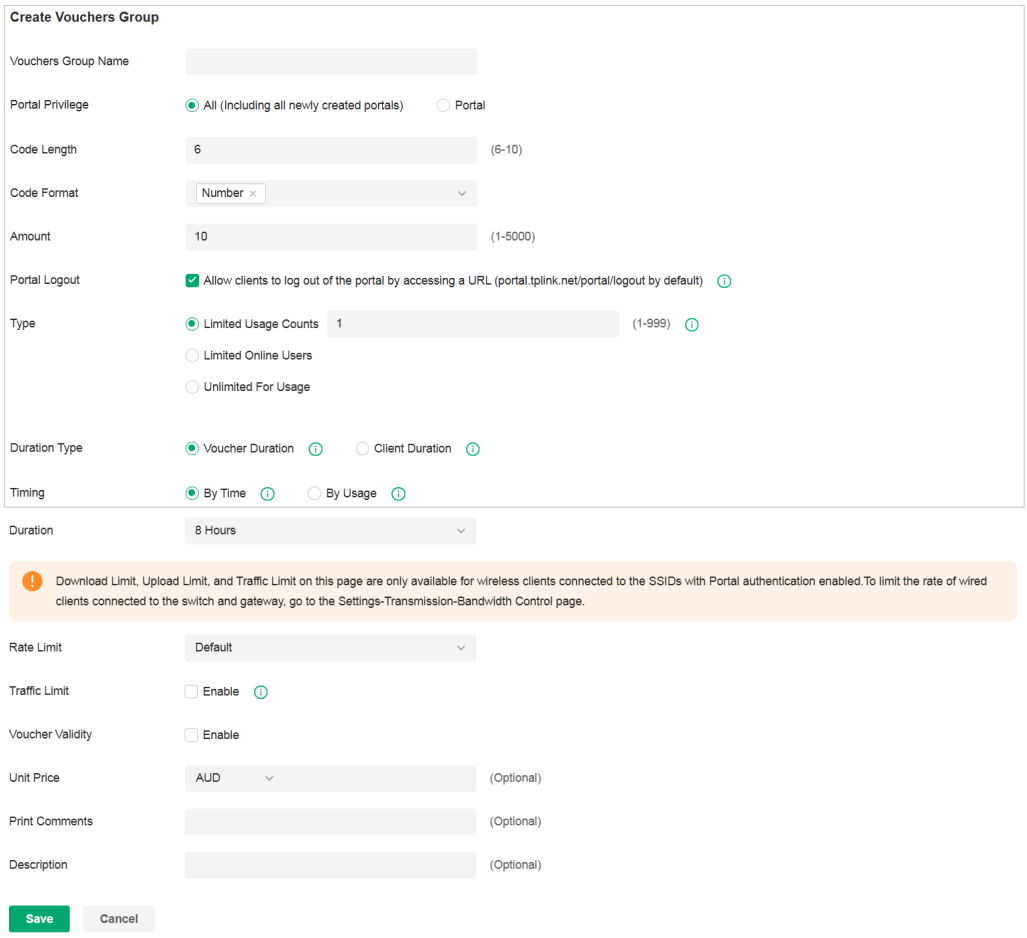
The Vouchers tab is used to create vouchers and manage unused voucher codes. With voucher configured and codes created, you can distribute the voucher codes generated by the controller to clients for them to access the network via portal authentication. For detailed configurations, refer to 4. 8. 1 Portal.

Create vouchers

Follow the steps below to create vouchers for authentication:

1. Click Hotspot in the sidebar of the Site interface and click Vouchers > Voucher Groups.

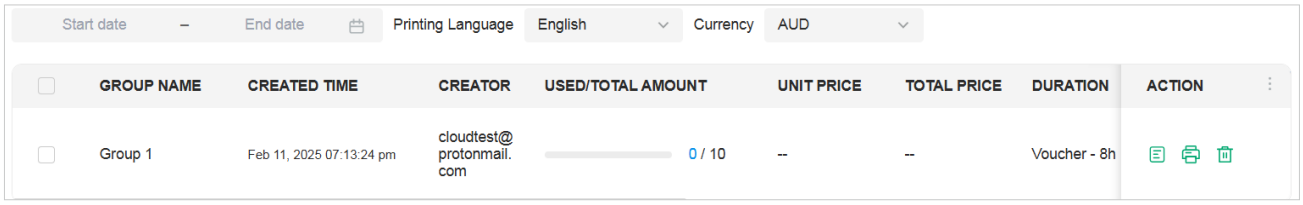
2. Click +Create Vouchers Group on the upper-right, and the following window pops up. Configure the following parameters and click Save.



Vouchers Group Name	Enter a name to identify the group.
Portal Privilege	All: The vouchers will take effect for all voucher type portals, including newly created ones. Portal: Select the portal for which the vouchers will take effect.
Code Length	Specify the length of the code(s) from 6 to 10 digits.
Code Format	Choose whether the voucher code is generated by numbers, letters, or a mixture.
Amount	Specify the number of voucher codes you want to create.
Portal Logout	Check the box to allow guests to log out of the portal by accessing a URL (portal.tplink.net/portal/logout by default). You can change the default URL by editing portal.logout.domain in the omada.properties file. **Note:** Some devices may require firmware update to support Portal Logout.

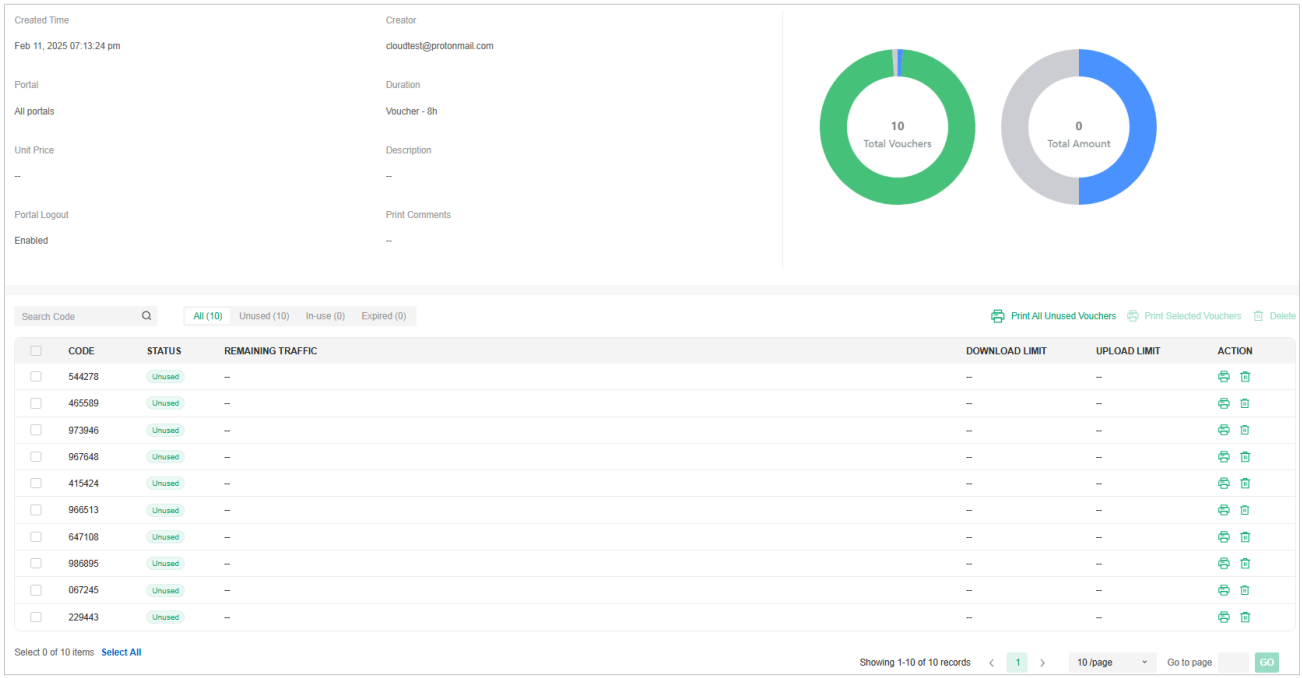
Type	Select a type to limit the usage counts or the number of authorized users of a voucher code. Limited Usage Counts: The voucher code can only be used for a limited number of times within its valid period. Limited Online Users: The voucher code can be used for an unlimited number of times within its valid period, but only a limited number of wireless clients can access the network with this voucher code at the same time. Unlimited For Usage: The voucher code can be used for an unlimited number of times within its valid period.
Duration Type	Specify whether to limit the voucher duration or client duration.
Timing	By time: The voucher code takes effect within a fixed period of time after authentication. By Usage: The voucher code takes effect according to the actual time used by the client.
Duration	Select the valid period for the voucher code(s).
Rate Limit	Select an existing rate limit profile, create a new rate limit profile or customize the rate limit for the voucher codes. Custom: Specify the download/upload rate limit based on needs. Download/Upload Limit: Click the checkbox and specify the rate limit for download/upload for wireless clients using the voucher code(s). The value of the download and upload rate can be set in Kbps or Mbps. Note: Download/Upload Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings >Transmission > Bandwidth Control.
Traffic Limit	Click the checkbox and specify the daily/weekly/monthly/total traffic limit for the voucher, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the client(s) can no longer access the network using the voucher. Note: Traffic Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings > Transmission > Bandwidth Control.
Voucher Validity	Enable this option and configure the start time and expiration time of the voucher. The voucher can no longer be used no matter whether it runs out of available time or reaches the expiration time
Unit Price (optional)	Set the amount and currency type for the voucher (for statistical purposes only).
Print Comments	Enter print comments if needed and the comments will be printed when you print the created voucher codes.
Description (optional)	Enter notes for the created voucher code(s), and the input description is displayed in the voucher list under the voucher tab.

3. The voucher group is generated.



2	The voucher code can be used for an unlimited number of times within its valid period, but only a limited number of wireless clients can access the internet with this voucher code at the same time. The number on the right shows the limited number of users.
2	The voucher code can only be used for a limited number of times within its valid period. The number on the right shows the limited number of authentication times.

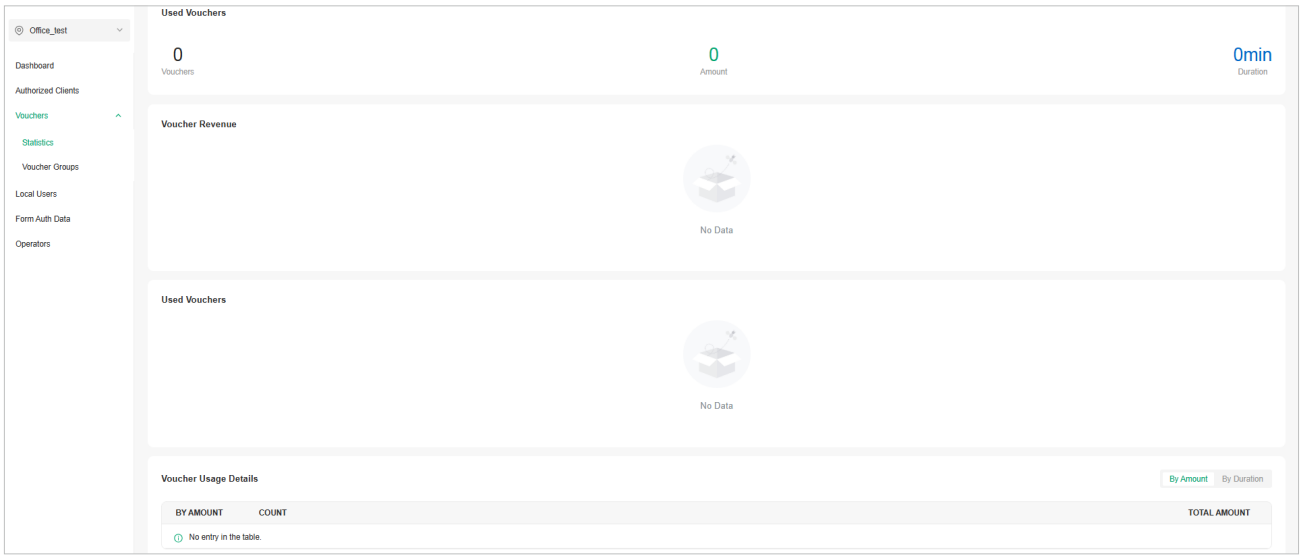
You can click the Details icon in the Action column to view the voucher codes.



4. Print the vouchers. Click to print a single voucher, or click checkboxes of vouchers and click Print Selected Vouchers to print the selected vouchers. And you can click Print All Unused Vouchers to print all unused vouchers.

544278 Valid for 8h Limited Usage Counts 1	**465589** Valid for 8h Limited Usage Counts 1	**973946** Valid for 8h Limited Usage Counts 1	**967648** Valid for 8h Limited Usage Counts 1
415424 Valid for 8h Limited Usage Counts 1	**966513** Valid for 8h Limited Usage Counts 1	**647108** Valid for 8h Limited Usage Counts 1	**986895** Valid for 8h Limited Usage Counts 1
067245 Valid for 8h Limited Usage Counts 1	**229443** Valid for 8h Limited Usage Counts 1		

5. Distribute the vouchers to clients, and then they can use the codes to pass authentication. If a voucher code expires, it will be automatically removed from the list.
6. To delete certain vouchers manually, click the trash bin icon to delete a single voucher, or Delete to delete multiple voucher codes at a time.
7. On the Vouchers > Statistic page, you can view the historical statistical data of vouchers.



7. 2. 4 Local Users

The Local Users tab is used to create user accounts for authentication. With the Local User configured, clients are required to enter the username and password to pass the authentication. You can create multiple accounts and assign them to different users. For detailed configurations, refer to 4. 8. 1 Portal.

Create Local Users

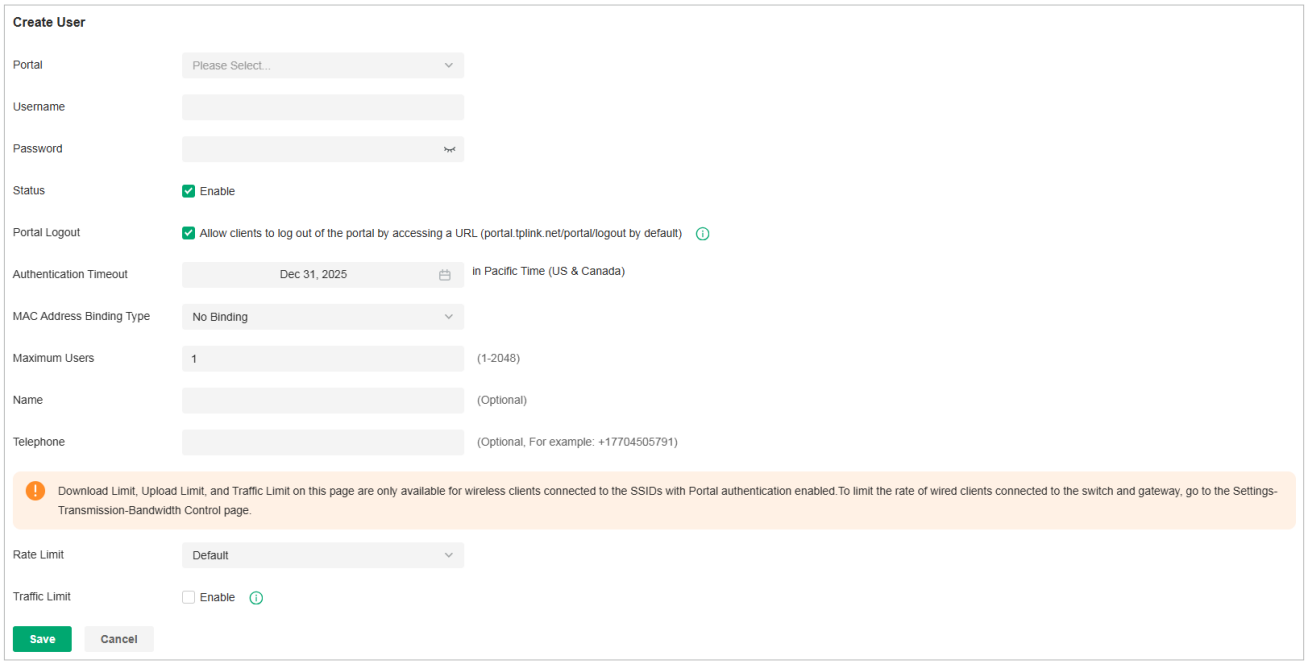
There are two ways to create local user accounts: create accounts on the page and import from a file.

To create local user accounts, follow the steps below.

1. Click Hotspot in the sidebar of the Site interface and click Local Users.
2. Create Local User accounts through either of the following ways.

Create Local User accounts

Click +Create User on the upper-right, and the following window pops up. Configure the following parameters and click Save.

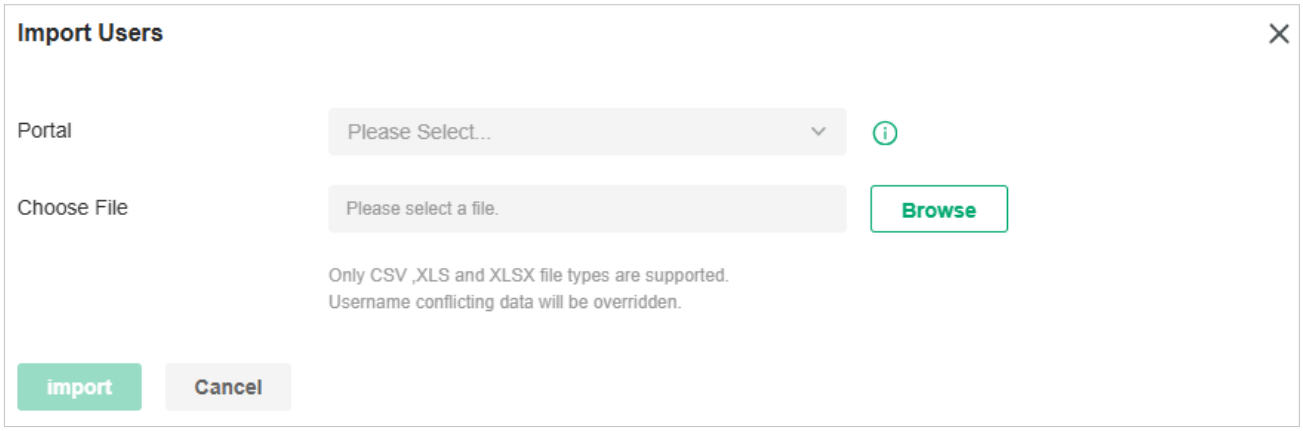


Portal	Select the portal for which the local users will take effect.
Username	Specify the username. The username should be different from the existing ones, and it is not editable once it is created.
Password	Specify the password. Local users are required to enter the username and password to pass authentication and access the network.
Status	When the status is enabled, it means the user account is valid. You can disabled the user account, and enable it later when needed.
Portal Logout	Check the box to allow guests to log out of the portal by accessing a URL (portal.tplink.net/portal/logout by default). You can change the default URL by editing portal.logout.domain in the omada.properties file. **Note:** Some devices may require firmware update to support Portal Logout.
Authentication Timeout	Specify the authentication timeout for local users. After timeout, the users need to log in again on the authentication page to access the network.

MAC Address Binding Type	There are three types of MAC binding: No Binding, Static Binding and Dynamic Binding. No Binding: No MAC address is bound to the local user account. Static Binding: Bind a MAC address to this user account manually. Then only the user with the this MAC address can use the username and password to pass the authentication. Dynamic Binding: The MAC address of the first user that passes the authentication will be bound to this account. Then only this user can use the username and password to pass the authentication.
Maximum Users	Specify the maximum number of users that can use this account to pass the authentication.
Name (optional)	Specify a name for identification.
Telephone (optional)	Specify a telephone number for identification.
Rate Limit	Select an existing rate limit profile, create a new rate limit profile or customize the rate limit for the local users. Custom: Specify the download/upload rate limit based on needs.
Traffic Limit	Click the checkbox and specify the daily/weekly/monthly/total traffic limit for the local user account, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the user(s) can no longer access the network using this account. Note: Traffic Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings > Transmission > Bandwidth Control.

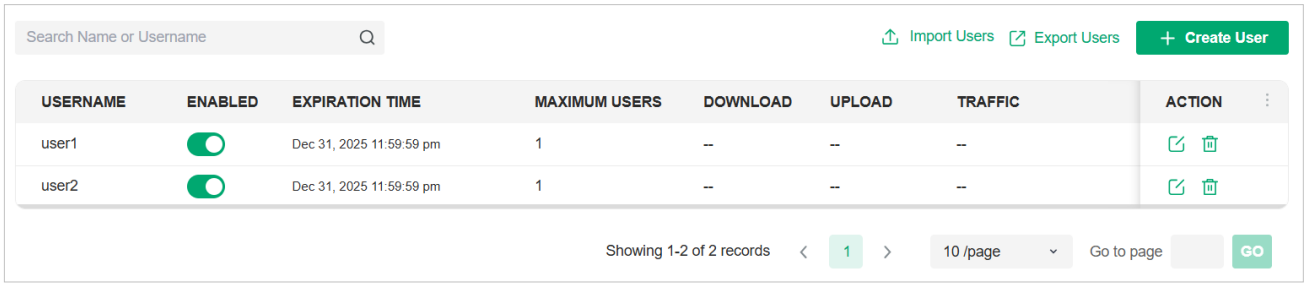
- **Create Local User accounts from files**

  Click Import Users on the upper-right, and the following window pops up. Select a file in the format of CVS or Excel, and click Import. To see required parameters and corresponding explanation, refer to Create Local User accounts. Note that the imported file will override the current user data.



Portal	Select the portal to which the local users will be imported.

3. The local user account(s) will be created and displayed in the module. You can view the information of the created local users, search certain accounts through the name, and use icons for management.



Import Users	Click to add local user(s) from files in the format of CVS or Excel. It is recommended when you need to create local users in batches. Select the portals based on needs, and the local users will be imported to the chosen portal. Note that the imported file will override the current user data.
Export Users	Click to export the local user(s) to files in the format of CVS or Excel. Select the portals based on needs, and the local users of the chosen portal will be exported.
	Click to edit the parameters for the local user.
	Click to delete the local user.

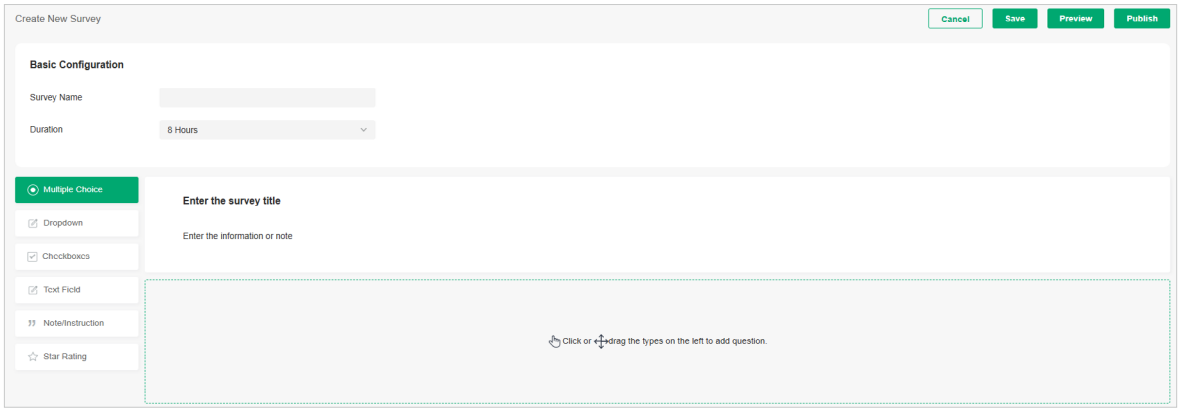
7. 2. 5 Form Auth Data

The Form Auth Data tab is used to create and manage surveys. You can customize your survey contents and publish it to collect data.

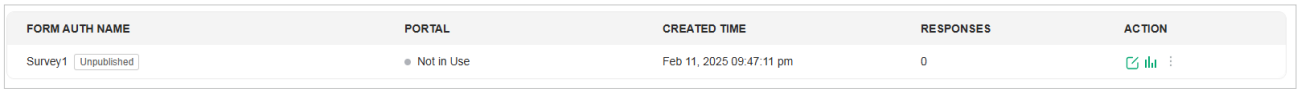
Create Surveys

To create surveys, follow the steps below.

1. Click Hotspot in the sidebar of the Site interface and click Form Auth Data.
2. **Click** Create New Survey and the following window pops up.



3. Specify the survey name and duration, then customize the contents.
4. Preview and save the settings or publish the survey.
5. The surveys are created and displayed in the table. You can use icons for management and click the ellipse icon for more management options.



7. 2. 6 Operators

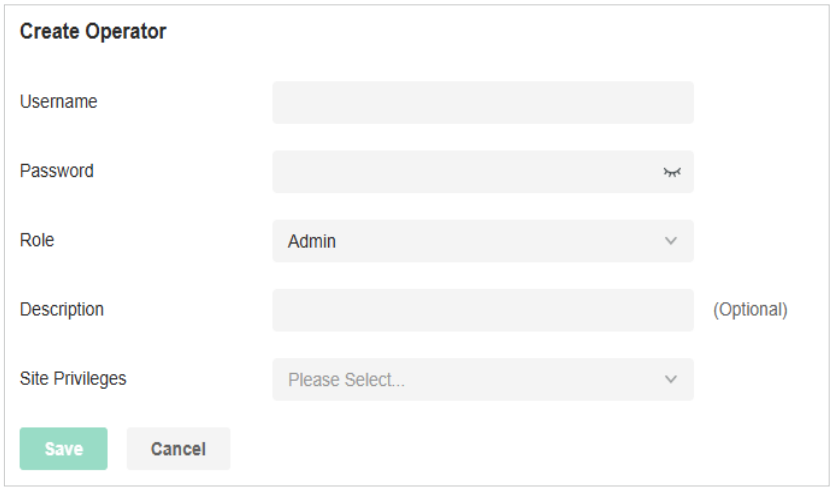
The Operators tab is used to manage and create operator accounts that can only be used to remotely log in to the Hotspot system and manage vouchers and local users for specified sites. The operators have no privileges to create operator accounts, which offers convenience and ensures security for client authentication.

Create Operators

To create operator accounts, follow the steps below.

1. Click Hotspot in the sidebar of the Site interface and click Operators.

2. Click Create Operator on the lower-left, and the following window pops up.



3. Specify the username, password, and role for the operator account. Admin role has read and write permissions, while Viewer role has read-only permissions.
4. (Optional) Enter a description for identification.
5. Select sites from the drop-down list of Site Privileges. Click Save.
6. The operator accounts are created and displayed in the table. You can view the information of the create operator accounts on the page, search certain accounts through the name and notes, and use icons for management.



7. Then you can use an operator account to log in to the Hotspot system:

- **For software controller**

  Visit the URL **https://Controller Host's IP Address:8043/ControllerID/login/#hotspot** (for example: **https://192.168.0.174:8043/4d4ede7983bb983545d017c628feaa3d/login/#hotspot**), and use the operator account to enter the Hotspot system.

- **For hardware controller**

  Visit the URL **https://Controller Host's IP Address:443/ControllerID/login/#hotspot** (for example: **https://192.168.0.174:443/4d4ede7983bb983545d017c628feaa3d/login/#hotspot**), and use the operator account to enter the Hotspot system.

- **For cloud-based controller**

  Visit the URL **https://URL of the controller/ControllerID/login/#hotspot**, and use the operator account to enter the Hotspot system.

Chapter 8

Monitor the Network

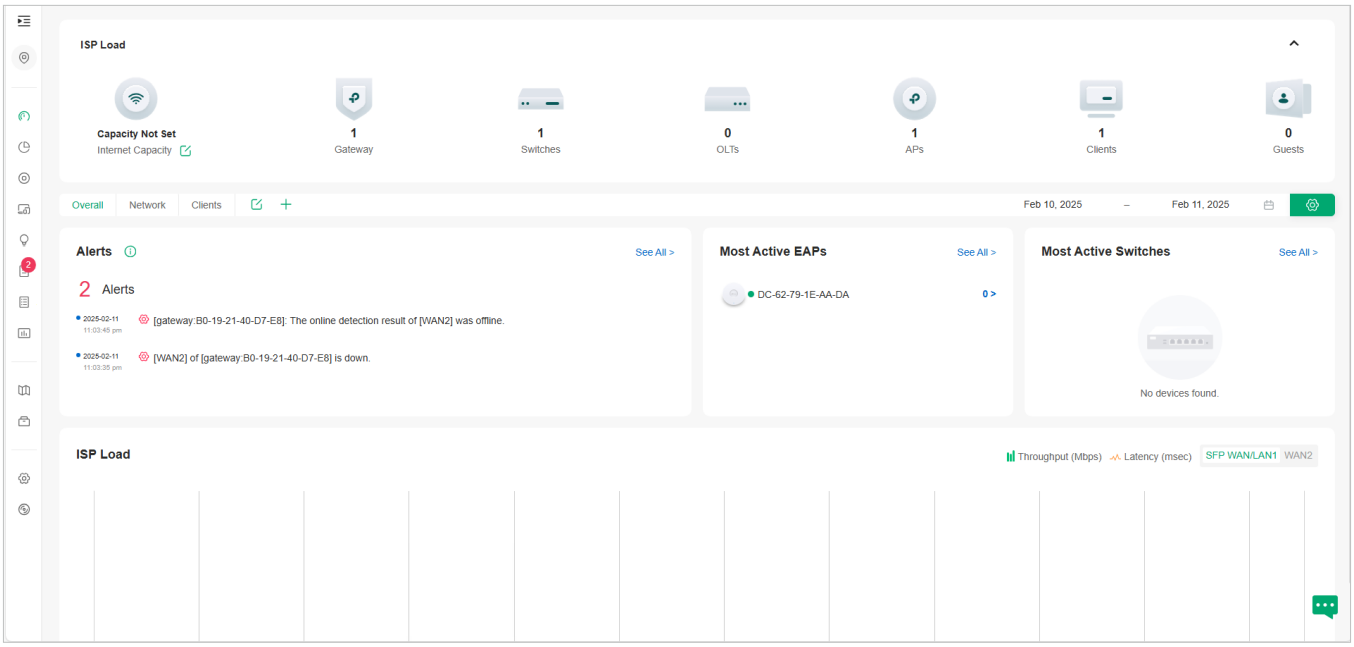
This chapter guides you on how to monitor the network devices, clients, and their statistics. Through visual and real-time presentations, the SDN Controller keeps you informed about the accurate status of the managed network. This chapter includes the following sections:

- 8. 1 View the Status of Network with Dashboard
- 8. 2 View the Statistics of the Network
- 8. 3 Monitor the Network with Map
- 8. 4 Monitor the Network with Reports
- 8. 5 View Statistics During Specified Period with Insight
- 8. 6 View and Manage Logs
- 8. 7 Audit Logs
- 8. 8 Monitor the Network with Tools

8. 1 View the Status of Network with Dashboard

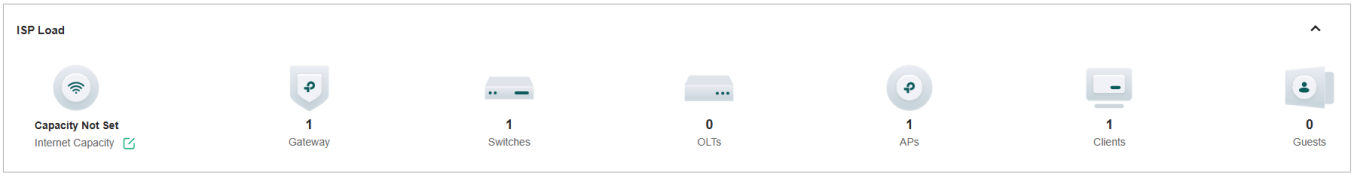
8. 1. 1 Page Layout of Dashboard

Dashboard is designed for a quick real-time monitor of the site network. An overview of network topology is at the top of Dashboard, and the below is a tab bar followed with customized widgets.

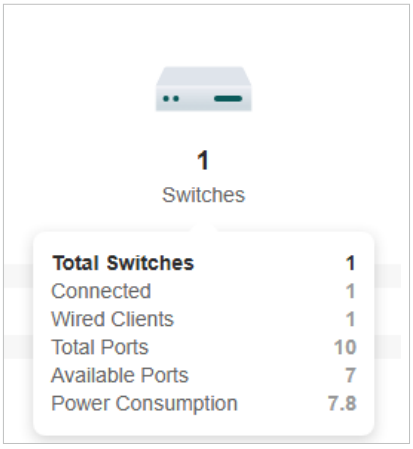


Topology Overview

Topology Overview on the top shows the status of ISP Load and numbers of devices, clients and guests.



You can hover the cursor over the gateway, switch, AP, client or guest icons to check their status. For detailed information, click the icon here to jump to the Devices or Clients section.



Tab Bar

You can customize the widgets displayed on the tab for Dashboard page. Three tabs are created by default and cannot be deleted.



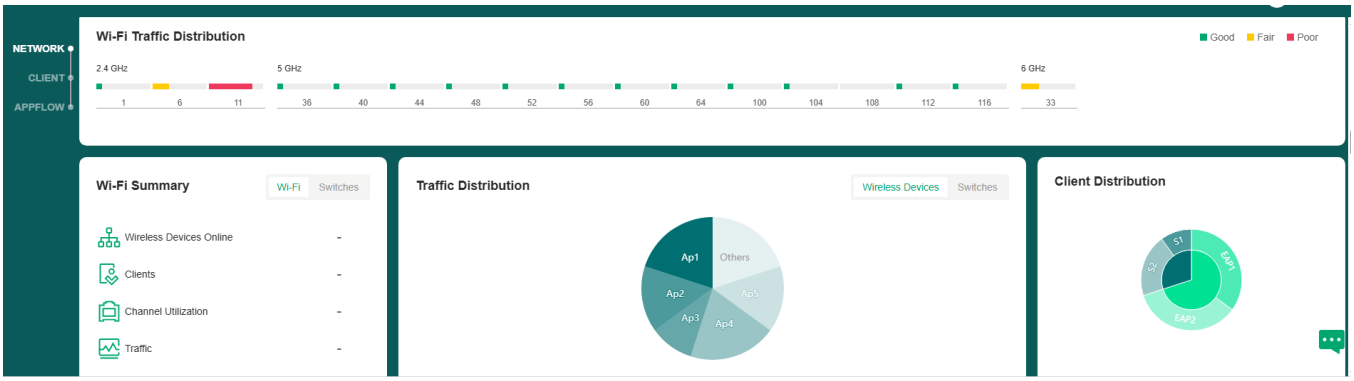
Overall	Displays the network overview information.
Network	Displays network information such as Alerts, Wi-Fi Traffic Distribution, and more.
Clients	Displays client information such as Most Active Clients, Clients Freq Distribution, and more.

In the tab bar, you can take the following action to edit the tabs and customize the widget to be displayed.

	Click the icon to edit the tabs. For the default tabs, you can reset them to the default settings. For a created tab, you can edit its name or delete it.
	Click the icon and enter the name in the pop-up window to create a new tab.
Feb 10, 2025 – Feb 11, 2025	Click the date to display a calendar. To quickly display the statistics of today, yesterday, last 24 hours, or last several days, click the default date/period at the right side in the calendar. To display the statistics of a specific date, click the date twice in the calendar. To display the statistics of a specific time range, click the start date and end date in the calendar.
	Click a tab and then click a widget in the pop-up page to add it to this tab or remove it.

8. 1. 2 Explanation of Widgets

The widgets are divided into different categories. You can click the setting icon to add or remove the widgets.

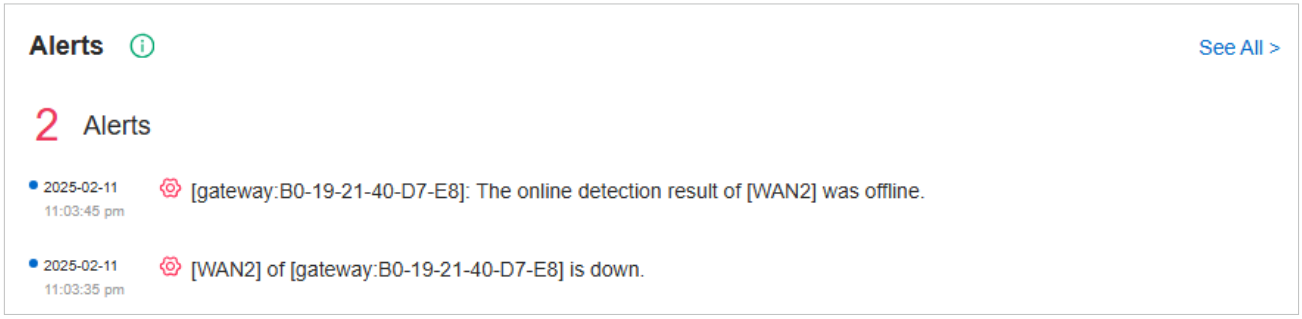


Network

Network widgets use lists and charts to illustrate the traffic status of wired and wireless networks in the site.

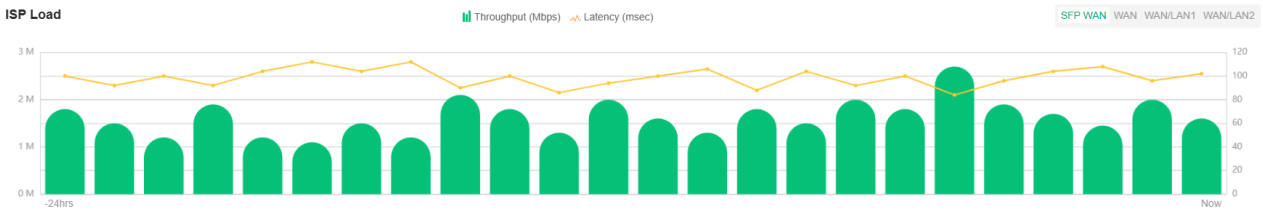
- **Alerts**

  The Alerts widget displays the total number of unarchived alerts happened in the site and details of the latest alerts. To view all the alerts and archive them, click See All to jump to Log > Alerts. To specify events appeared in Alerts, go to Log > Notifications and configure the events as the Alert level. For details, refer to 8. 6 View and Manage Logs.



- **ISP Load**

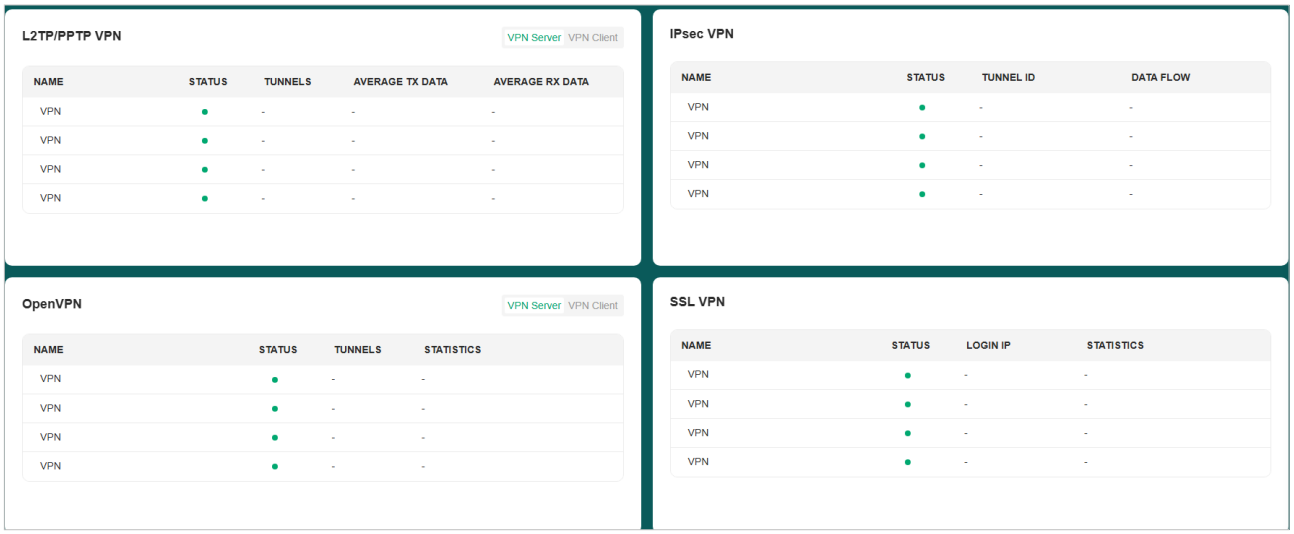
  ISP Load use a line chart to display the throughput and latency of gateway's WAN port within the time range. Click the tab on the right to view the statistics of each WAN port and move the cursor on the line chart to view specific values of throughput and latency. For detailed statistics of certain gateway's WAN port within a time range, refer to 8. 2 View the Statistics of the Network.



  To test the current download and unload speed and the latency of WAN port, click Test Speed on the widget to display the speed test result.

- **VPNs**

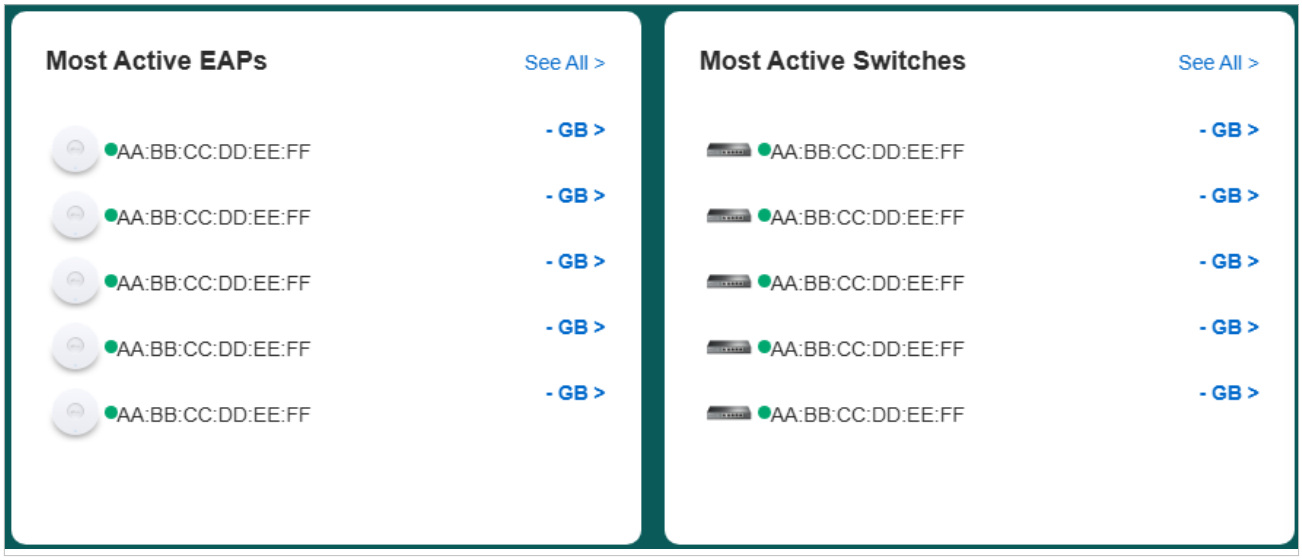
  VPN widgets display the information of VPN servers and VPN clients. Click the corresponding tab to display the statistics.



- **Most Active EAPs/Most Active Switches**

  These two widgets can display most active EAPs and switches in the site based on the total number of traffic within the time range. Only the devices that has been adopted by the controller will be displayed.

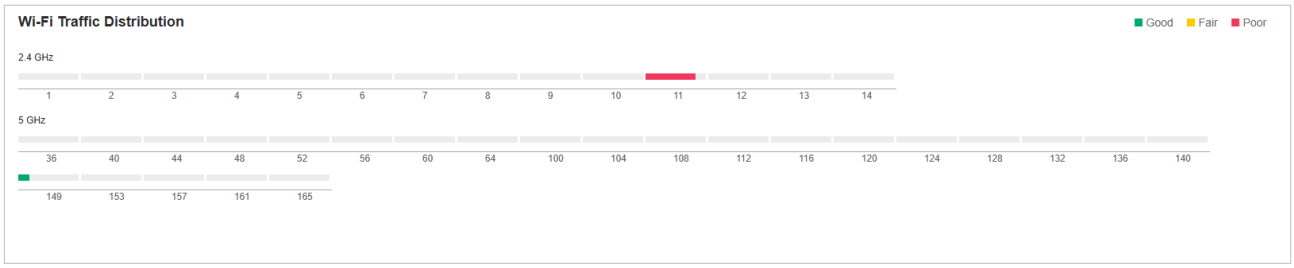
  To view all the devices discovered by the controller, click See All to jump to the Devices section. You can also click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to 6 Configure and Monitor Controller-Managed Devices.



- **Wi-Fi Traffic Distribution**

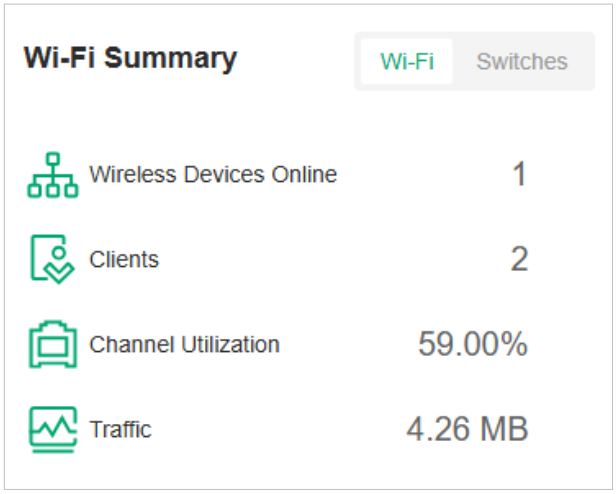
  The Wi-Fi Traffic Distribution widget displays channel distribution of all connected EAPs in the site. Good, Fair, and Poor are used to describe channel status which indicates channel interference from

low to high. You can hover your cursor over the band to view the number of EAPs and clients on the channel.



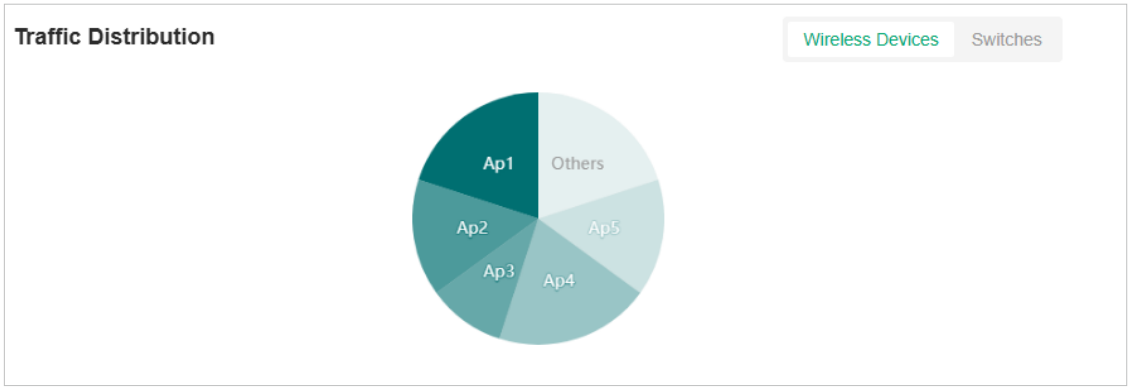
- **Wi-Fi Summary**

The Wi-Fi Summary widget summarizes the real-time status of wireless networks in the site, including the number of connected EAPs and clients, the channel utilization, and the total number of traffic within the time range.



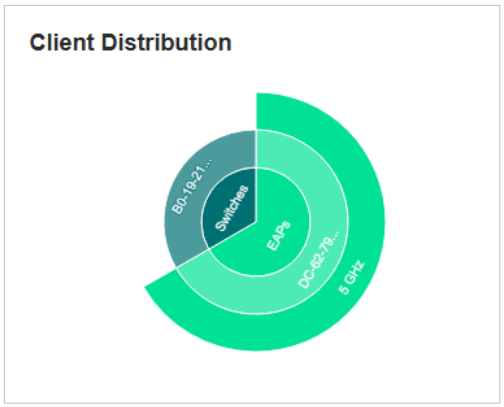
- **Traffic Distribution**

The Traffic Distribution widget uses a pie chart to display the traffic distribution on EAPs and switches in the site within the time range. Click the tab to display the statistic of EAPs or switches, and click the slice to view the total number of traffic, its proportion, and the device name.



- **Client Distribution**

  The Client Distribution widget uses a sunburst chart to display the real-time distribution of connected clients in the site. The chart has up to three levels. The inner circle is divided by the device category the clients connected to, the middle is by the device name, and the outer is by the frequency band. You can hover the cursor over the slice to view specific values.



- **Traffic Activities**

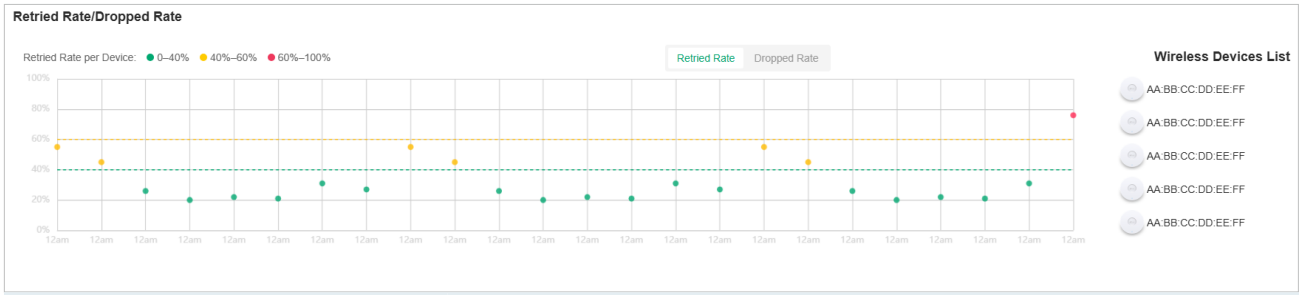
  The Traffic Activities widget displays the Tx and Rx data of EAPs and switches within the time range. Only activities of the devices in the connected status currently will be counted.

  Click the tab to display the statistic of EAPs or switches, and move the cursor on the line chart to view specific values of traffic. For detailed statistics of certain devices within a time range, refer to 8. 2 View the Statistics of the Network.



- **Retried Rate/Dropped Rate**

  The Retried Rate/Dropped Rate widget displays the rate of retried and dropped packets of the connected EAPs within the time range. Select an AP from the list and click the tab to display the chart of retried rate or dropped rate. You can move the cursor on the point to view specific values.

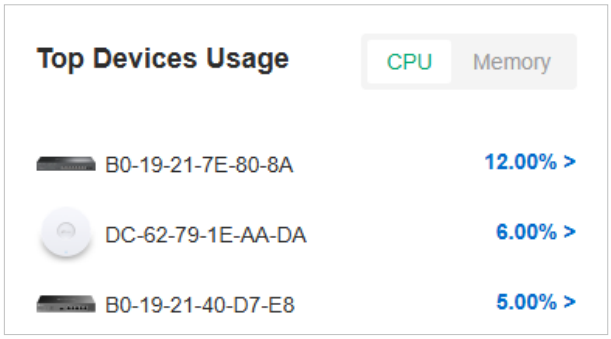


Retried Rate	Displays the percentage of packets that needed to be re-sent because they were corrupted upon arriving at the proper destination.

Dropped Rate	Displays the percentage of packets that were dropped before reaching their intended destination.

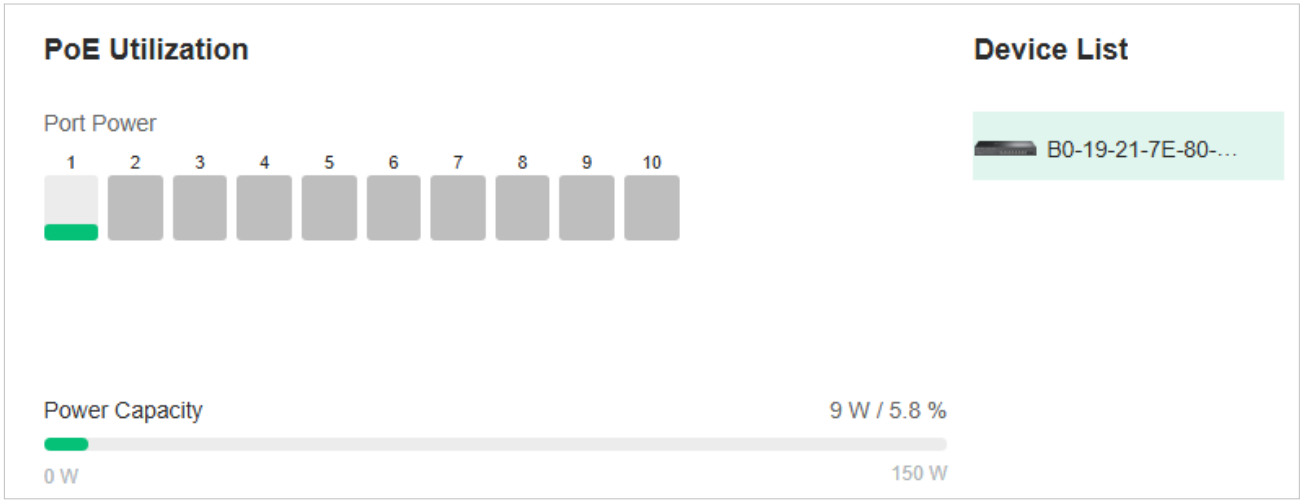
- **Top Devices Usage**

  The Top Devices Usage widget displays the CPU utilization and memory utilization of devices within the time range. Click the tab to select the CPU or memory for display. Click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to 6 Configure and Monitor Controller-Managed Devices.



- **PoE Utilization**

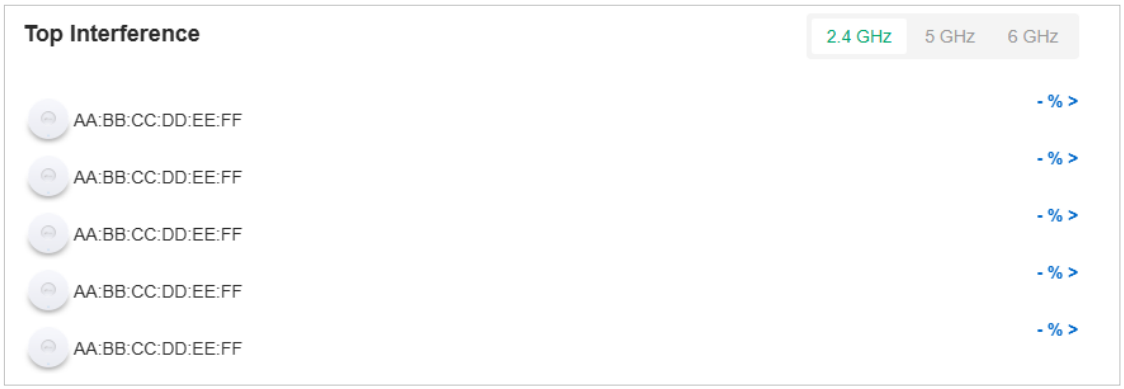
  The PoE Utilization widgets describes the PoE utilization of a switch. Select a switch from the switch list to display the ports connected to PoE devices. You can hover the cursor over a certain port to view specific values. The bar below displays the current power capacity provided by PoE and its proportion of the PoE budget.



- **Top Interference**

  The Top Interference widget displays the environment interference of wireless products. Click the tab to select the band. Click the traffic number in the widget to open the device's Properties window

for further configurations and monitoring. For details, refer to 6 Configure and Monitor Controller-Managed Devices.



Client

Client widgets use lists and charts to illustrate the traffic status of wired and wireless clients in the site.

- **Most Active Clients**

  The Most Active Clients widget can display most active clients. Only the clients in the connected status currently will be displayed.

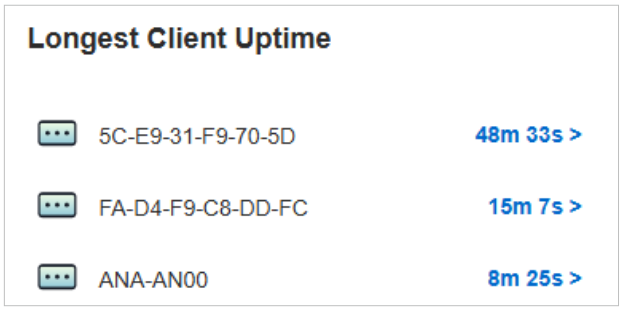
  To view all the clients connected to the network, click See All to jump to the Clients section. You can also click the traffic number in the widget to open the client's Properties window for further configurations and monitoring. For details, refer to 7.1 Manage Wired and Wireless Clients in Clients Page.



- **Longest Client Uptime**

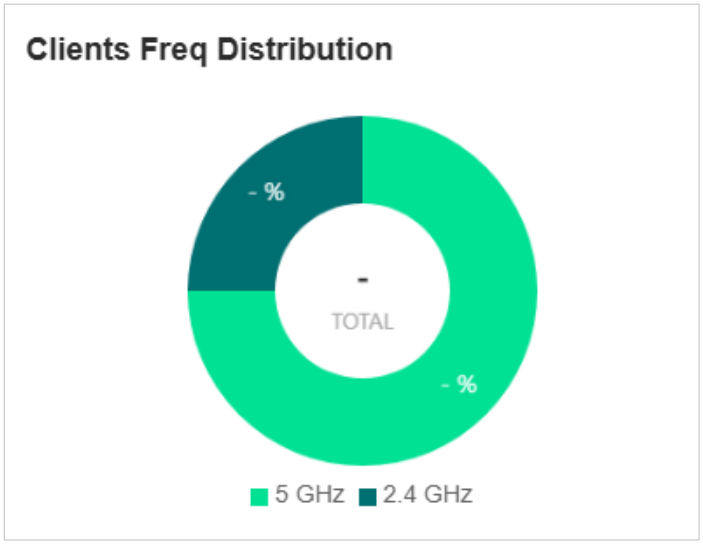
  The Longest Client Uptime widget can display top clients sorted by the uptime. Only the clients in the connected status currently will be displayed. You can also click the uptime in the widget to open

the client's Properties window for further configurations and monitoring. For details, refer to 7.1 Manage Wired and Wireless Clients in Clients Page.



- **Clients Freq Distribution**

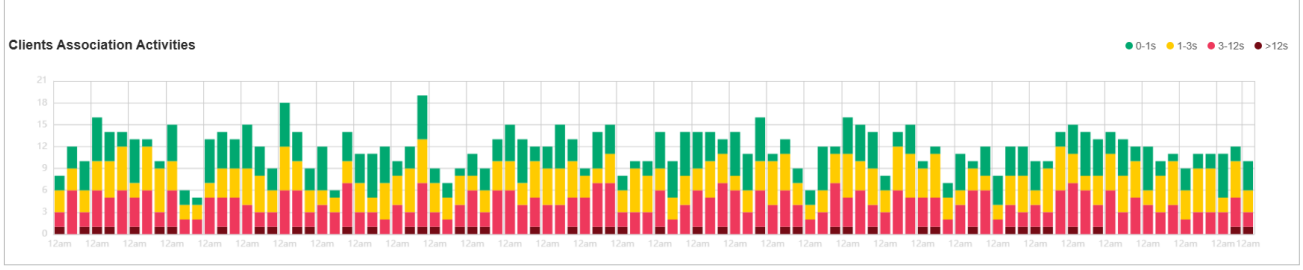
  The Clients Freq Distribution widget uses a donut chart to display the distribution of wireless clients connected to the bands in the site. The chart has two levels. The inner circle shows the total number of wireless clients, and the outer displays the proportion of clients that connect to the two bands. You can hover the cursor over the slice to view the number of clients in a band.



- **Clients Association Activities**

  The Clients Association Activities widget displays how the number of client connected to EAPs changes over time and the duration during which the clients communicate with the EAPs. In the stacked chart, you can easily compare the total number of clients and analyze the variation of each time period.

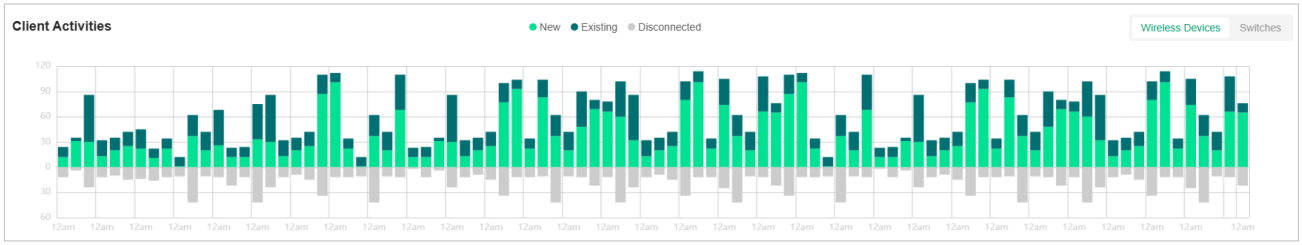
  The total value of a column shows the total number of clients connected to EAPs in this time period, and the segments in four colors represents the client number of different durations in specific time.



- **Client Activities**

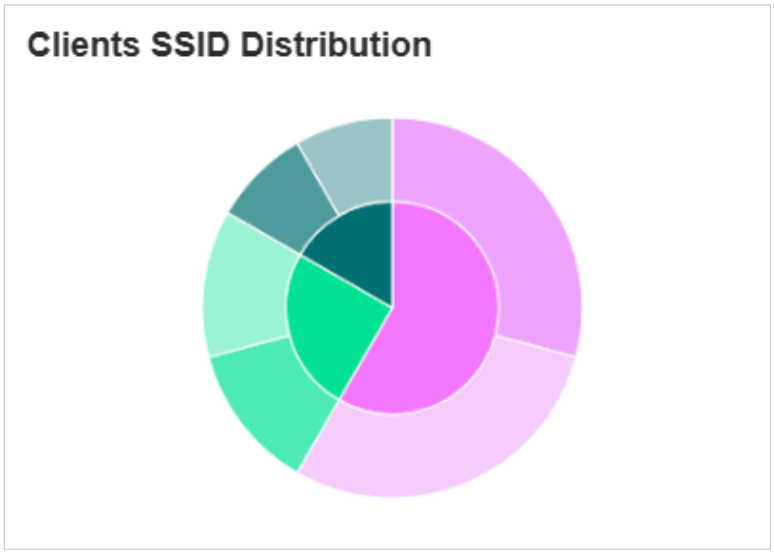
  The Client Activities widget displays how the number of connected client changes over time within the time range. In the stacked chart, you can easily compare the total number of clients and analyze the variation of each time period.

  The total value of a column shows the total number of connected clients in this time period, and the segments in three colors shows the change of client number compared with the last time period. Blue represents the newly connected clients, orange is the clients have been connected in the last period, and gray is the newly disconnected clients.



- **Clients SSID Distribution**

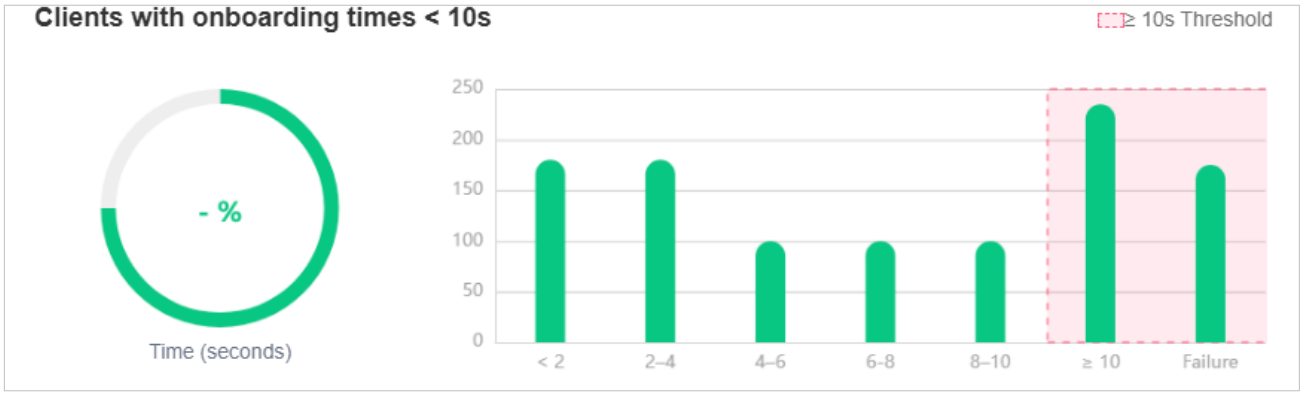
  The SSID Distribution widget uses a sunburst chart to display the distribution of wireless clients connected to the different SSIDs in the site. The chart has two levels. The inner circle is divided by the EAP's SSID that the clients connected to, and the outer is by the frequency band. You can hover the cursor over the slice to view the number of clients connected to the SSID in a band. Click a certain SSID to further display the statistics of its band frequency distribution.



- **Clients with Onboarding Times**

  The Clients with Onboarding Times widget describes the time wireless clients uses when connecting to a certain SSID. The donut chart on the left shows the proportion of clients that uses less than

10 seconds to connect to the devices. The line graph on the right displays the number of clients according to the different time that the clients takes to connect to the SSIDs.



- **Clients with RSSI**

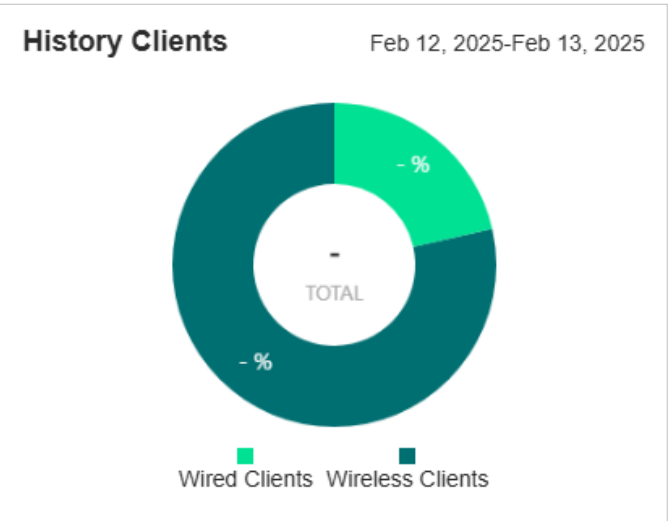
The Clients with RSSI widget describes the RSSI (Received Signal Strength Indication) that wireless clients experience in the environment. RSSI is a negative value measuring the power level being received after any possible loss at the antenna and cable level. The higher the RSSI value, the stronger the signal. The donut chart on the left shows the proportion of clients whose RSSI value is bigger than -72 dBm. The line graph on the right displays the number of clients according to the different range values of RSSI.



- **History Clients**

This widget uses a donut chart to display the distribution of wired and wireless clients in the site. The chart has two levels. The inner circle shows the total number of clients, and the outer displays

the proportion of each client type. You can hover the cursor over the slice to view the number of a client type.



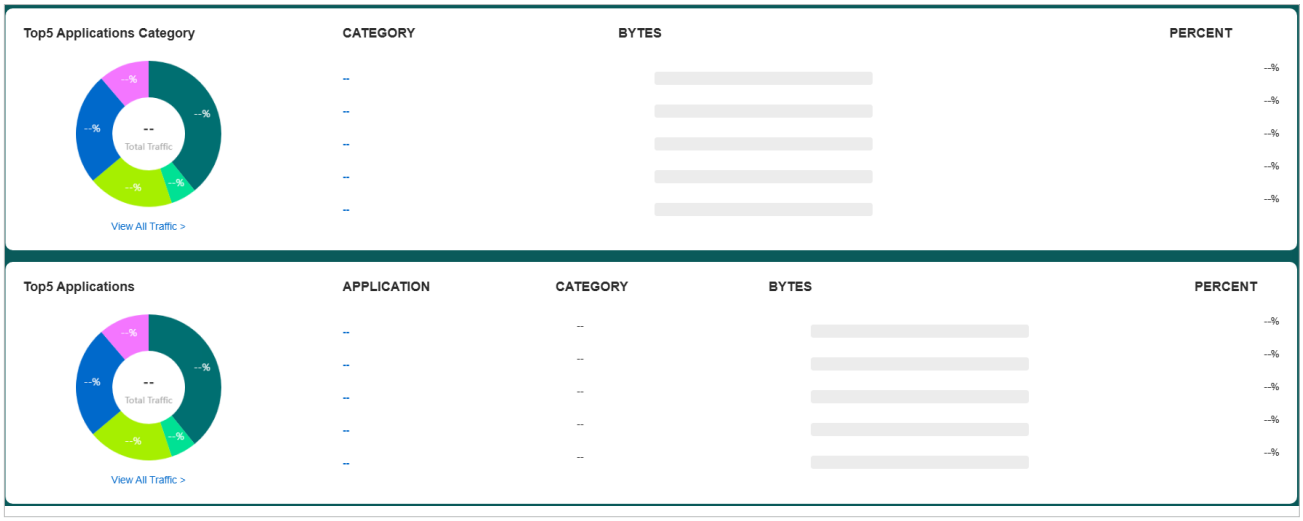
AppFlow

AppFlow widgets use lists and charts to illustrate the application information in the site.

- **Top Application Categories / Top Applications**

  These two widgets display top application categories and top applications in the site.

  To view detailed traffic information, click View All Traffic to go to the Application Analytics page. A DPI-supported gateway is required for detailed traffic information.



8. 2 View the Statistics of the Network

Statistics provides a visual representation of device data in the SDN Controller. You can easily monitor the network traffic and performance under the following tabs, Performance, Switch Statistics, and Speed Test Statistics.

8. 2. 1 Performance

In Performance, you can view the device performance in a specified period by graphs, such as user counts, CPU and memory usage, and transmitted and received packets. The graphs vary due to the device type and status.

Tab Bar

The tabs and calendar on the top are used to specify the displayed statistics.



	Click to select a device from the drop-down list to view its statistics. The tabs vary due to the type of the selected device.
	Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right. The available time range is restricted by the time interval. Before selecting a long time range, select Hourly or Daily as the time interval.
	Select 5 minutes, Hourly, or Daily to specify the time interval of the data. When selecting a long time range, a longer time interval is recommended for a better view.
	(For an AP) Click to select the band of the AP to view the statistics.

- **Gateway Statistics**

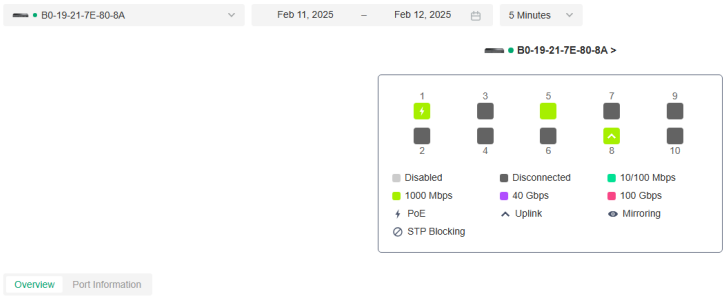
  Click to select the port of the gateway on the tab to view the statistics.

- **Switch Statistics**

  Click Overview to view the general switch statistics, or click Port Performance and select a tab to view the port statistics.

For a switch, you can view the current status of ports and its traffic statistics in the specified time range via a monitor panel and graphs.



Port Status

Disabled	The port is Disable. To enable it, go to the Devices page.
Disconnected	The port is enabled but connects to no devices or clients.
1000 Mbps	The port is running at 1000 Mbps.
10/100 Mbps	The port is running at 10/100 Mbps.
PoE	A PoE port connected to a powered device (PD).
Uplink	An uplink port connected to WAN.
Mirroring	A mirroring port that is mirroring another switch port.
STP Blocking	A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.

Tabs

Sort: Natural	Select Natural, Transmitted, Received, or Total to specify the graph order of ports. Natural: Displays the line graphs in ascending order of the port number. Transmitted: Displays the line graphs in descending order based on the traffic volume of transmitted packets. Received: Displays the line graphs in descending order based on the traffic volume of received packets. Total: Displays the line graphs in descending order based on the total traffic volume of transmitted and received packets.
Rate Traffic Packets	Specify the data type. Rate: Displays the traffic rate. Traffic: Displays the traffic statistics. Packets: Displays the total number of packets.

All Broadcast Multicast	If you select Packet, click the tab to specify which type of packet statistics to be displayed. All: Displays statistics of all packets, including broadcast and multicast packets. Broadcast: Displays statistics of broadcast packets only. Multicast: Displays statistics of multicast packets only.

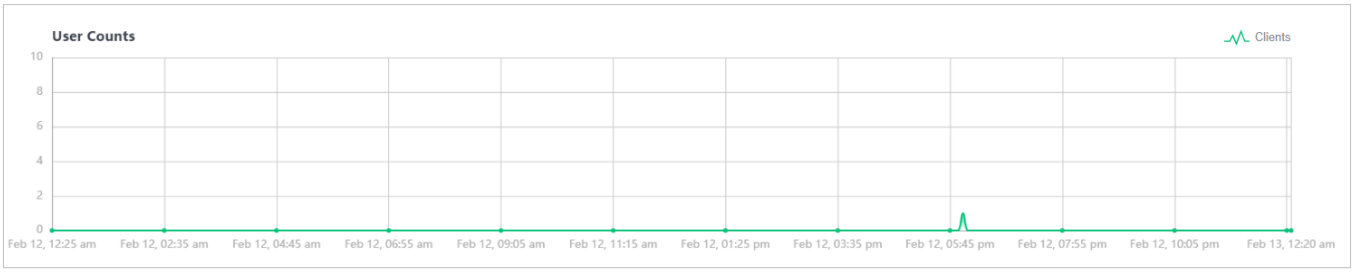
Statistical Graphs

Statistical graphs vary according to the type of devices. The chart below shows the statistical graphs which correspond to the gateway, switch, and AP.

Gateway	User Counts, Usage, Traffic, Packets
Switch	User counts, Usage, Port Port Information Graphs
AP	User Counts, Usage, Traffic, Packets, Packets, Multicast/Broadcast Packets, Dropped, Errors, Retries

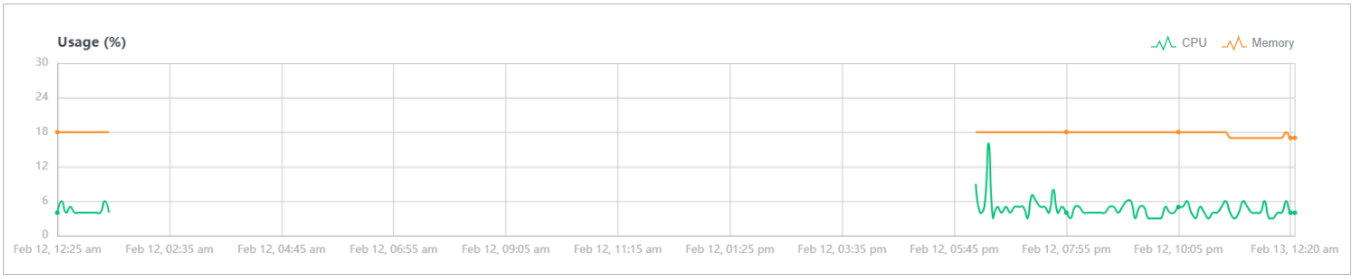
■ User Counts

The User Counts graph displays the number of users connected to the devices during the selected time range. Hover the cursor over the line to display the specific values.



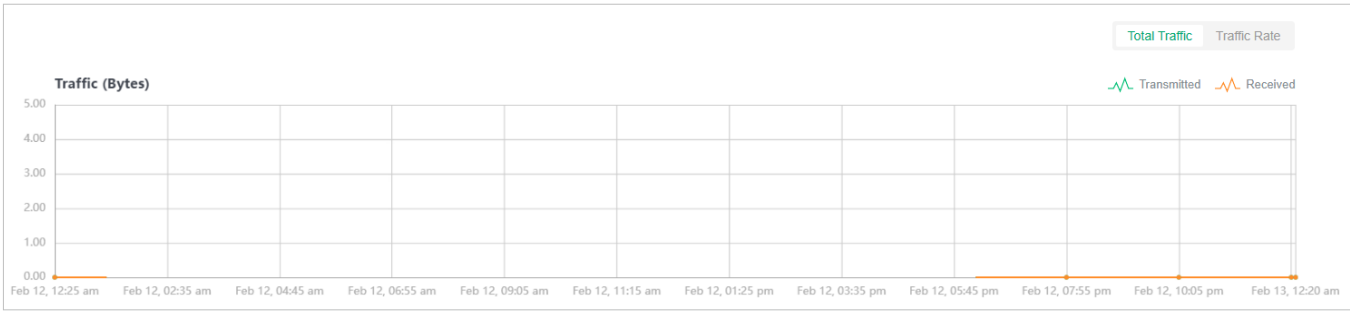
■ Usage

The Usage graph uses the orange line and yellow line to display the percentage of CPU usage and used memory during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



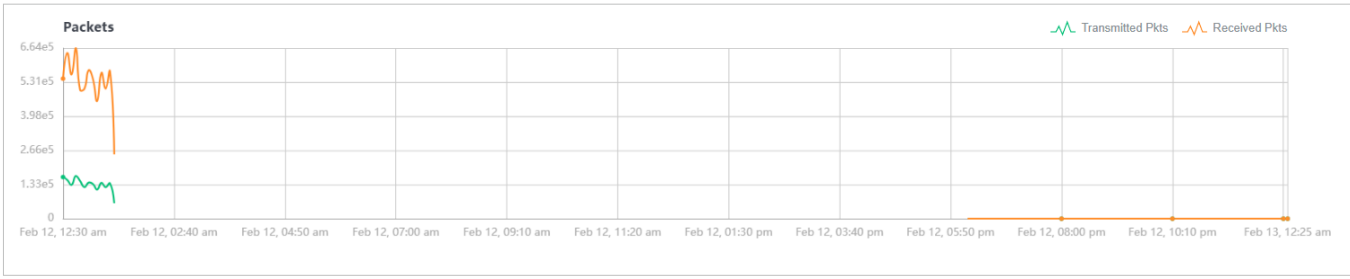
Traffic

The Traffic graph uses the dark blue line and light blue line to display the bytes of data transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



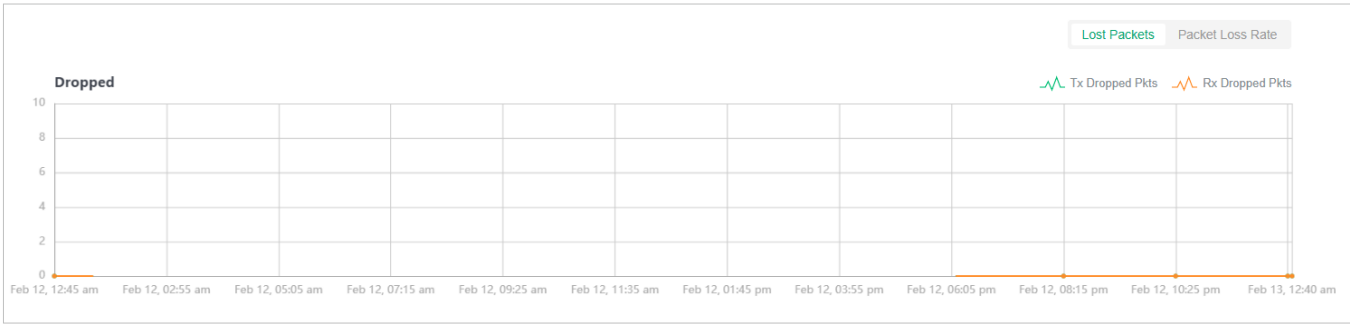
Packets

The Packets graph uses the dark blue line and light blue line to display the number of packets transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



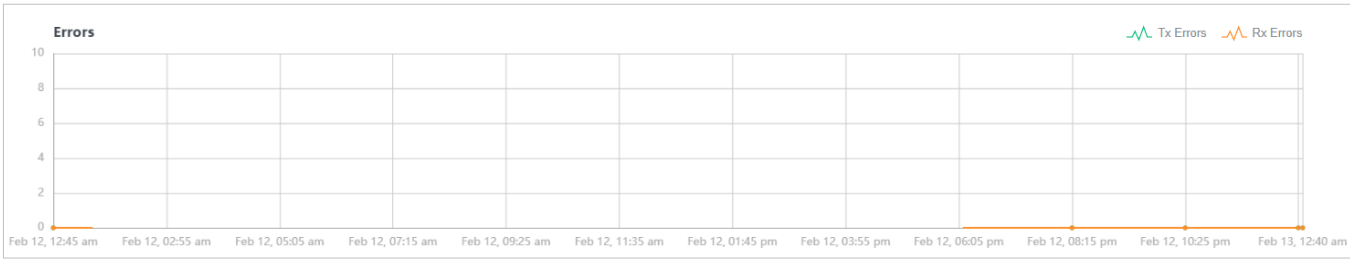
Dropped

The Dropped graph uses the dark blue line and light blue line to display the number of dropped Tx packets and Rx packets during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



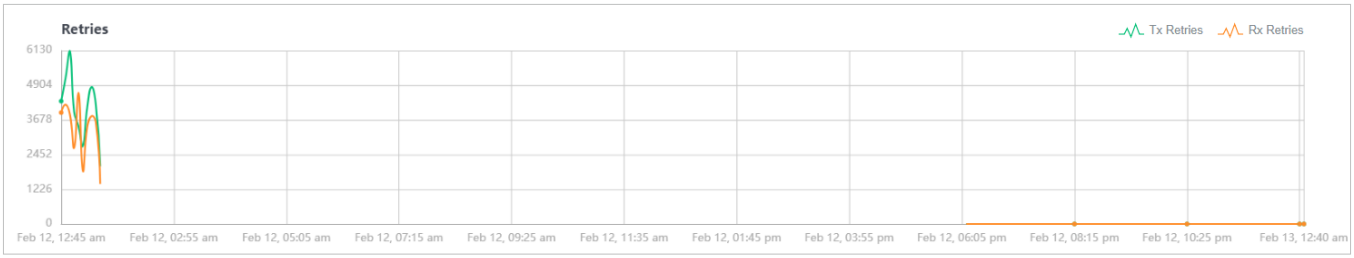
- **Errors**

The Errors graph uses the dark blue line and light blue line to display the number of error packets sent to AP and received by AP during the selected time range, respectively. Hover the cursor over the line to display the specific values.



- **Retries**

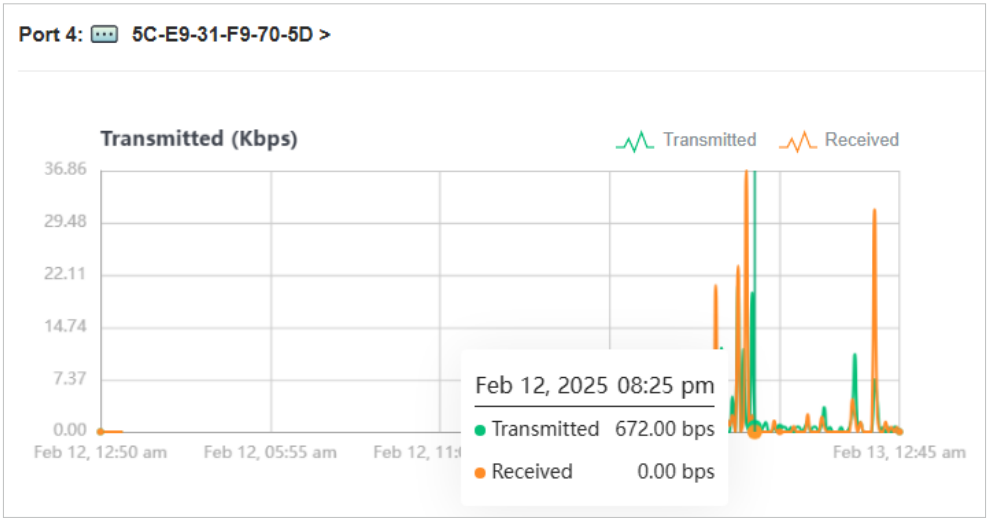
The Retries graph uses the dark blue line and light blue line to display the number of times that the data packets are transmitted again and received again during the selected period, respectively. Hover the cursor over the lines to display the specific values.



Port Information Graphs (only for Switches)

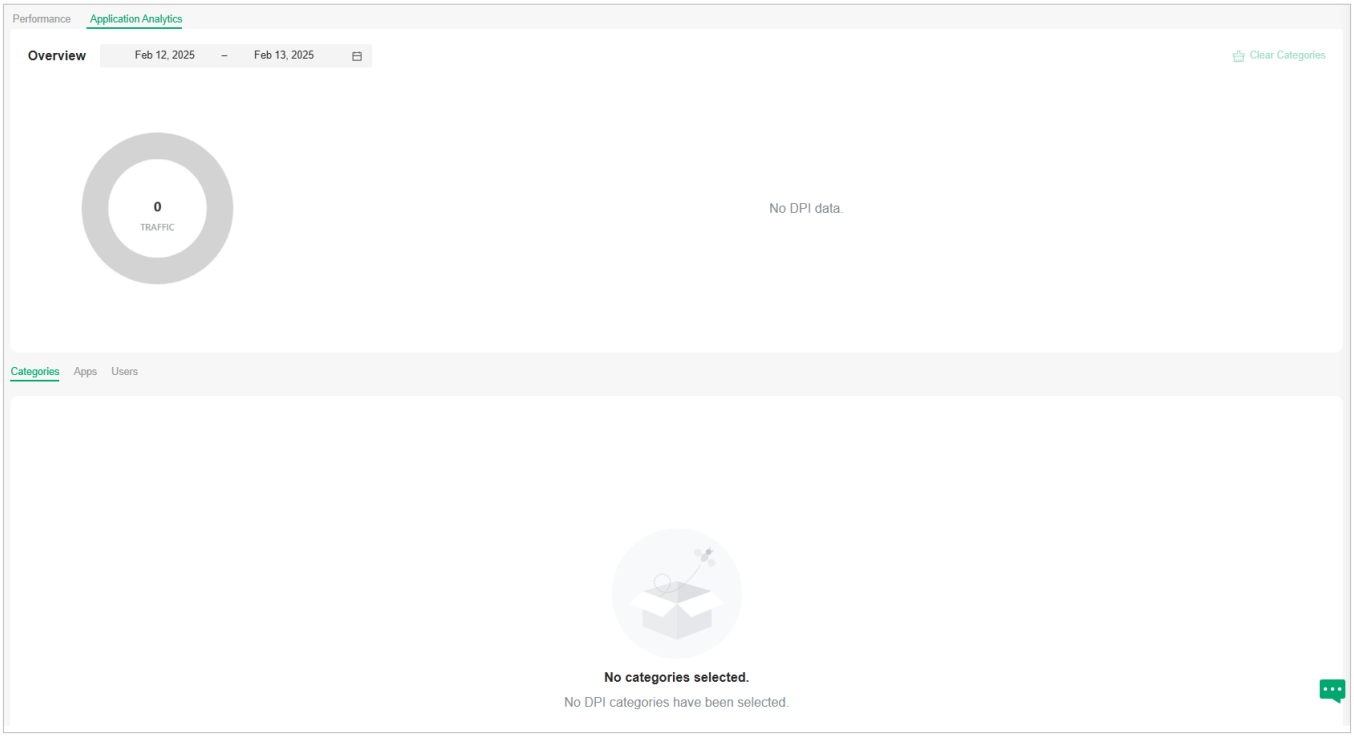
Port information graphs of a switch display the traffic statistics of active ports.

You can specify the data type by clicking the Rate Traffic Packets tabs. Colorful lines are used to indicate the transmitted and received statistics. Hover the cursor over the lines to display the specific values. To view and configure the device connected to the port, click the device name beside the port number.



8. 2. 2 Application Analytics

In Application Analytics, you can view detailed traffic information in a specified period by graphs.

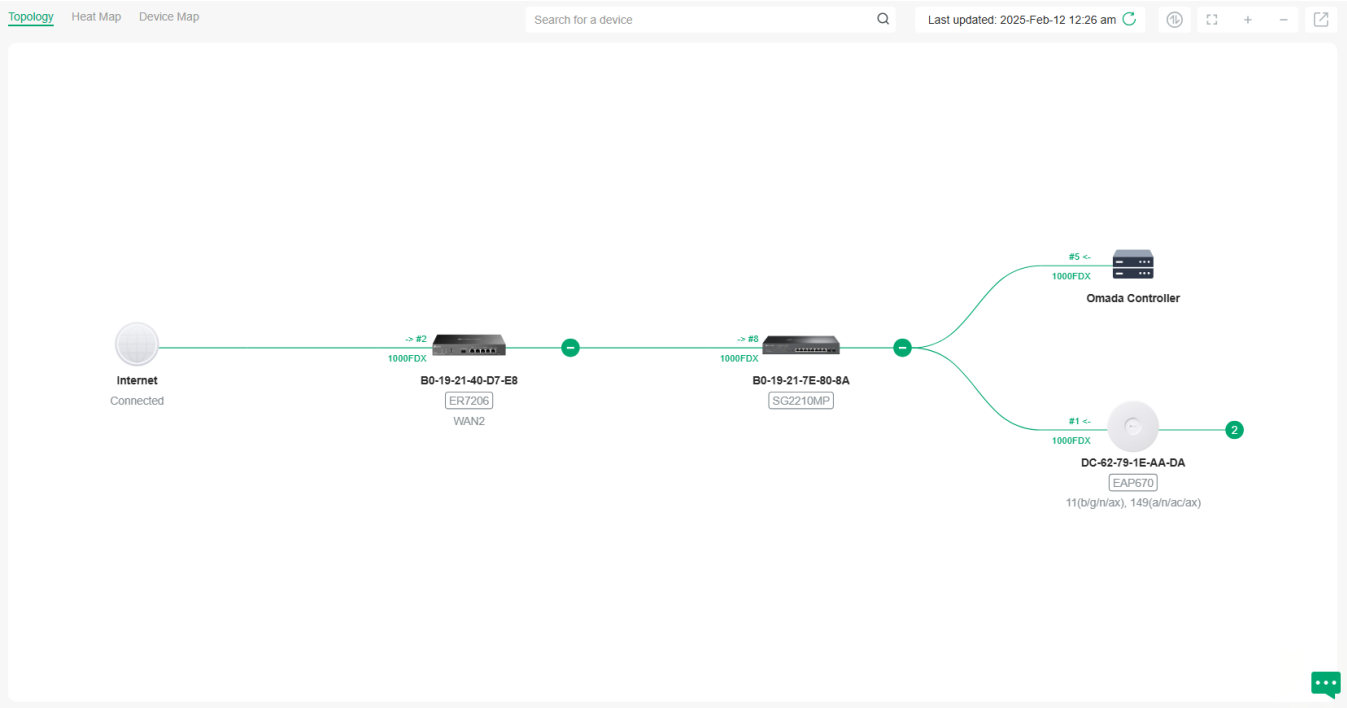


8. 3 Monitor the Network with Map

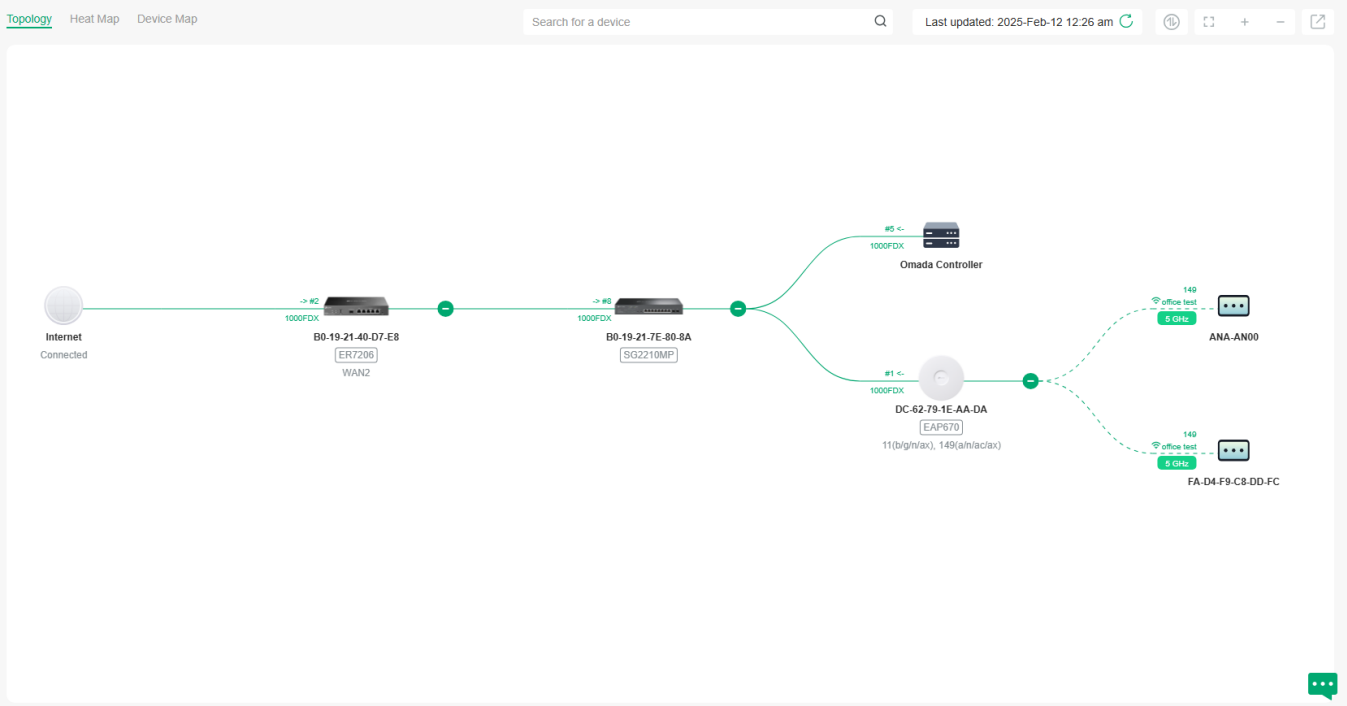
With the Map function, you can look over the topology and device provisioning of network in Topology, customizes a visual representation of your network in Heat Map, and visually display the geographic location of each device and site in Device Map and Site Map.

8. 3. 1 Topology

Go to Map > Topology, and you can view the topology generated by the controller automatically. You can click the icon of devices to open the Properties window. For detailed configuration and monitoring in the Properties window, refer to 6 Configure and Monitor Controller-Managed Devices.



For a better overview of the network topology, you can control the display of branches, the size of the diagram, and the link labels.



- **Display of Branches**

  The default view shows the all devices connected by solid and dotted lines. Click the icon of the client group to view clients connected to the same device. Click the nods ⊕ to unfold or ⊖ to fold the branches.

- **Diagram Size**

  Click the icons at the right corner to adjust the size of the topology and view the legends.

	Click to fit the topology to the web page.
	Click to zoom in the topology.
	Click to zoom out the topology.
	Click to view the meaning of lines in the topology. Solid and dotted lines are used to indicate wired and wireless connections, respectively, and four colors are used to indicate the link speed.

- **Link Labels**

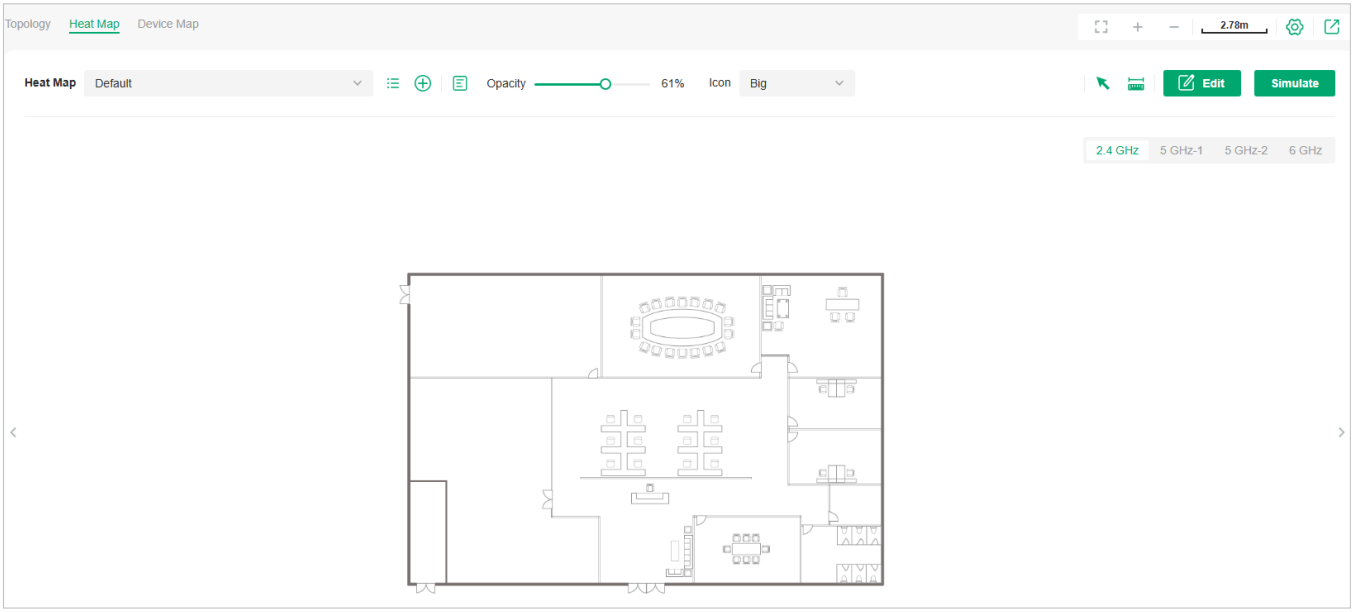
  Click Link Labels at the left corner, and labels will appear to display the link status. Information on the labels varies due to the link connections.

	(For the WAN port of the gateway connected to the internet) Displays the port name, link speed and duplex type.

-> #8 1000FDX	(For simple wired connections) Displays the connected port number, link speed, and duplex type. Note that only the switch's port number can be displayed in the label.
LAG1#4,5 <->LAG2#7,8 1000 FDX	(For Link Aggregation) Displays the LAG ID, port number of LAG members, LAG speed, and duplex type.
↑360Mbps ↓400Mbps 100% (-35dBm)	(For wireless connections between APs) Displays the negotiation rate of uplink and downlink and the RSSI (displayed in percentage and dBm).
149 office test 5 GHz	(For wireless connections between clients) Displays the connected SSID, wireless channel of AP, and its signal strength.

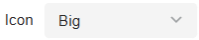
8. 3. 2 Heat Map

Go to Map > Heat Map, and a default map is shown as below. You can upload your local map images and add devices and different types of walls to customize a visual representation of your network.



Click the following icons to add, edit, and select the map. After selecting a map, click and drag in the devices from the Devices list to place it on the map according to the actual locations.

Heat Map Default	Click to select a map from the drop-down list to place the devices.
	Click to edit maps in the pop-up window. Click the edit icon to edit the description and layout of the map. Click the delete icon to delete the map.

	Click to add a map. In the pop-up window, enter the description, select the layout, and upload an image in the .jpg, .jpeg, .gif, .png, .bmp, .tiff format.
	Adjust the opacity of the map.
	Click to select the icon size displayed on the map.
	Click to use the selection tool to select the elements including walls and devices on the map.
	Click to use the measurement tool. Draw a line on the map to measure the actual distance according to the map scale.
	Click to edit the elements including walls and devices on the map.
	Click to simulate the network heat map. Note: It is required to click Simulate to generate a new heat map after editing elements on the map.
	Click to fit the map to the web page.
	Click to zoom in the map.
	Click to zoom out the map.
	Click to set the map scale. Draw a line on the map by clicking and dragging, and then define the distance of the line.
	Click to set the default height of the added devices and the information displayed on the map.
	Click to export the network coverage report.

Configuration

To generate a visual representation and heat map of your network, follow these steps:

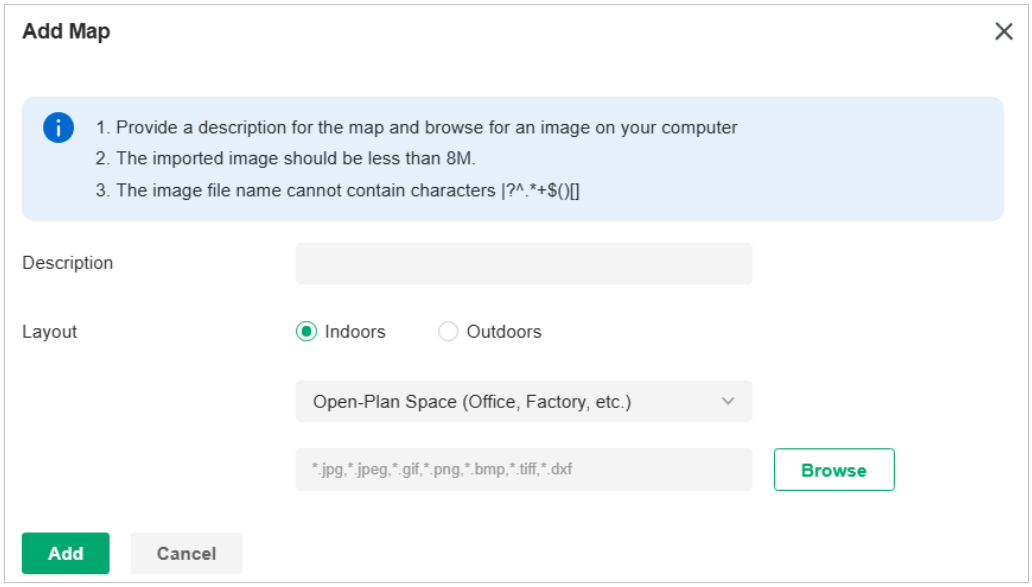
1) Add a map and configure the general parameters for the map.

2) Add devices and walls, and configure the parameters.

3) View simulation results.

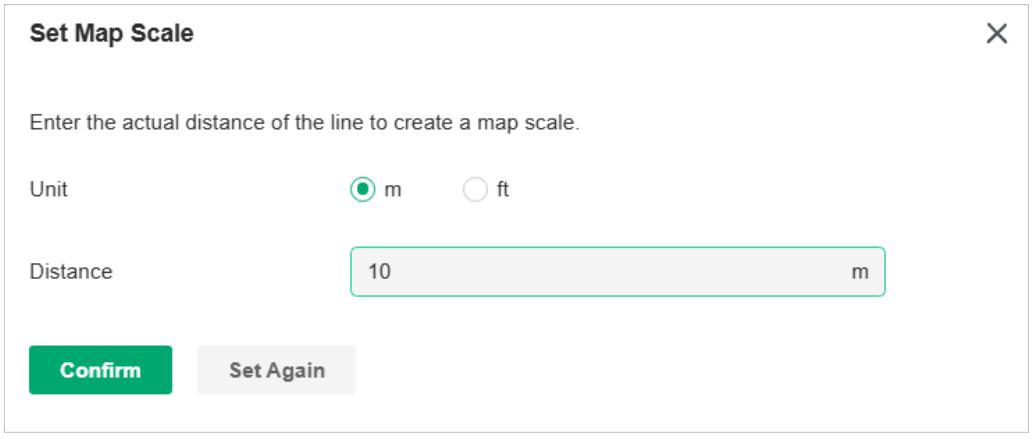
Step 1: Add Map

1. Go to Map > Heat Map and click ⊕ to add a new map. Then click Add.

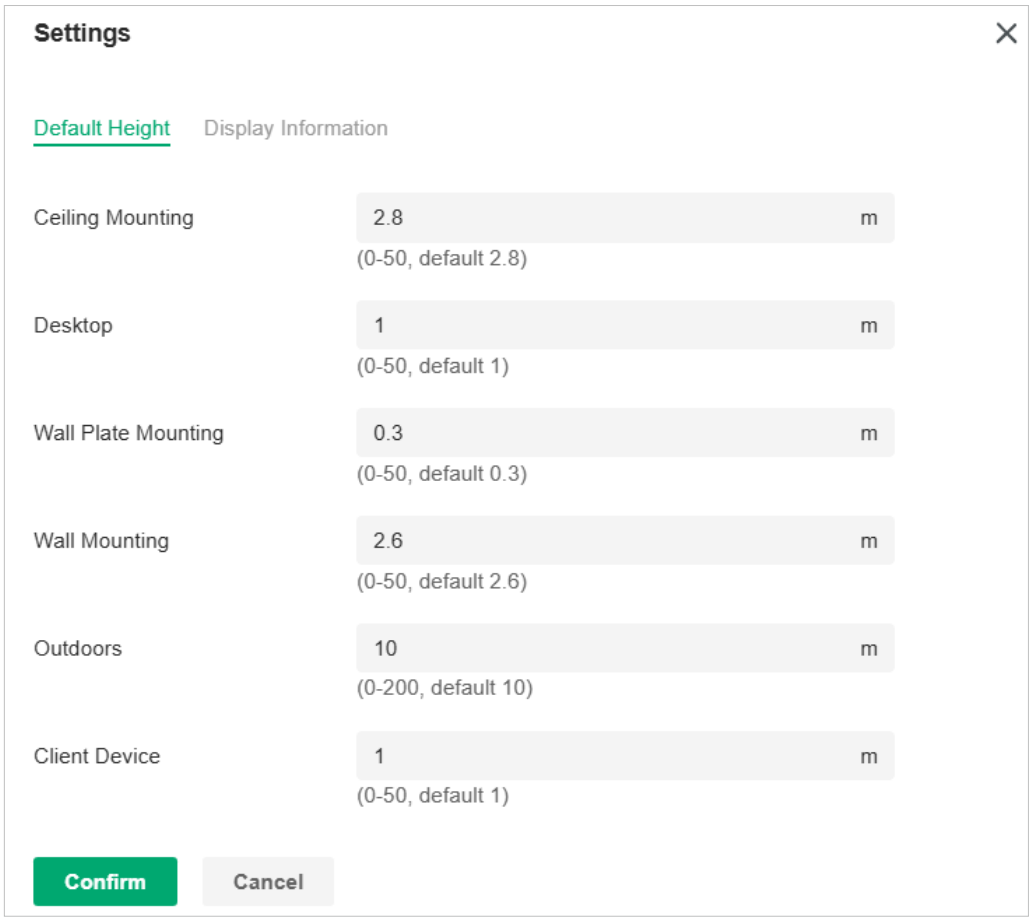


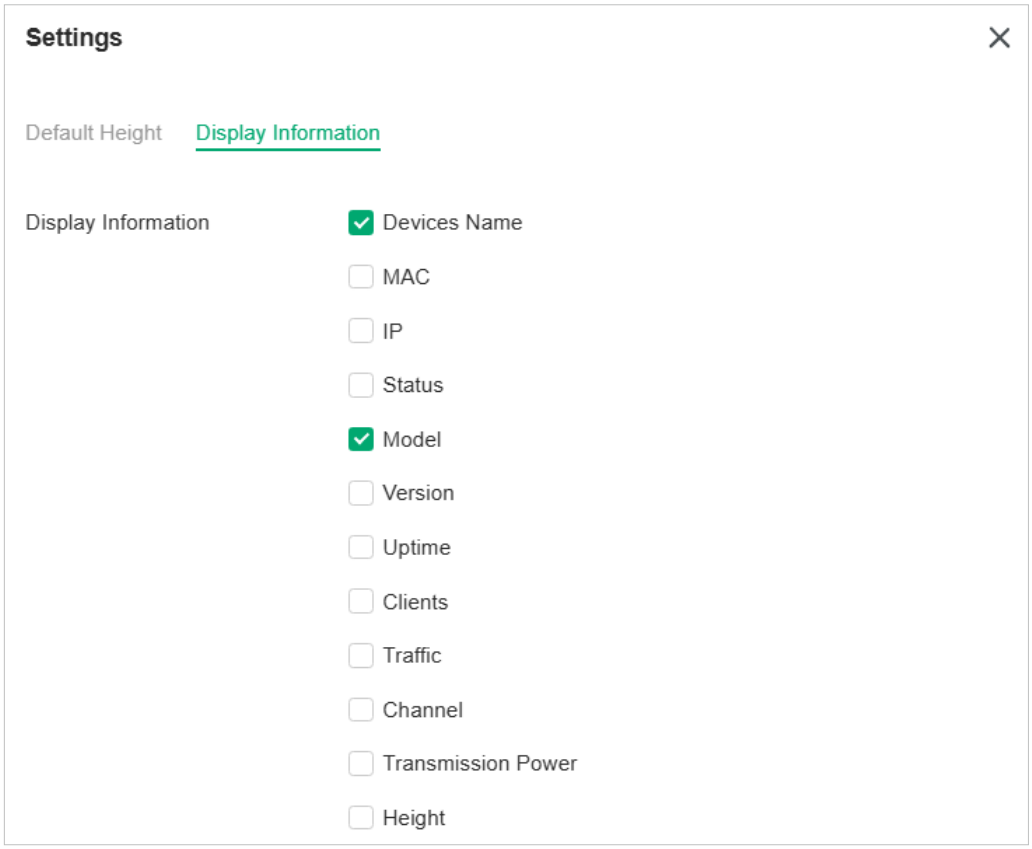
Description	Enter a description for the map.
Layout	Select the general layout of the map, which will make the simulation more accurate and the upload the map in the .jpg, .jpeg, .gif, .png, .bmp, .tiff, .dxf format. **Tip:** You can upload a CAD (.dxf) file, and the controller will automatically identify the walls in the layout.

2. Click the scale icon on the upper right to set a map scale. Draw a line on the map by clicking and dragging, and then define the distance of the line.



3. Click the settings icon to set the default height of the added devices and the information displayed on the map. Then click Confirm.

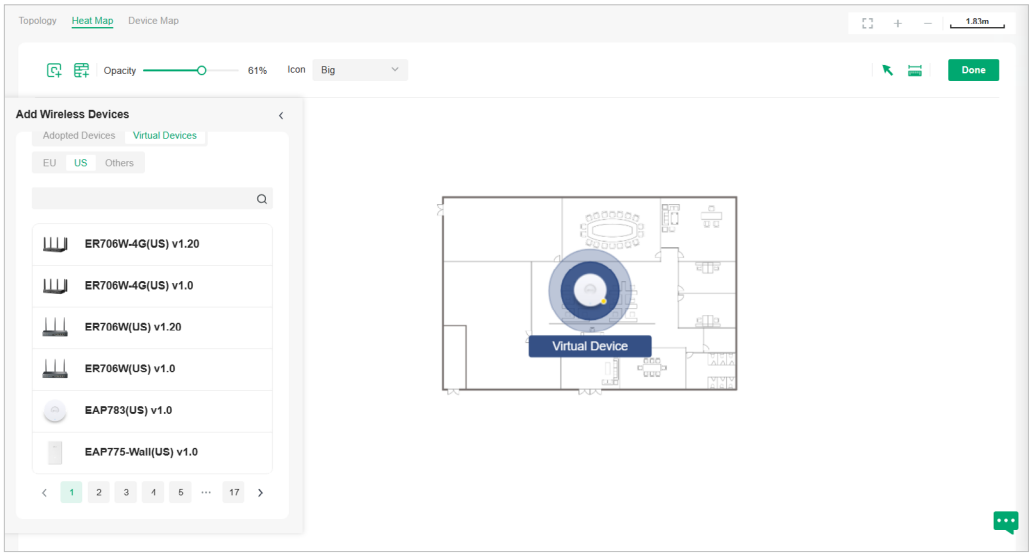




Default Height	Specify the default height for devices. You can change the height for individual device later.
Display Information	Select the information you want to see on the map.

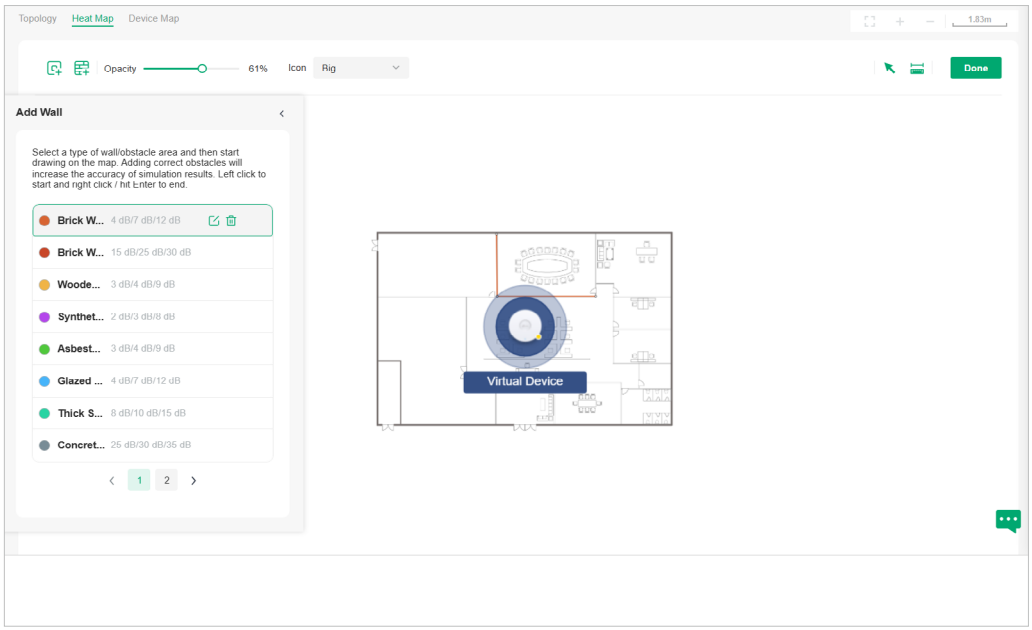
Step 2: Add Devices and Walls

1. Click the Edit icon to enter the editing status of the map.
2. Click the Add Wireless Devices icon on the upper left, and the list of adopted devices and virtual devices will appear. Drag the devices to the desired place on the map.



3. Click the Add Wall icon on the upper left. Select a type of wall/obstacle area and then start drawing on the map. Left click to start and right click / hit Enter to end.

   You can also edit the details parameters of the walls and obstacles, delete, and add walls. Adding correct obstacles will increase the accuracy of simulation results.



4. Click the Done icon to exit the editing status of the map.

Step 3: View and Export Results

It is required to click Simulate to generate a new heat map after editing elements on the map.

1. Click the Simulate icon to generate the heat map. You can adjust the receiver sensitivity, show signal strength, and view the simulation results according to your needs.



Show Signal Strength	Enable the feature, and you can move the cursor to view the signal strength of a specific location.
Show Simulation	Enable or disable the display of simulation results on the map.
2.4 GHz 5 GHz-1 5 GHz-2 6 GHz	Select 2.4GHz or 5GHz to view the simulation results of the band.
	Click and follow the instruction to specify an area to view the signal strength and the corresponding percentage.
Strong Receiver sensitivity -75 dBm Weak	Adjust the receiver sensitivity, and the new settings will take effect after refreshing the simulation.

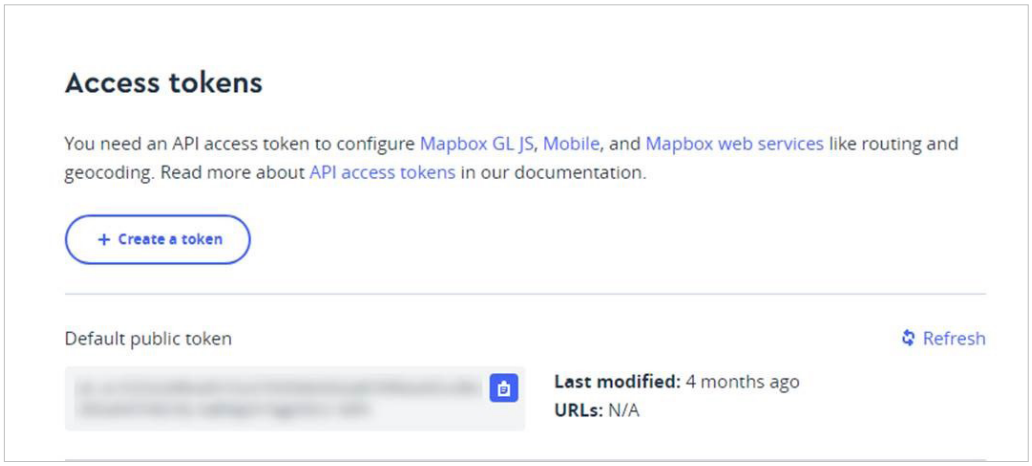
2. (Optional) If you want to export a network coverage report, click the Export icon on the upper right to export a report in .docx format.

8. 3. 3 Device Map

Prerequisite

A valid Mapbox API Access Token is required to use the Device Map function.

Visit https://www.mapbox.com, register an account, and obtain the default token on the account page.



Configuration

1. Launch the controller and access a site. Go to Map > Device Map.
2. Click Bind API Access Token, enter the Mapbox API Access Token you obtained, then click Apply.

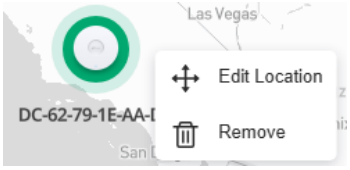


3. Use the map to manage your devices.

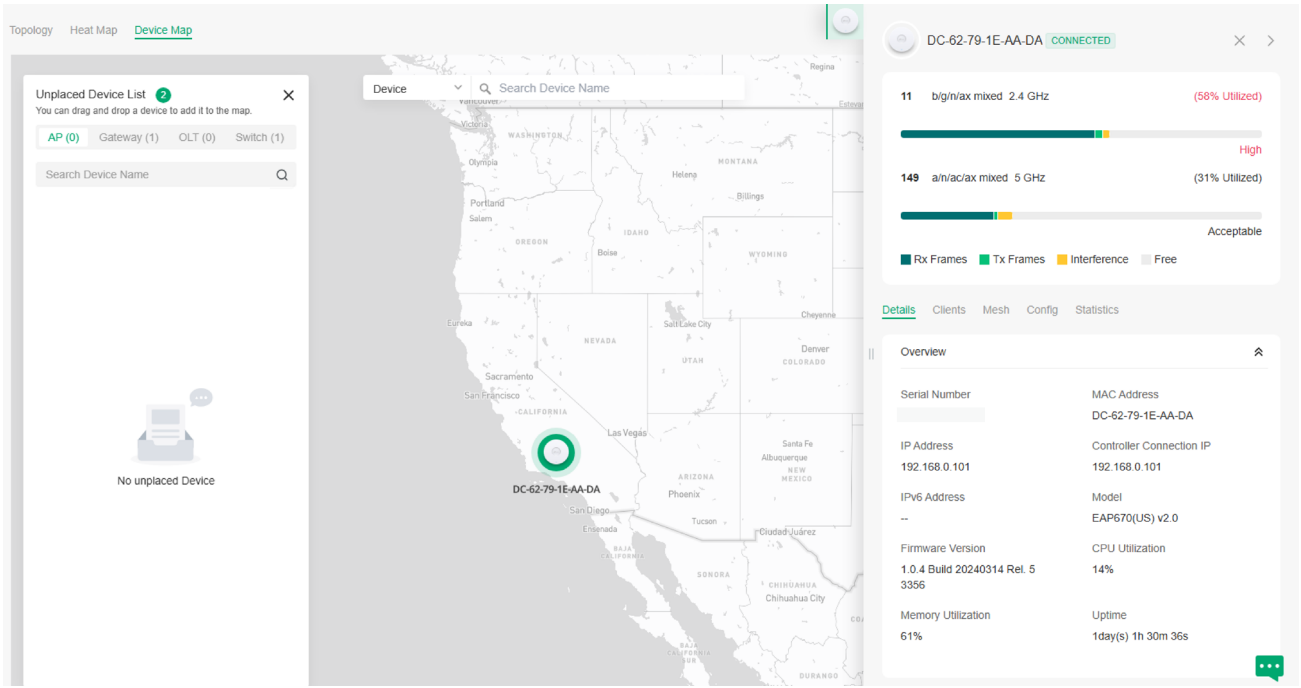


Unplaced Device List	Display a list of sites that are not marked on the map. You can drag and drop a site to add it to the map.
Search bar	Select a catogary and enter the keyword to search for a site or address.
	Click to change or unbind the Mapbox API Access Token.
	Zoom in and zoom out the map.
	Locate to current location.

Right-click a device icon to edit location or remove it from the map.



Click a device icon to view device info and edit settings.

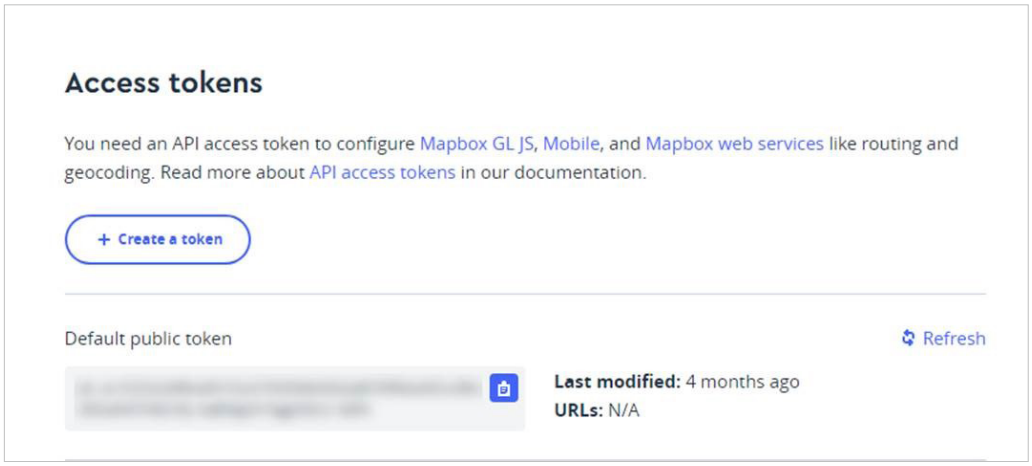


8. 3. 4 Site Map

Prerequisite

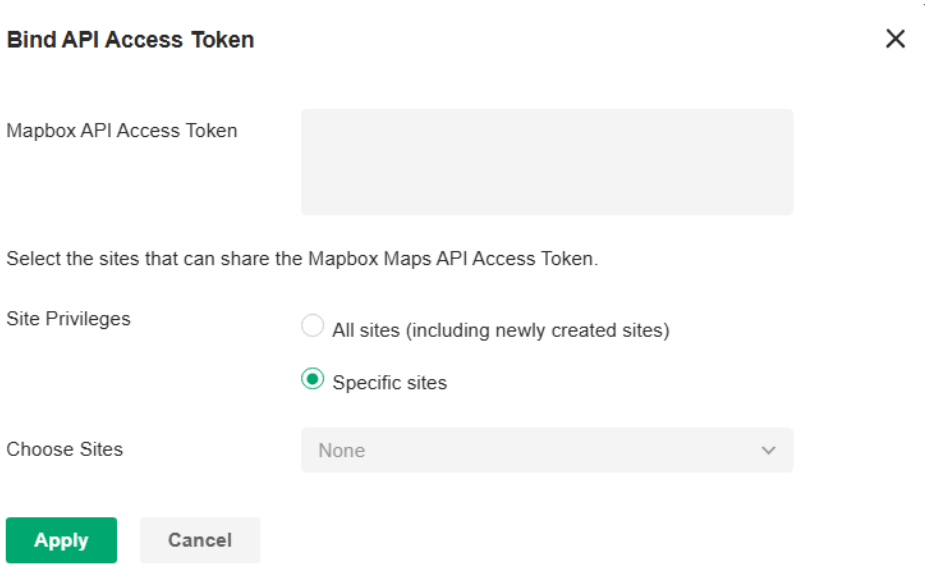
A valid Mapbox API Access Token is required to use the Site Map function.

Visit https://www.mapbox.com, register an account, and obtain the default token on the account page.

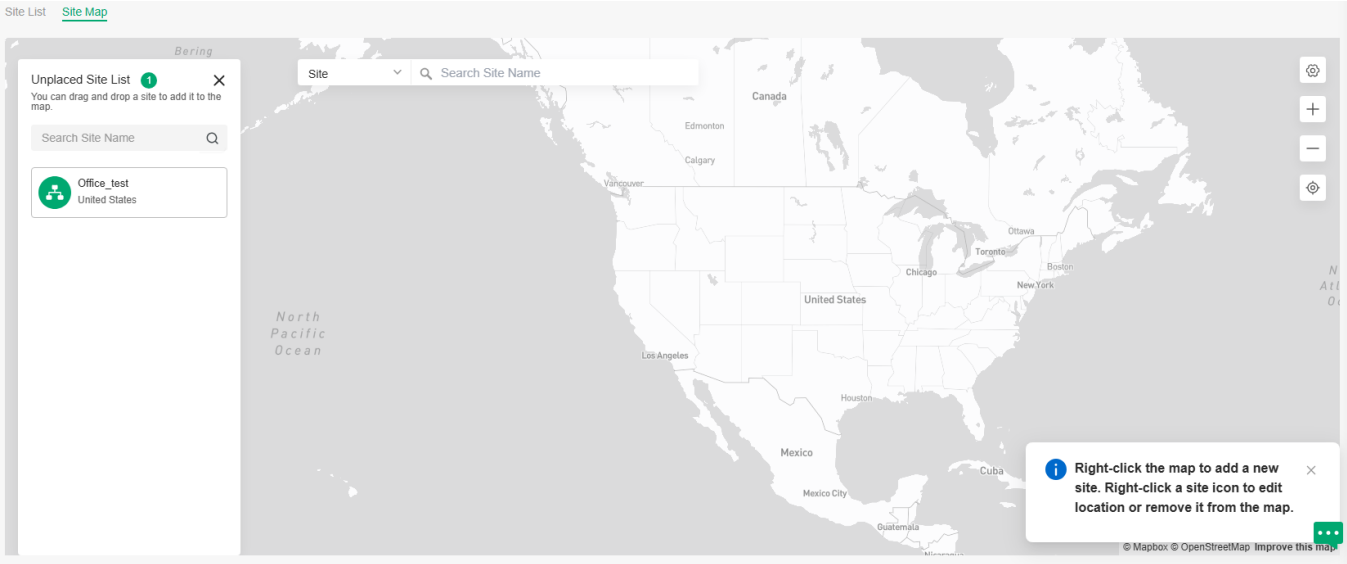


Configuration

1. Launch the controller and access the Global View. Go to Dashboard > Site Map.
2. Click Bind API Access Token, enter the Mapbox API Access Token you obtained, select the sites that can share the token, then click Apply.

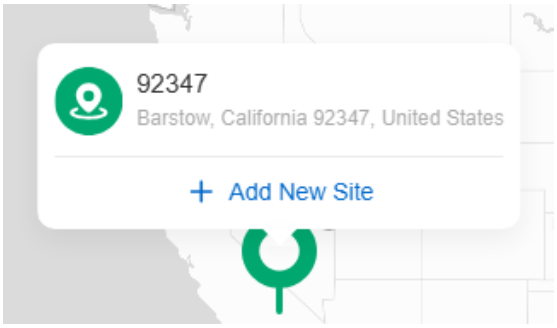


3. Use the map to manage your sites.

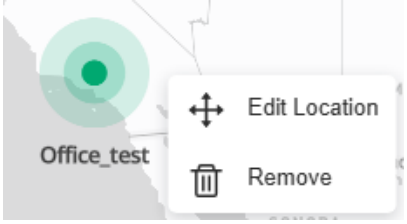


Unplaced Site List	Display a list of sites that are not marked on the map. You can drag and drop a site to add it to the map.
Search bar	Select a catogary and enter the keyword to search for a site or address.
	Click to change or unbind the Mapbox API Access Token.
	Zoom in and zoom out the map.
	Locate to current location.

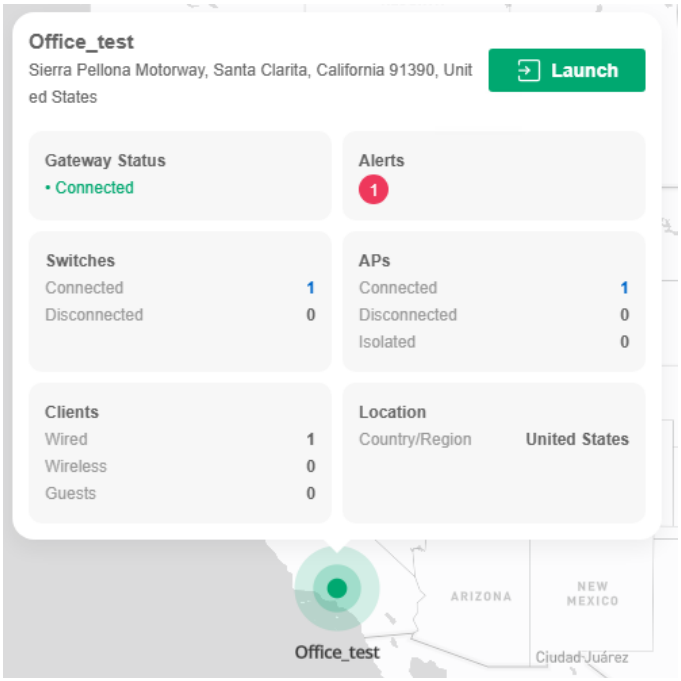
Right-click the map to add a new site.



Right-click a site icon to edit location or remove it from the map.



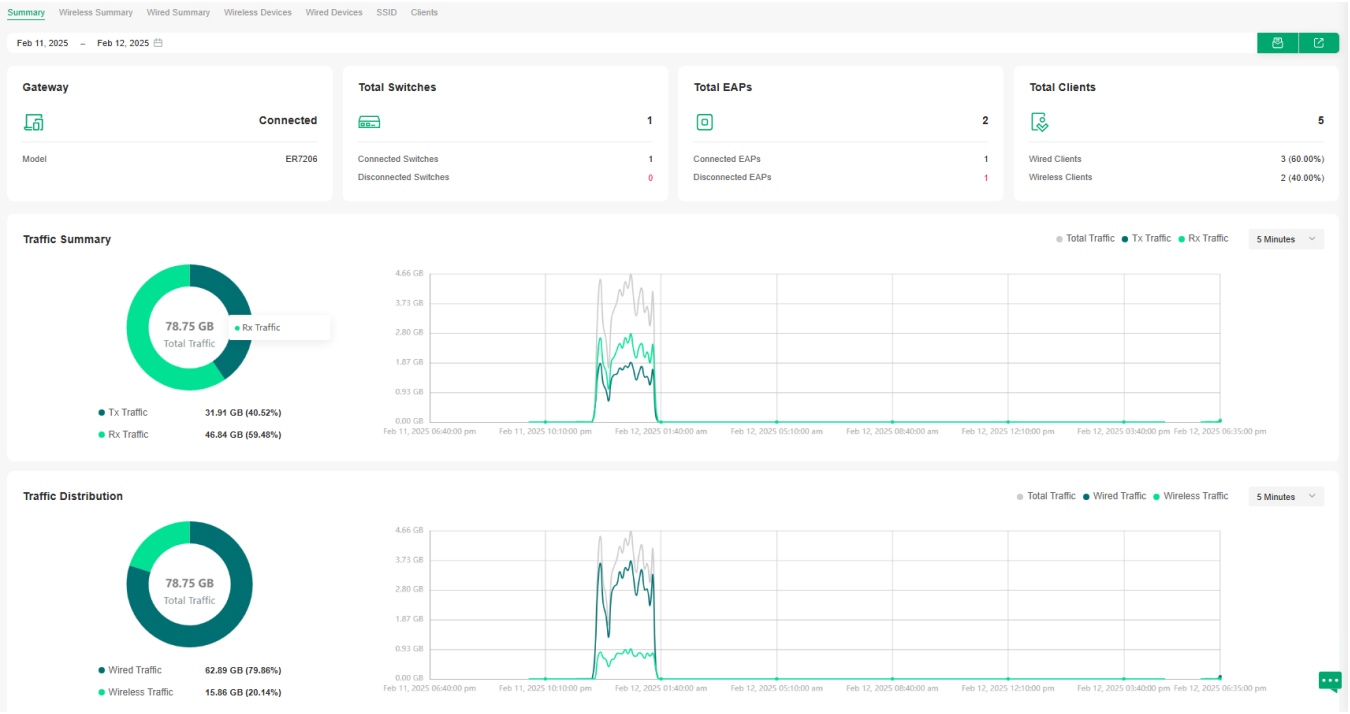
Click a site to view site info, and click Launch to access the site.



8. 4 Monitor the Network with Reports

Network Report shows the statistics of various network indicators and their changes over time, helping network administrators to intuitively and comprehensively understand the current and historical operating status of their network. Thus, it facilitates network administrators to decide whether the controller and devices needs to be upgraded and optimized. It also provides network administrators and SI with data support for reporting network conditions.

Go to Reports, and you can view the connection data of the devices in the topology and the statistics of various network indicators and their changes over time. Click the tabs on the top to view the statistics of specific section of the network.



Summary	Display the statistics summary of the whole network.
Wireless Summary	Display the wireless statistics summary of the whole network, including data related to APs, wireless clients, and wireless traffic.
Wired Summary	Display the wired statistics summary of the whole network, including data related to gateway, switches, wired clients, and wired traffic.
Wireless Devices	Display details of APs in the network, including AP Traffic, CPU Utilization, Memory Utilization, Total Clients, Alerts, and Reboot Times.
Wired Devices	Display details of gateway and switches in the network, including Traffic, CPU Utilization, Memory Utilization, Total Clients, Alerts, and Reboot Times.
SSID	Display the statistics of SSIDs in the network, including Traffic, Total Clients, and Activities.
Clients	Display the statistics of Clients in the network, including Distribution, Client Activities, and Client Numbers.

When you are accessing the controller locally, you can export the network report or send the report via email by clicking the icons on the upper right.

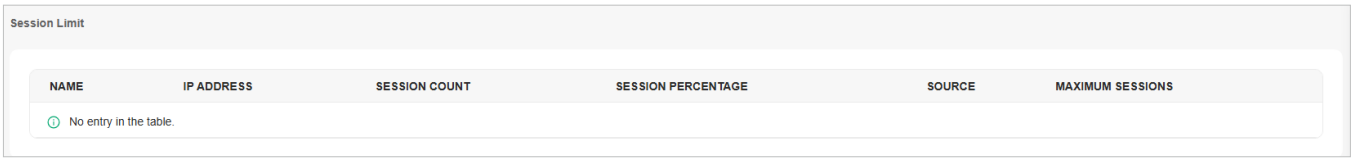
	Click to send the report via email. Both Send Now and Send Schedule are available.
	Click to export and the network report locally. Note that for Linux system, please install Chromium before exporting the network report and make sure you can run Chromium as root.

8. 5 View Statistics During Specified Period with Insight

In the Insight page, you can monitor the site history of connected clients, portal authorizations, and rouge APs. For a better monitoring, you can specify the time period and classify the clients and APs.

8. 5. 1 Session Limit

In Session Limit, you can view the session limit information in a table.

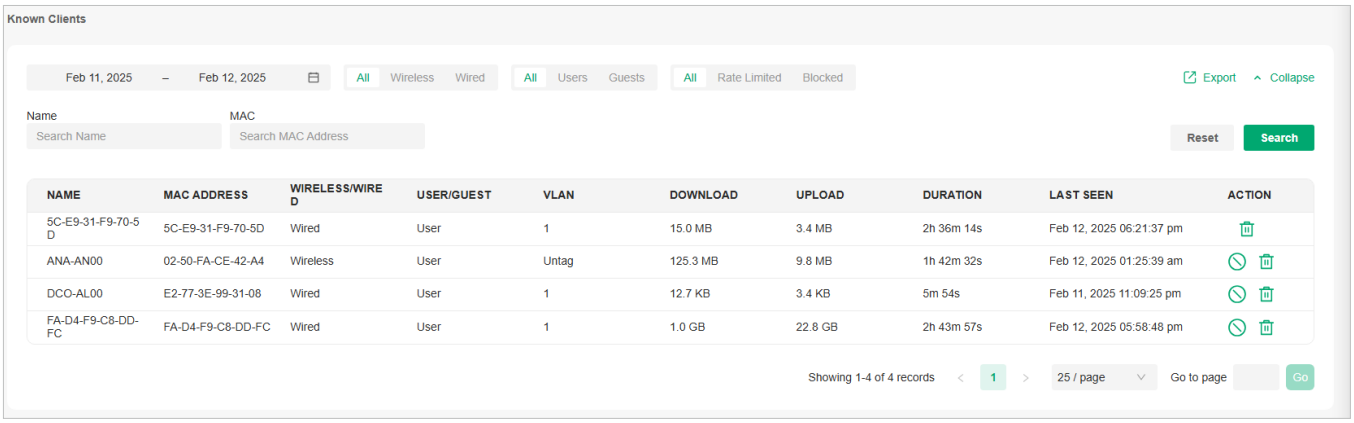


Name	Display the name of the session.
IP Address	Display the IP address of the session.
Session Count	Display the count of the session.
Session Percentage	Display the percentage of the session.
Source	Display the source of the session.
Maximum Sessions	Display the maximum number of sessions.

8. 5. 2 Known Clients

In Known Clients, a table lists all clients that connected to the network before in the site.

In the table, you can view the client's basic information, role and connection statistics, including download and upload traffics, connection duration, and the last time it connected to the network.



A search bar, a time selector and three tabs are above the table for searching and filtering.

	Enter the client name or MAC address to search the clients.
	Filter the clients based on Last Seen. Click the selector to open the calendar. Click a specific date twice in the calendar to display the records on the day. To display the records of a time range, click the start date and end date in the calendar.
  	Click the tabs to filter the clients listed in the table. The three tabs can take effect simultaneously. All/Wireless/Wired: Click All to display both wireless and wired clients. Click Wireless or Wired to display wireless or wired clients only. All/Users/Guests: Click All to display both users and guests. Click Users or Gusets to display users or guests only. Guests are users connected to the wireless guest network. To configure guest network, refer to 4. 3 Configure Wireless Networks. All/Rate Limited/Blocked: Click All to display both rate limited and blocked clients. Click Rate Limited or Blocked to display rate limited or blocked clients only. To configure Rate Limit, refer to 4. 7. 3 Rate Limit. To block the clients, click the Block icon in the table.

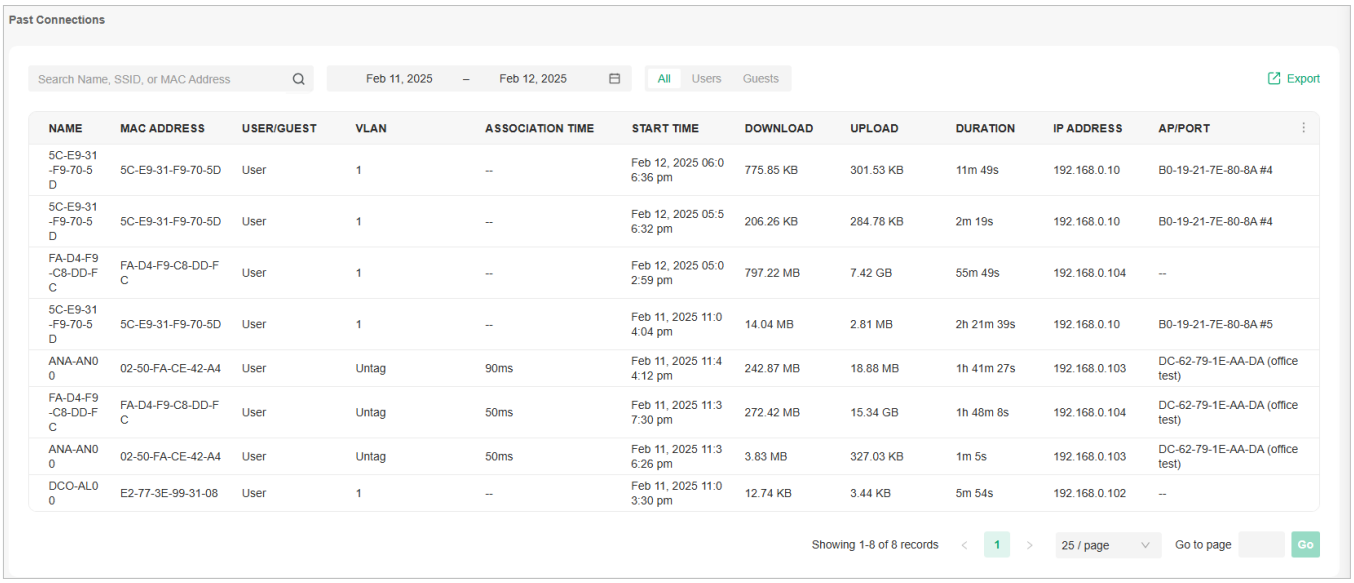
You can also take actions to block or forget the client. For detailed monitor and management, click the entry in the table to open the Properties window of the client. For more details, refer to 7. 1. 2 Using the Clients Table to Monitor and Manage the Clients.

	(For unblocked clients) Click to block the client in the site. Once blocked, the client is banned from connecting to the network in the site.
	(For blocked clients) Click to unblock the client in the site.
	Click to forget the client. Once forget, all statistics and history of the client in the site are dropped.

8. 5. 3 Past Connections

In Past Connections, a table displays information about previous client connection sessions.

In the table, you can view the client's name, MAC address, association time and duration, download and upload traffic, IP address, and the network/port it connected to.



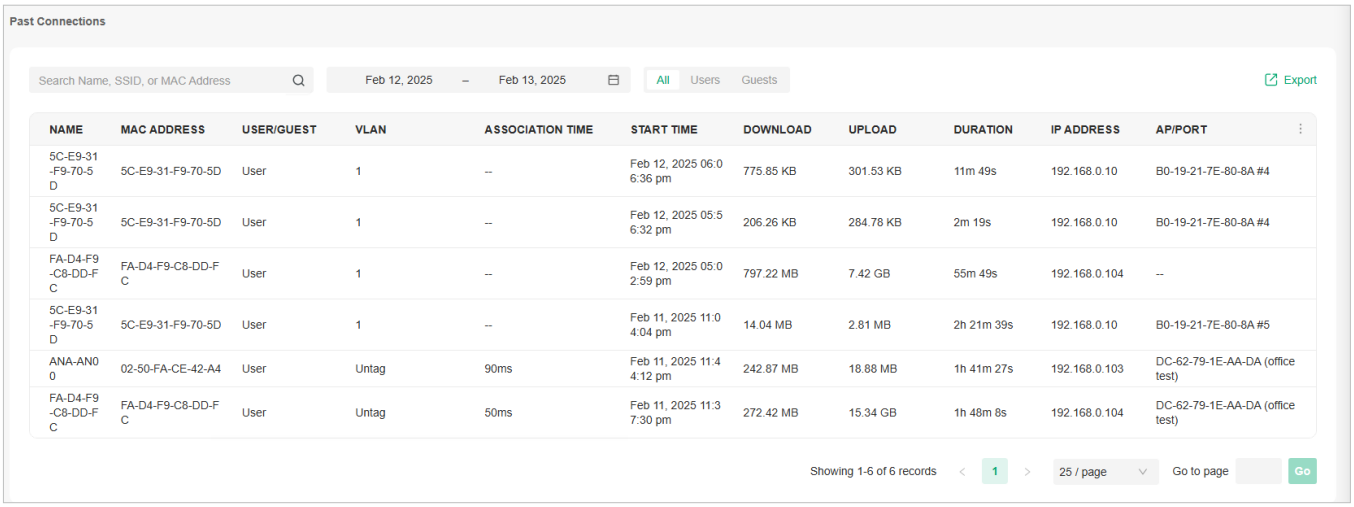
A search bar and a time selector are above the table for searching and filtering.

Search Name, SSID, or MAC Address	Enter the client name, SSID or MAC address to search the clients.
Start date – End date	Filter the clients based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display client connection sessions on the day. To display the client connection sessions during a time range, click the start date and end date in the calendar.

8. 5. 4 Past Portal Authorizations

In Past Portal Authorization, a table lists all clients that passed the portal authorization before.

In the table, you can view the client's name, MAC address, authorization credential, uplink and downlink traffics, authorization time and duration, IP address, and the network/port it connected to. For detailed monitoring and management, refer to 7. 2 Manage Client Authentication in Hotspot.



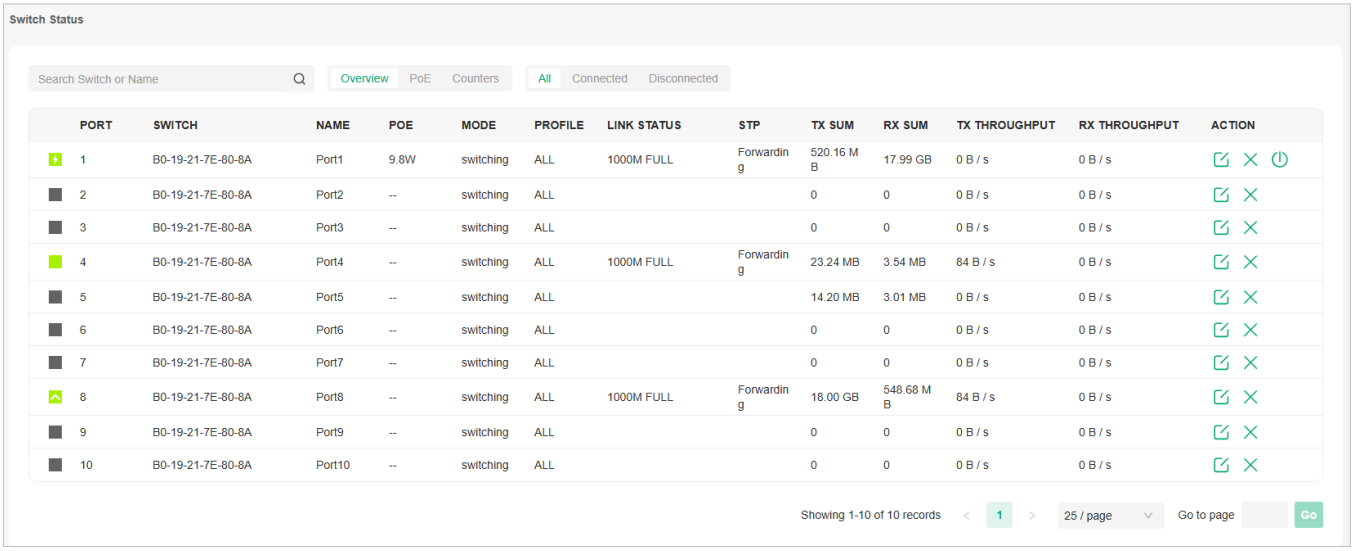
A search bar and a time selector are above the table for searching and filtering.

	Enter the client name, MAC address, Authorized By, or SSID/Network to search the clients.
	Filter the clients based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display the clients authorized on the day. To display the clients authorized during a time range, click the start date and end date in the calendar.

8. 5. 5 Switch Status

In Switch Status, a table displays information about the status of the switches managed by the controller.

In the table, you can view the ports, PoE status, mode, and traffic activity of the switches.



A search bar and two tabs are above the table for searching and filtering. You can also click the icons in the Action column for quick operation.

	Enter the switch or name to search.
	Click the tabs to filter the switch ports listed in the table. The two tabs can take effect simultaneously. Overview/PoE/Counters: Click Overview to display the general status of each port. Click PoE to display the PoE configurations and status of each port. Click Counters to display TX and RX rates for each port. All/Connected/Disconnected: Filter the ports by their link status. Click All to display information of all ports. Click Connected or Disconnected to display all connected or disconnected ports.
	Click to edit the configurations of the port.
	Click to clear all statistics of the port.
	(Only for the PoE port that is connected to a PD) Click the button and the port will stop to supply power to the connected PD momentarily in order to reboot the PD.

The listed information when you select Overview on the first tab is explained as follows.

Port	Display the port number and status of the port . 10/100 Mbps: The port is running at 10/100 Mbps. 1000 Mbps: The port is running at 1000 Mbps. 2.5 Gbps: The port is running at 2.5 Gbps. 10 Gbps: The port is running at 10 Gbps. Disabled: The port is disabled. Disconnected: The port is enabled but connects to no devices or clients. PoE: The PoE port is connected to a powered device (PD). Uplink: The port is an uplink port connected to WAN. Mirroring: The port is a mirroring port that is mirroring another switch port. STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.
Switch	Display the MAC address or the alias of the switch.
Name	Display the name of the port.

PoE	Display the PoE status of the port. --: PoE is disabled _W: Display the power output of the port in watts.
Mode	Display the operation mode of the port. Switching: The default mode. Mirroring: The network traffic of this port will receive the mirrored traffic from its mirrored port. Aggregating: The port is a part of an aggregate link
Profile	Display the switch port profile that takes effect on the port.
Link Status	Display the connection speed and duplex mode of the port.
STP	Display the Spanning Tree Protocol (STP) mode.
TX Sum	Display the amount of transmitted data.
RX Sum	Display the amount of received data.
TX Throughput	Display the transmit throughput rate.
RX Throughput	Display the receive throughput rate.

The listed information when you select PoE on the first tab is explained as follows.

Port	Display the port number and status of the port . 10/100 Mbps: The port is running at 10/100 Mbps. 1000 Mbps: The port is running at 1000 Mbps. 2.5 Gbps: The port is running at 2.5 Gbps. 10 Gbps: The port is running at 10 Gbps. Disabled: The port is disabled. Disconnected: The port is enabled but connects to no devices or clients. PoE: The PoE port is connected to a powered device (PD). Uplink: The port is an uplink port connected to WAN. Mirroring: The port is a mirroring port that is mirroring another switch port. STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.
Switch	Display the MAC address or the alias of the switch.

Name	Display the name of the port.
PoE	Display the PoE status of the port. --: PoE is disabled _W: Display the power output of the port in watts.
PD Class	Display the power requirement of the PD connected to the PoE port.
Power	Display the power output of the port in watts.
Voltage	Display the voltage output in volts.
Current	Display the current output in amperes.

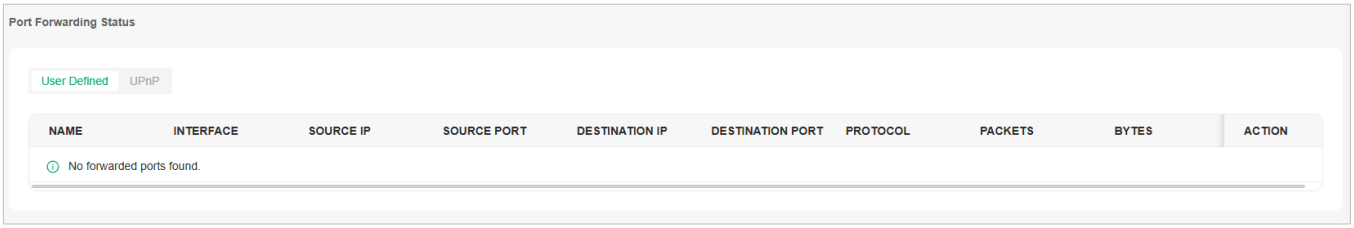
The listed information when you select Counters on the first tab is explained as follows.

Port	Display the port number and status of the port . 10/100 Mbps: The port is running at 10/100 Mbps. 1000 Mbps: The port is running at 1000 Mbps. 2.5 Gbps: The port is running at 2.5 Gbps. 10 Gbps: The port is running at 10 Gbps. Disabled: The port is disabled. Disconnected: The port is enabled but connects to no devices or clients. PoE: The PoE port is connected to a powered device (PD). Uplink: The port is an uplink port connected to WAN. Mirroring: The port is a mirroring port that is mirroring another switch port. STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.
Switch	Display the MAC address or the alias of the switch.
TX Bytes	Display the number of transmitted bytes.
TX Frames	Display the number of transmitted frames.
TX Multicast	Display the number of transmitted multicast packets.
TX Broadcast	Display the number of transmitted broadcast packets.
TX Errors	Display the number of transmitted error packets.
RX Bytes	Display the number of received bytes.

RX Frames	Display the number of received frames.
RX Multicast	Display the number of received multicast packets.
RX Broadcast	Display the number of received broasdcast packets.
RX Errors	Display the number of received error packets.

8. 5. 6 Port Forwarding Status

In Port Forwarding Status, a table displays information about the port forwarding entries used by the gateway managed by the controller.



A tab is above the table for filtering. You can also click the icons in the Action column for quick operation.

User Defined UPnP	Click the tab to filter the port forwarding entries listed in the table. User-defined/UPnP: Click User Defined to display the port forwarding entries created by the user. Click UPnP to display the UPnP port forwarding entries.
	Click to edit the configurations of the port forwarding entry.

The listed information is explained as follows.

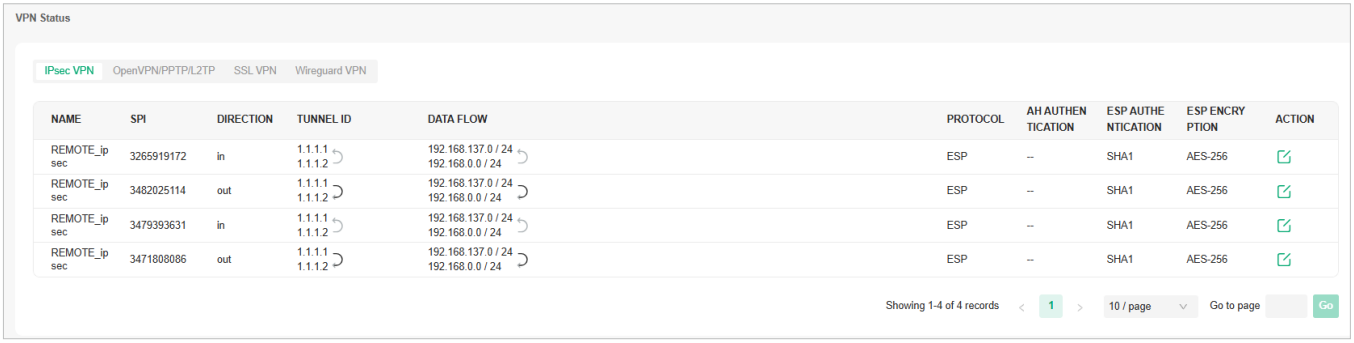
Name	Display the name of the port forwarding entry.
Interface	Display the WANs used by the port forwarding entry.
Source IP	(Only for user-defined entries) Display the source IP address. A specific IP address/Mask: The specified source IP address. 0.0.0.0/0: All IP addresses are set as the source IP address.
Source Port	The traffic through the source port, also known as internal port, will be forwarded to the LAN.
Destination IP	Display the destination IP address, and it will receive the forwarded port traffic.
Destination Port	Display the destination port, also known as internal port, that will receive the forwarded traffic.
Protocol	Display the protocol that will be forwarded.

Packets	Display the number of transferred packets.
Bytes	Display the number of transferred bytes.
Lease Duration	(Only for UPnP port forwarding) Display the uptime of the port forwarding entry.

8. 5. 7 VPN Status

In VPN Status, a table displays the existing VPN tunnels and corresponding information. Click the tab to filter the routing information listed in the table.

- **IPsec VPN**



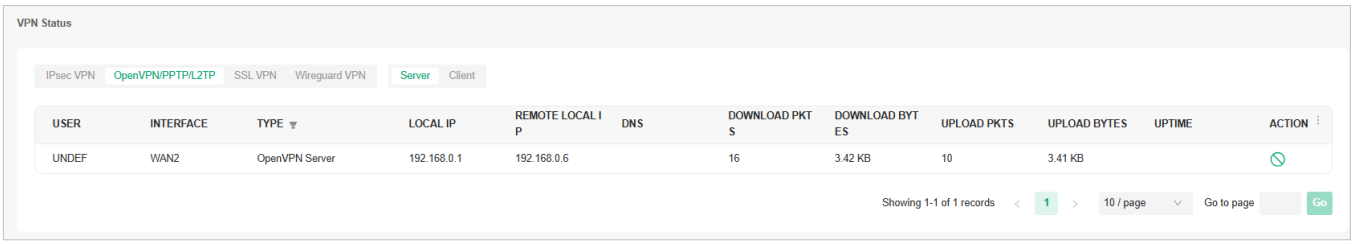
The listed information of IPsec VPN table is explained as follows.

Name	Display the name of the IPsec VPN entry.
SPI	Display the Security Parameter Index of VPN.
Direction	Display the direction of the VPN process.
Tunnel ID	Display the local and remote IP address/name. The arrow indicates the traffic direction.
Data Flow	Display local and remote subnet. The arrow indicates the direction.
Protocol	Display the authentication and encryption protocol of the entry.
AH Authentication	Display checksum algorithms of the entry.
ESP Authentication	Display the algorithms for ESP authentication.
ESP Encryption	Display the algorithms for ESP encryption.

- **OpenVPN/PPTP/L2TP**

When you select OpenVPN/PPTP/L2TP, you can further choose Server or Client.

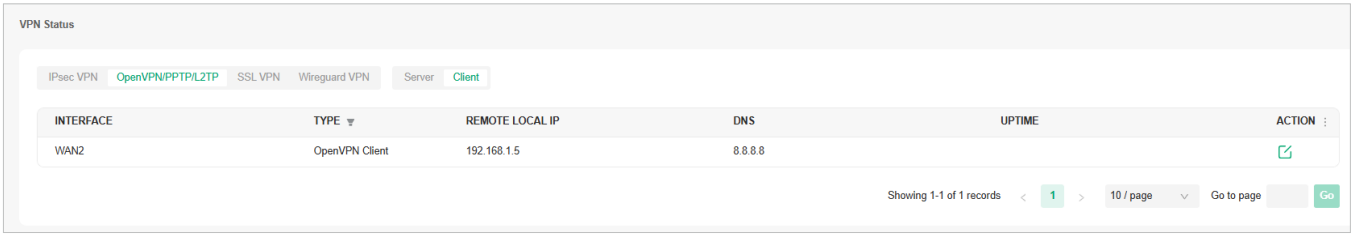
The listed information of OpenVPN/PPTP/L2TP (Server) table is explained as follows (some information listed below is hidden by default). You can further filter the entries based on their type.



User	Display the username of the remote user.
Interface	Display the interface that the traffic goes through.
Type	Display the connection type.
Local IP	Display the local IP address of the VPN tunnel.
Remote Local IP	Display the IP address of the remote user of the VPN tunnel.
DNS	Display the DNS address of the VPN tunnel.
Download Pkts	Display the amount of data downloaded as packets.
Download Bytes	Display the amount of data downloaded as bytes.
Upload Pkts	Display the amount of data uploaded as bytes.
Upload Bytes	Display the amount of data uploaded as bytes.
Uptime	Display the time duration that the VPN tunnel has been active.

You can click the terminate icon in the Action column to terminate the VPN tunnel.

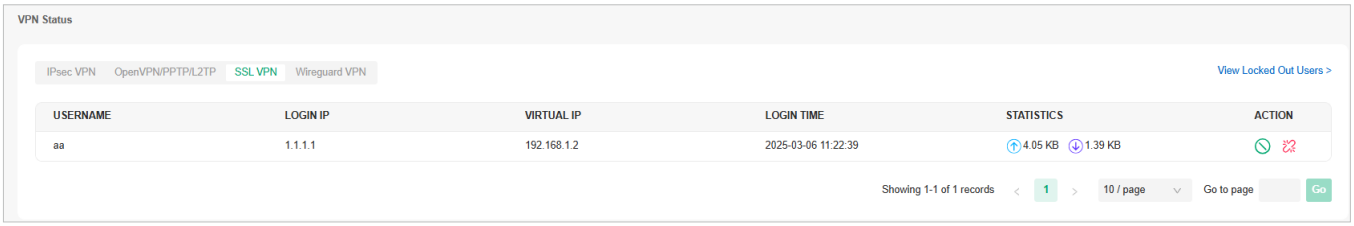
The listed information of OpenVPN/PPTP/L2TP (Client) table is explained as follows (some information listed below is hidden by default). You can further filter the entries based on their type.



Interface	Display the interface that the traffic goes through.
Tunnel	Display the name of the VPN client.
Type	Display the connection type.

Remote Local IP	Display the IP address of the remote user of the VPN tunnel.
DNS	Display the DNS address of the VPN tunnel.
Download Pkts	Display the amount of data downloaded as packets.
Download Bytes	Display the amount of data downloaded as bytes.
Upload Pkts	Display the amount of data uploaded as bytes.
Upload Bytes	Display the amount of data uploaded as bytes.
Uptime	Display the time duration that the VPN tunnel has been active.

■ SSL VPN



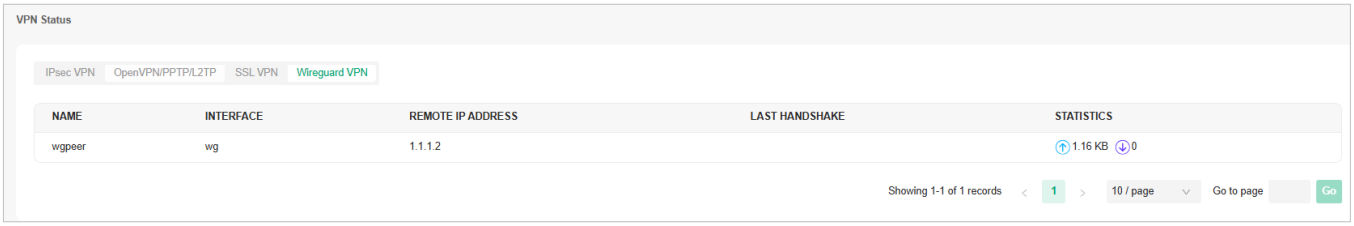
The listed information of SSL VPN table is explained as follows.

Username	Display the username of the remote user.
Login IP	Display the login IP address of the remote user.
Virtual IP	Display the virtual IP address of the remote user.
Login Time	Display the login time of the remote user.
Statistics	Display the upload and download traffic of the remote user.

You can click the lock icon in the Action column to lock out the user. You can click View Locked Out Users to manage the locked out users.

You can click the disconnect icon to disconnect the user.

■ Wireguard VPN

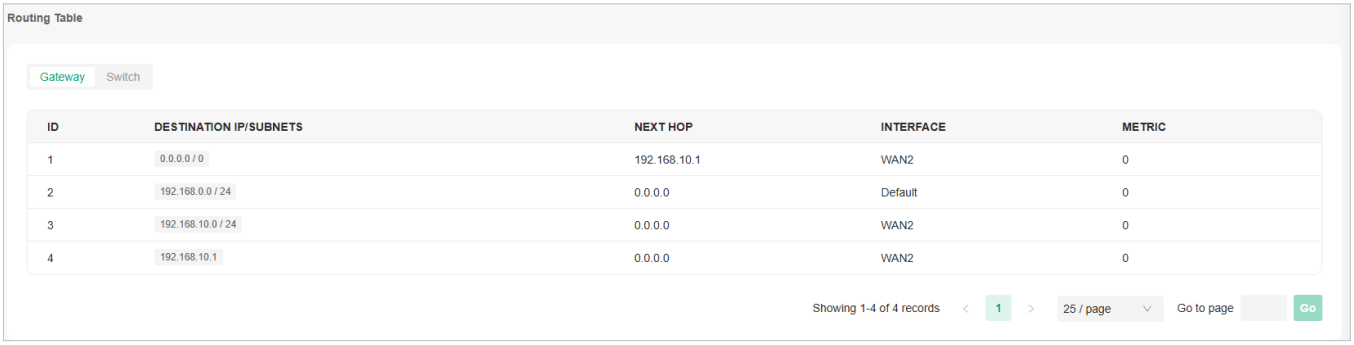


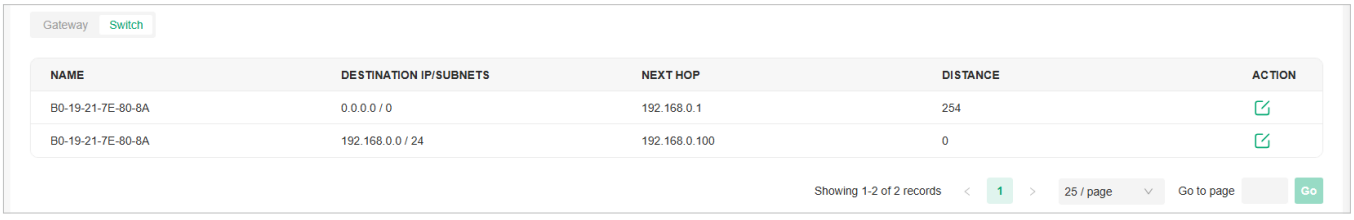
The listed information of Wireguard VPN table is explained as follows.

Name	Display the name of the WireGuard interface.
Interface	Display the interface that the traffic goes through.
Remote IP Address	Display the remote IP address of the WireGuard interface.
Last Handshake	Display the last handshake of the WireGuard interface.
Statistics	Display the upload and download traffic of the WireGuard interface.

8. 5. 8 Routing Table

Routing Table displays information of routing entries that have taken effect.





A tab is above the table for filtering. You can also click the icons in the Action column for quick operation.

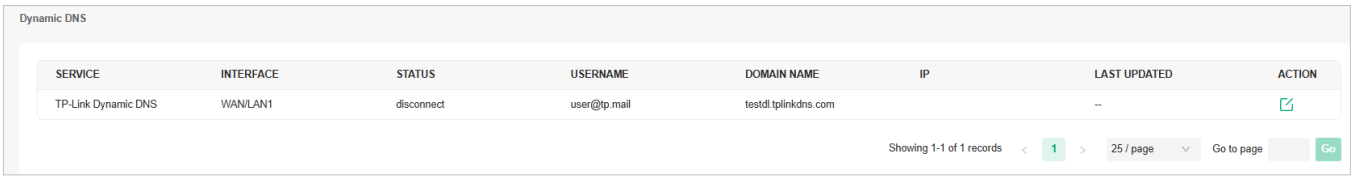
Gateway Switch	Click the tab to filter the routing information listed in the table. Gateway/Switch: Click to display the routing information of the gateway or the switch.
	(Only for switch) Click to configure the static routes.

The listed information is explained as follows.

Destination IP/Subnets	Display the destination IP addresses of the routing entry..
Next Hop	Display the IP address of the next hop.
Interface	(Only for Gateway) Display the interface that the traffic of the entry goes through.
Metric	(Only for Gateway) Display the number of hops before reaching the destination. Generally, if there are a few routing entries with the same destination, the routing with the lowest metric will be used.
Distance	(Only for Switch) Display the administrative distance of the routing entry. It is used to decide the priority among routes to the same destination. Among routes to the same destination, the route with the lowest distance value will be used.

8. 5. 9 Dynamic DNS

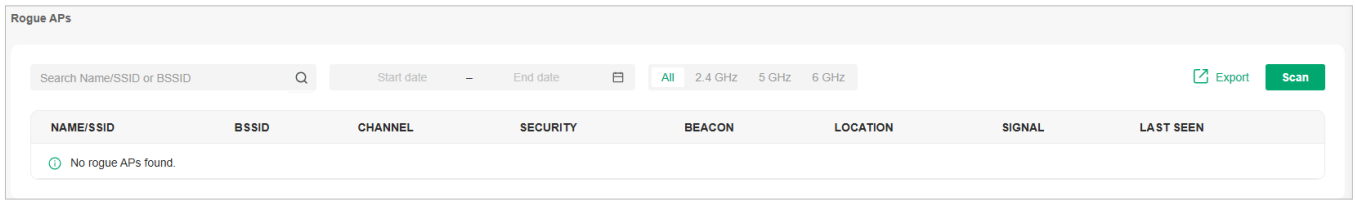
In Dynamic DNS, a table displays information about the uses of the dynamic DNS services. You can click the Edit icon in the Action column to edit the entry.



Service	Display the name of the DDNS service.
Interface	Display the WANs used by the DDNS entry.
Status	Display the status of the latest DDNS update.
Username	Display the username of the DDNS account.
Domain Name	Display domain name registered with the DDNS service.
IP	Display the IP address of the domain name.
Last Updated	Display the time when the IP address of the domain name was last updated.

8. 5. 10 Rogue APs

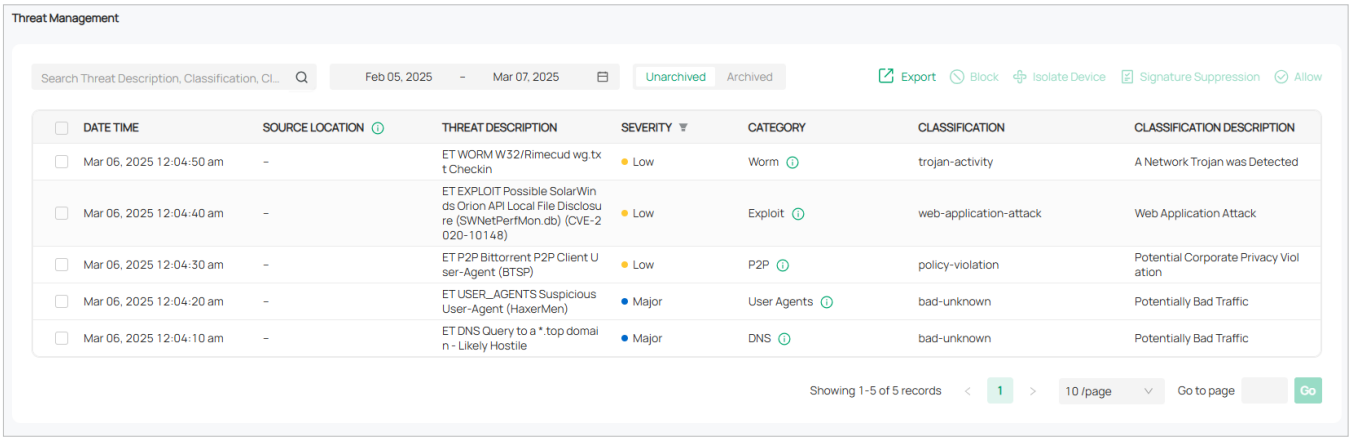
A rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. In Rogue APs, you can scan rogue APs and view the rogue APs scanned before.



	Enter the client name/SSID or BSSID to search the clients.
	Filter the rogue APs based on Last Seen. Click the selector to open the calendar. Click a specific date twice in the calendar to display the rogue APs scanned on the day. To display the scanned AP during a time range, click the start date and end date in the calendar.
	Click the tab to filter the rogue APs listed in the table based on the frequency band.
	Click to scan rogue APs. It may take several minutes, and the wireless service may be influenced during scanning.
BSSID	A string with a similar form as MAC address to recognize access points.
Channel	Displays the operation channel and standard of the rogue AP.
Security	Displays the security strategy of the rogue AP.
Beacon	Displays the beacon interval of the rogue AP. Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients, and the interval means how often the AP send a beacon to clients.
Location	Displays the managed AP nearest to the rogue AP. You can click the nearest AP to open its Properties window.
Signal	Displays the signal strength in percentage and dBm).
Last Seen	Display the last time that the rogue AP was scanned by the controller.

8. 5. 11 Threat Management

IDS/IPS can detect buffer overflows, Trojan horses, worms, SQL injections and other attacks to protect the network security of users. When the device discovers a threat, the corresponding threat log will be displayed.



Search Threat Description, Classification, Cl...	Enter the threat description, classisfication or classification description to search the clients.
Start date - End date	Filter the threat entries based on Last Seen. Click the selector to open the calendar. Click a specific date twice in the calendar to display the threat detected on the day. To display the detected threats during a time range, click the start date and end date in the calendar.
Unarchived Archived	Click the tab to filter the unarchived and archived entries.
Export	Click to export the entries in .CSV or .XLSX format.
Block	Drop traffic to/from the external IP address and the specific internal IP address. If you block an entry, it will be added to the Block List at Settings > Network Security > IDS/IPS.
Isolate Device	Drop traffic to/from the external IP address and any internal IP address.
Signature Suppression	Mute the alerting on certain signatures. This will also disable blocking on traffic matching the designated suppression rule. If you suppress the signature of an entry, it will be added to the Signature Suppression list at Settings > Network Security > IDS/IPS.
Allow	Trust the IP address so that the traffic, depending on the direction selected, will not get blocked to or from the identified IP address. If you allow an entry, it will be added to the Allow List at Settings > Network Security > IDS/IPS.
Date Time	Displays the time of the threat.
Source Location	Displays the source location of the threat.

Threat Description	Displays the description of the threat.
Severity	Displays the severity of the threat.
Category	Displays the category of the threat.
Classification	Displays the classification of the threat.
Classification Description	Displays the description of the classification.

8. 6 View and Manage Logs

The controller uses logs to record the activities of the system, devices, users and administrators, which provides powerful supports to monitor operations and diagnose anomalies. In the Logs page, you can conveniently monitor the logs in 8. 6. 1 Alerts and 8. 6. 2 Events, and configure their notification levels in 8. 6. 3 Notifications.

All logs can be classified from the following four aspects.

- **Occurred Hierarchies**

  Two categories in occurred hierarchies are Controller and Site, which indicate the log activities happened, respectively, at the controller level and in the certain site. Only Main Administrators can view the logs happened at the controller level.

- **Notifications**

  Two categories in notifications are Event and Alert, and you can classify the logs into them by yourself.

- **Severities**

  Three levels in severities are Error, Warning, and Info, whose influences are ranked from high to low.

- **Contents**

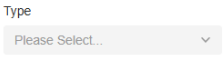
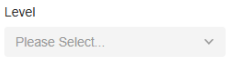
  Four types in contents are Operation, System, Device, and Client, which indicate the log contents relating to.

8. 6. 1 Alerts

Alerts are the logs that need to be noticed and archived specially. You can configure the logs as Alerts in Notifications, and all the logs configured as Alerts are listed under the Alerts tab for you to search, filter, and archive.

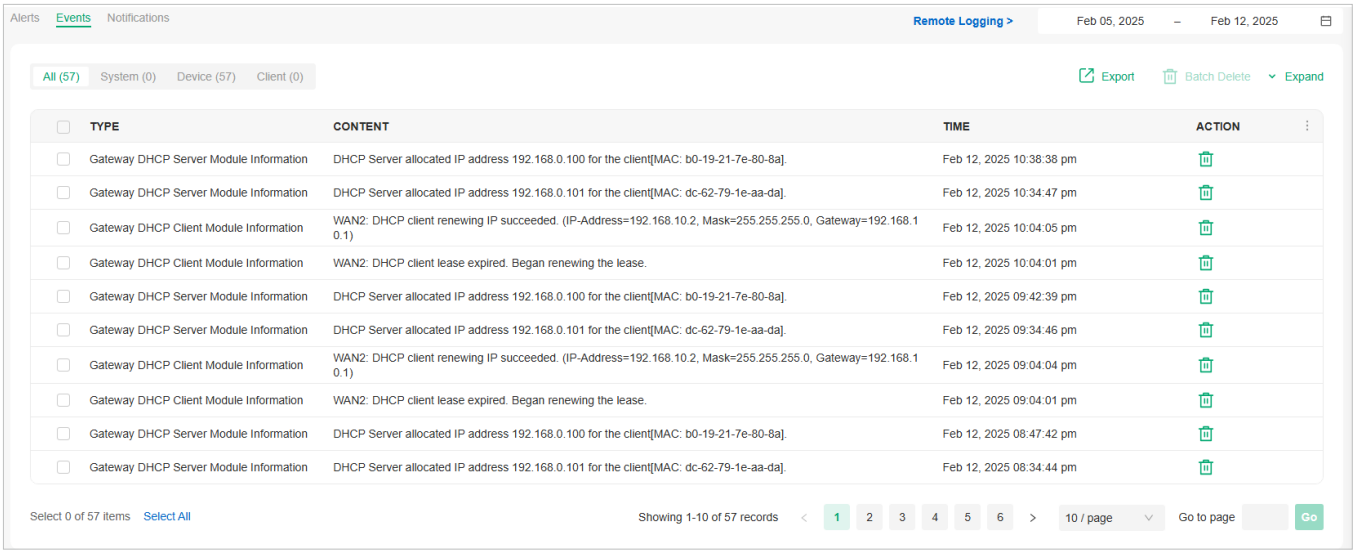


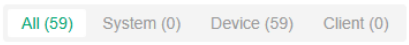
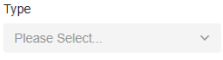
 	Click to change the view mode for a better overview. : Displays the logs in a table. : Displays the logs in graphs.
	Click the tab to filter the unresolved and resolved logs. You can click the Resolved icon or Batch Resolved to resolve a single log and all, respectively.

	Click All to display all types of logs. Click System or Deviceto display the corresponding type of logs only.
	Click to export the logs in .CSV or .XLSX format.
	Click to resolve the logs in batches.
	Click to delete the logs in batches.
	Expand: Click to display more filters. Collapse: Click to display less filters.
	Select the content type to filter the logs.
	Select the severity levels to filter the logs.
	Enter the key words to search the logs.
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.
Time	Displays when the activity happened.
	Click to resolve the log entry.
	Click to delete the log entry. Once deleted the logs cannot be recovered.

8. 6. 2 Events

Events are the logs that can be viewed but have no notifications. You can configure the logs as Events in Notifications, and all the logs configured as Events are listed under the Events tab for you to search and filter.

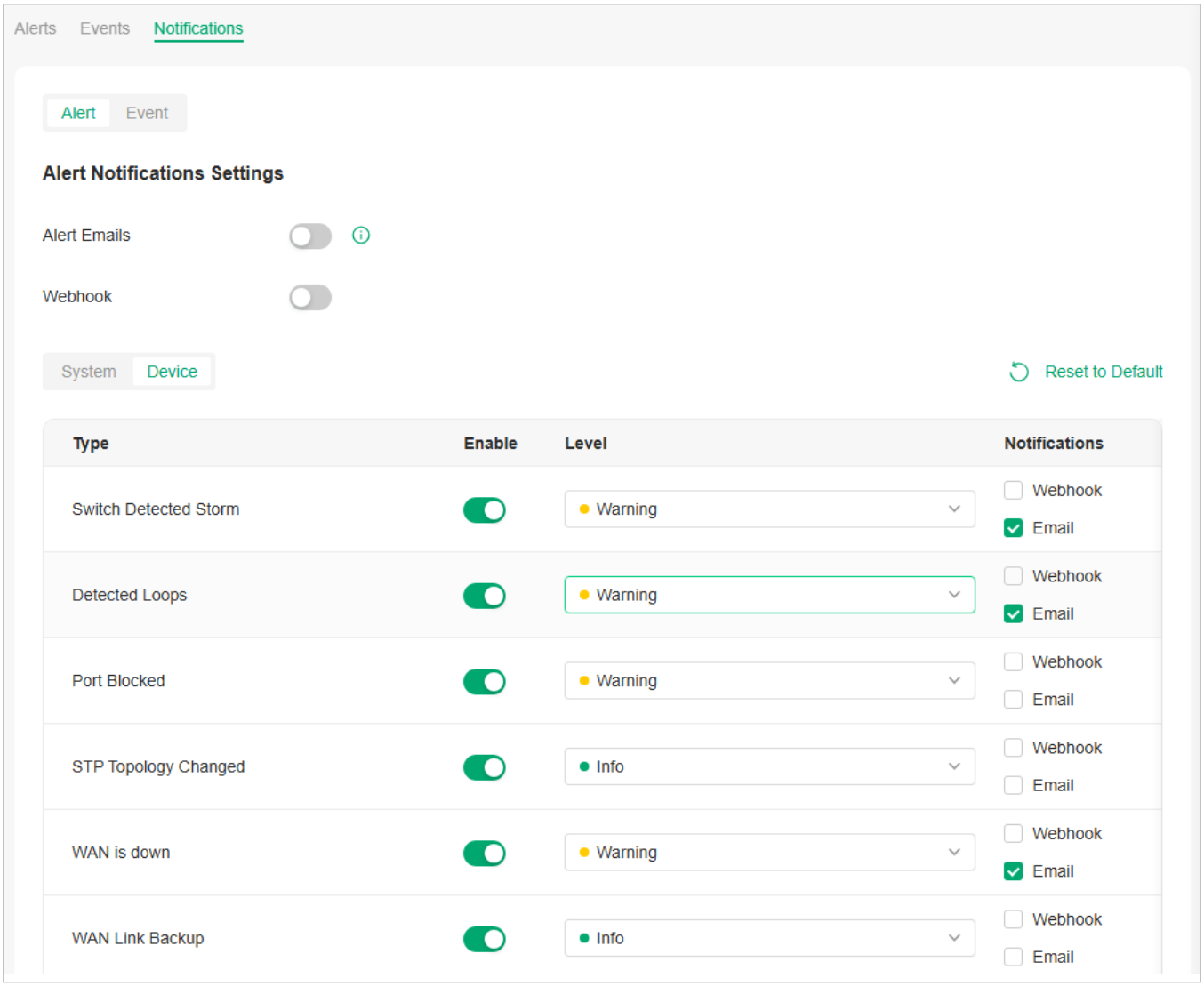


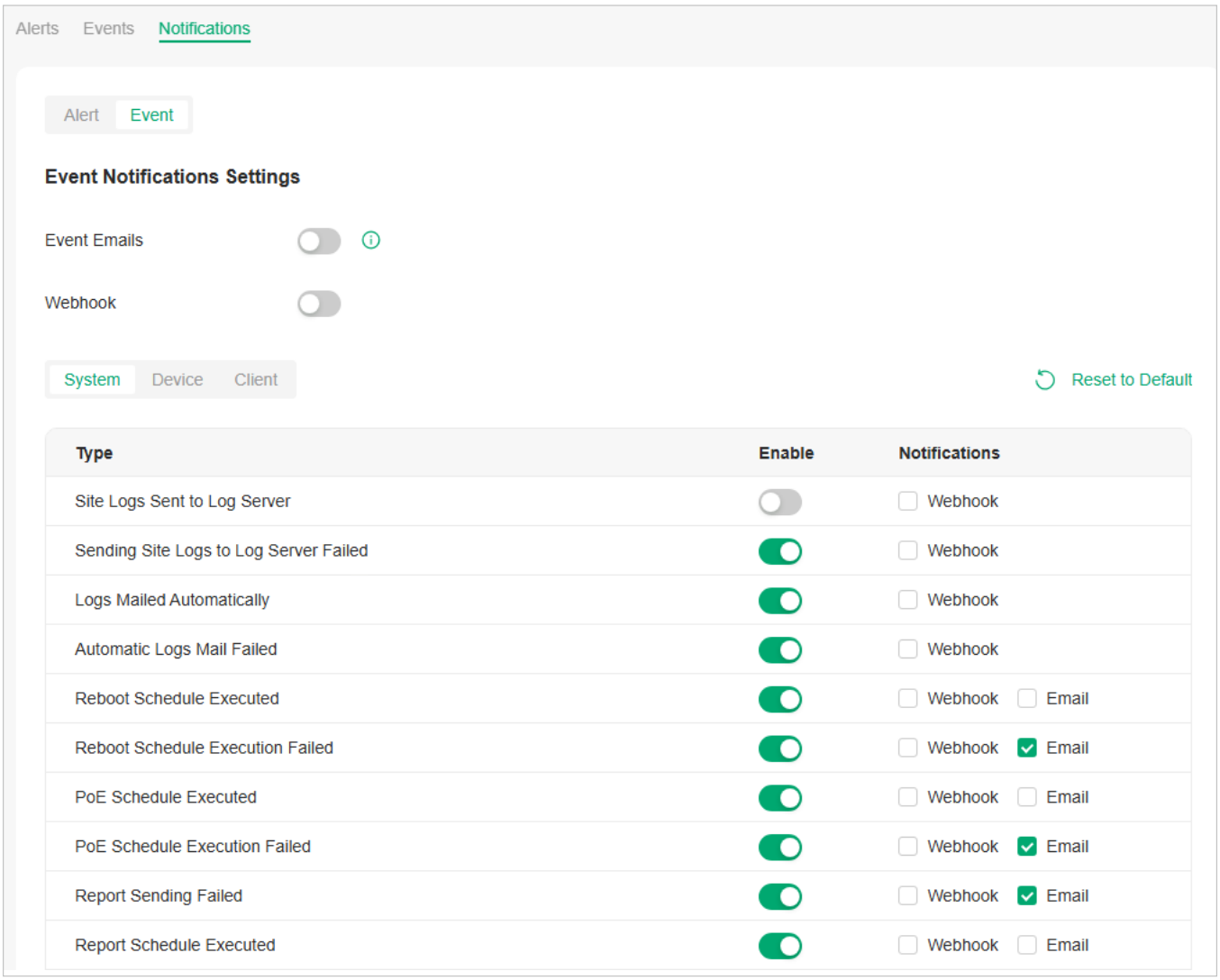
	Filter the logs based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display the logs on the day. To display the logs during a time range, click the start date and end date in the calendar.
	All/System/Device/Client: Click All to display all types of logs. Click System or Device or Client to display the corresponding type of logs only.
	Click to export the logs in .CSV or .XLSX format.
	Click to delete the logs in batches.
 	Expand: Click to display more filters. Collapse: Click to display less filters.
	Select the content type to filter the logs.
	Enter the key words to search the logs.
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.
Time	Displays when the activity happened.

	Click to delete the corresponding event logs.

8. 6. 3 Notifications

In Notifications, you can find all kinds of activity logs classified by the content and specify their notification categories as Event and Alert for the current site. Also, you can enable Email for the logs. With proper configurations, the controller will send emails to the administrators when it records the logs.





To specify the logs as Alert/Event, click the corresponding checkboxes of logs and click Apply. The following icons and tab are provided as auxiliaries.

Reset to Default	Click to reset all notification configurations in the current site to the default.
Alert Event	Click the tabs to select the activity logs, and then the enabled logs will be displayed under the Events/Alerts tab.
System Device System Device Client	Click the tabs to display the configurations of corresponding log types.
Email	Enable the checkboxes to specify the activity logs as alert/event logs. With proper settings in Site and Admin, the controller can send emails to notify the administrators and viewers of the site's logs once generated.
Webhook	Enable the checkboxes to specify the activity logs as alert logs. With proper settings, the logs will be sent to the corresponding log server via Webhook.

The Email checkboxes are used to enable Alert Emails for the logs. To make sure the administrators and viewers can receive alert emails of the site, follow the following steps:

1) Enable Mail Server

2) Enable Alert Emails in Site

3) Enable Alert Emails in Admin

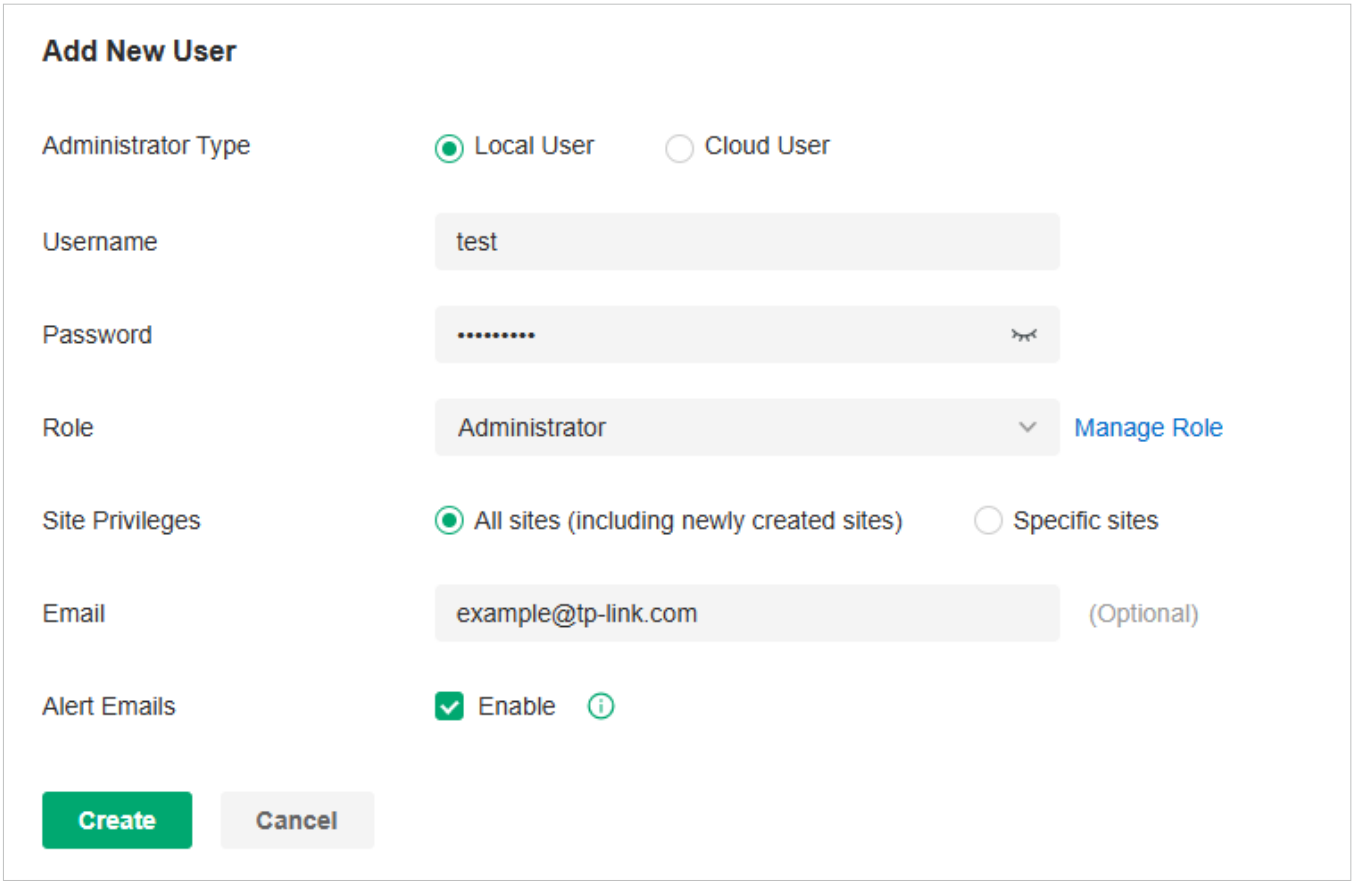
4) Enable Alert Emails in Logs

Step 1: Enable Mail Server

Launch the controller and access the Global View. Go to Settings > Server Settings to enable Mail Server. For detailed configuration, refer to 5.5.1 Mail Server.

Step 2: Enable Alert Emails in Accounts

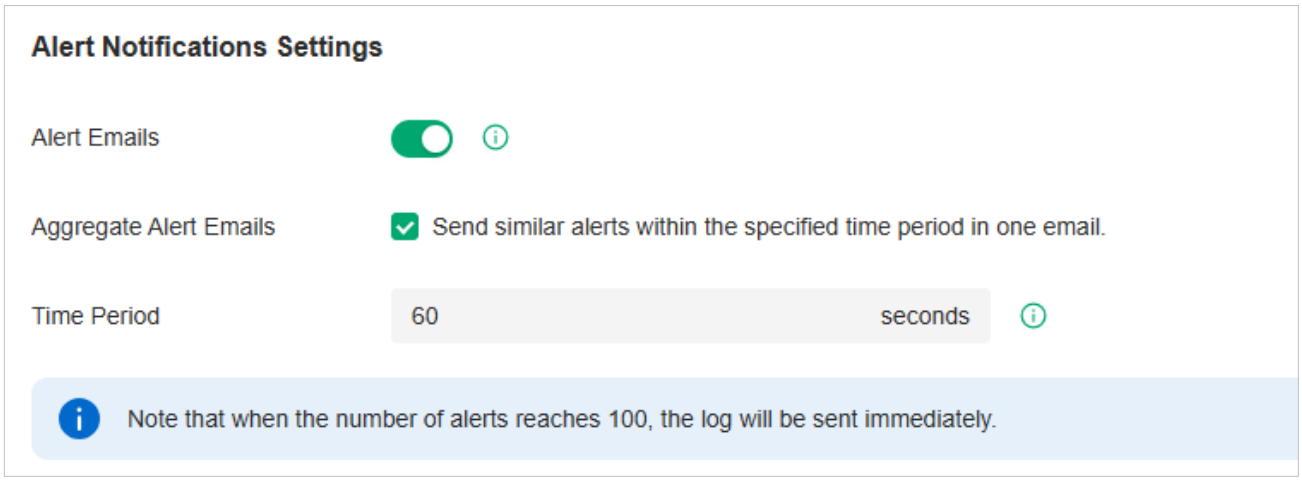
In Global View, go to Accounts > User and configure Alert Emails for the administrators and viewers to receive the emails. Click Add New Admin Account to create an account or click the Edit icon to edit an account. Enter the email address in Email and enable Alert Emails. Save the settings.



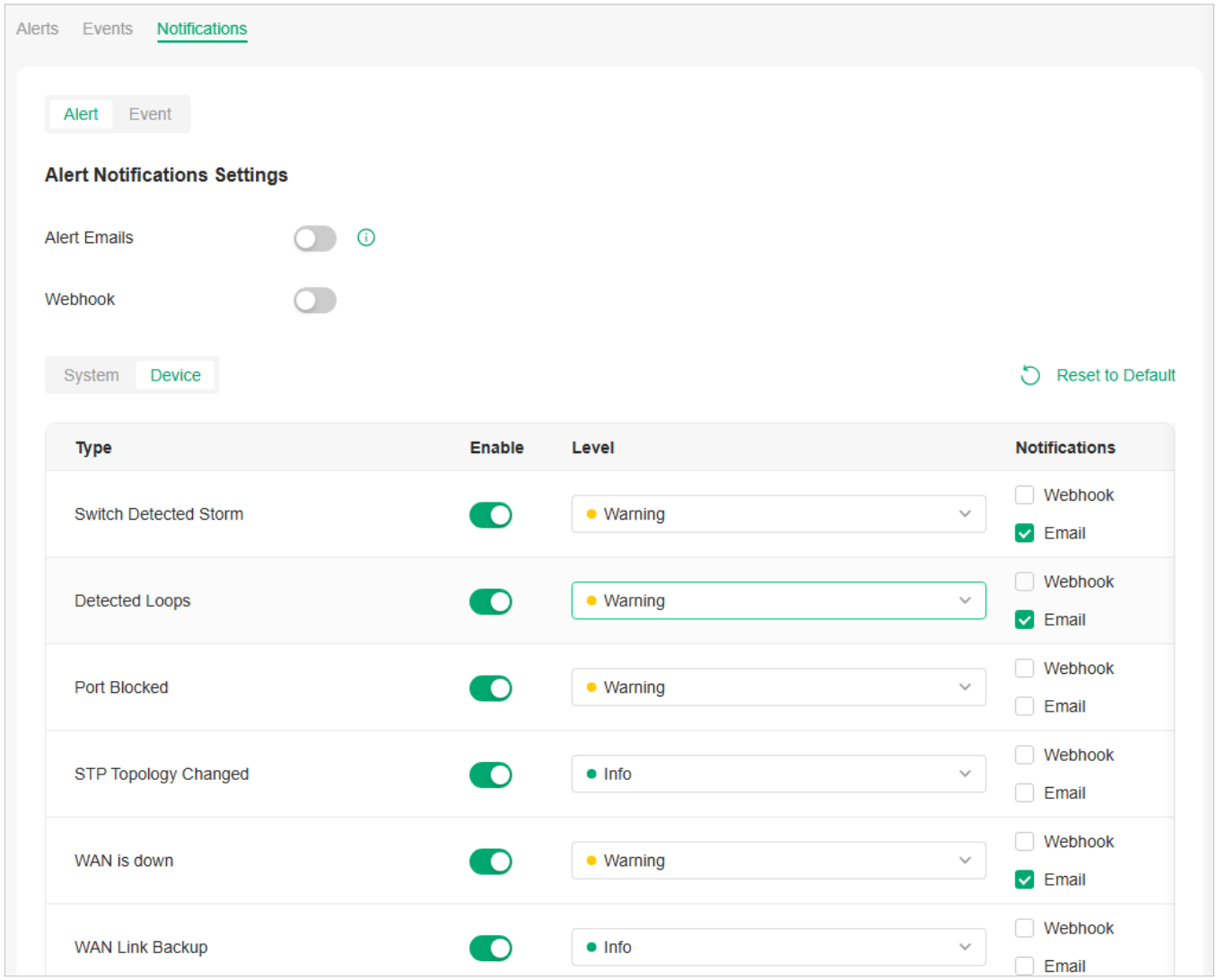
Step 3: Enable Alert Emails in Site

1. Access a site.

2. Go to Logs > Notifications. Enable Alert Emails.



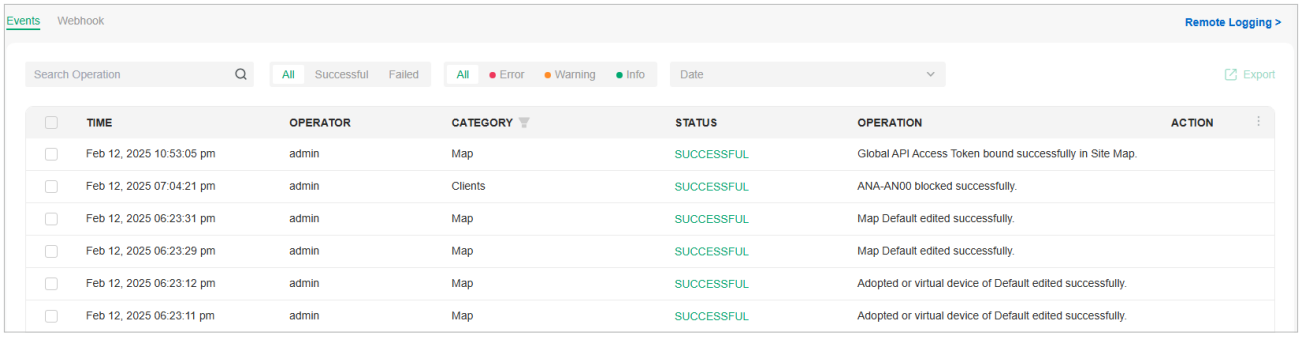
3. (Optional) Enable Aggregate Alert Emails and specify the time period. Similar alerts within the specified time period will be collected and sent to administrators and viewers in one email.
4. Click a tab of content types and enable Email for the activity logs that the controller emails administrators. Click Save.



8. 7 Audit Logs

Audit log records information about which accounts have accessed the system or site, and what operations they have performed during a given period of time.

1. Launch your controller.
2. In the Global View or Site View, go to the Audit Logs page.
3. On the Events page, check and manage the audit logs.



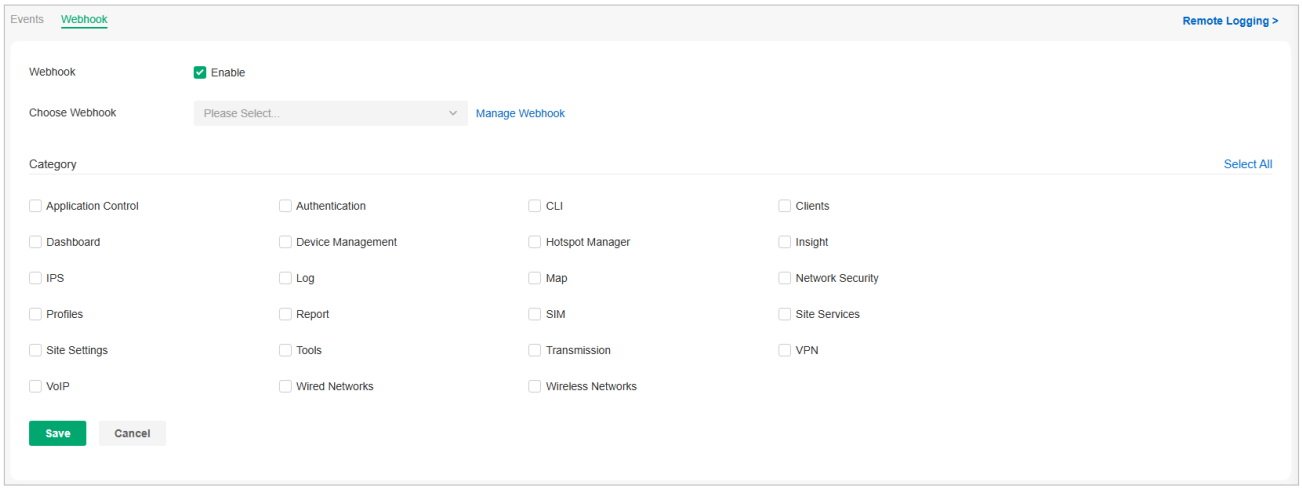
- **If you want to export audit logs:**

  Check the boxes to select entries, click Export on the upper right corner, and specify the file type to download.

- **If you want to save audit logs to your own server:**

  Click Remote Logging on the upper right corner, and follow the instructions to go to Settings > Site > Services > Remote Logging to configure the Syslog server.

4. On the Notifications page, enable Webhook and choose which modules will be sent to the corresponding log server via Webhook.



8. 8 Monitor the Network with Tools

The controller provides many tools for you to analyze your network:

- **Network Check**

  Test the device connectivity via ping, traceroute, or DNSLookup.

- **Packet Capture**

  Capture packets for network troubleshooting.

- **Terminal**

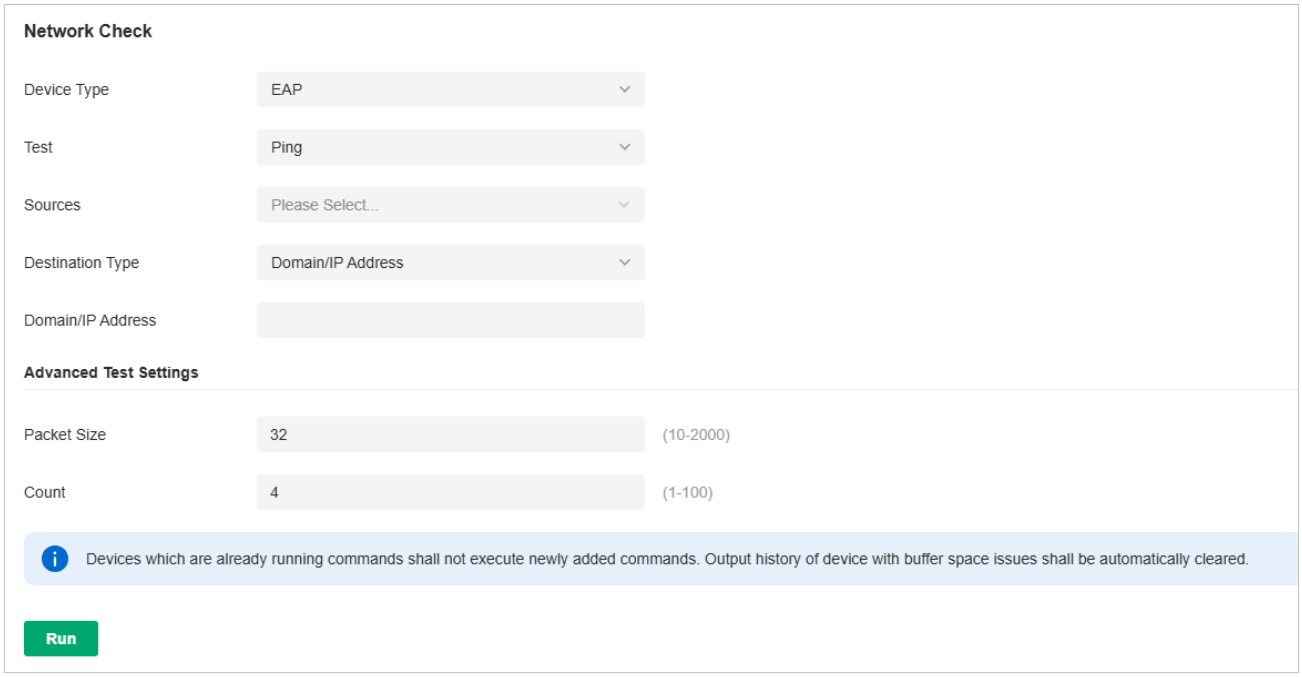
  Open Terminal to execute CLI or Shell commands.

Note:

Firmware updates are required for earlier devices to support these tools.

8. 8. 1 Network Check

1. Launch the controller and access a site.
2. Go to Network Tools > Network Check.
3. Configure the test parameters.



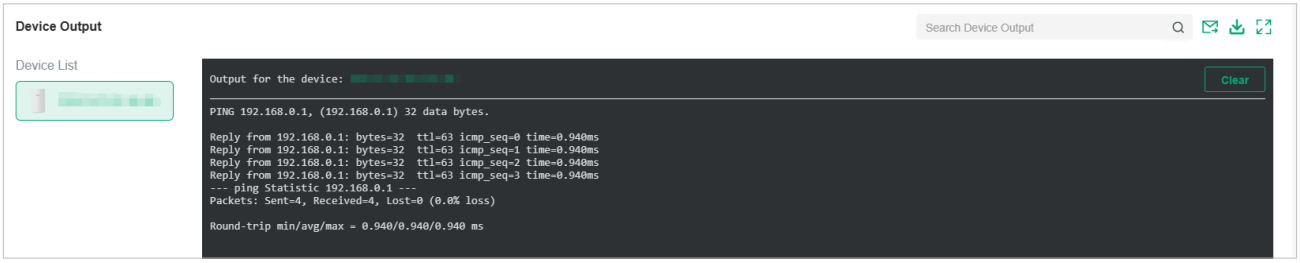
Device Type	Select the device type to perform a test.

Test	Choose a tool to test the device connectivity. Ping: Tests the connectivity between the specified sources and destination, and measures the round-trip time. Traceroute: Displays the route (path) the specified sources have passed to reach the specified destination, and measures transit delays of packets across an Internet Protocol network. DNSLookup: Helps find DNS records of a domain name. ARP Table: Helps check the ARP table of the device.
Sources	Select one or multiple devices to perform a test.
Destination Type	Select the destination type and specify the destination to test. The options vary with the test type. For the Ping test, you can specify the Domain/IP Address or Client. Client is available only when an AP device performs the ping test. For the Traceroute test, you can specify the Domain/IP Address. For the DNSLookup test, you can specify the Domain.
Advanced Test Settings	(Only for the Ping test) Packet Size: Specify the size of ping packets. Count: Specify the number of ping packets.

Note:

- Devices which are already running commands shall not execute newly added commands.
- Output history of device with buffer space issues shall be automatically cleared.

4. Click Run to perform the test. You can view the test result in the Device Output section.

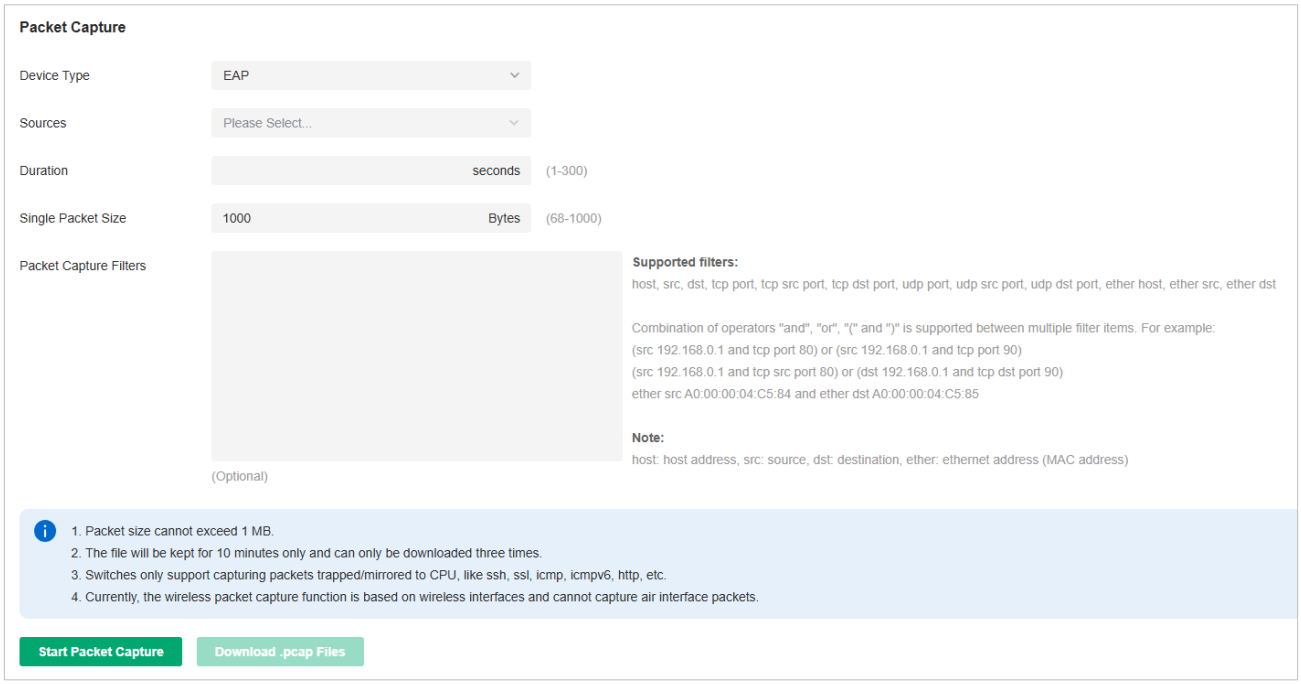


You can click the Email/Download/Zoom icons above the test result field to email the test logs to a mailbox, download the test logs locally, or zoom in/out the display area.

8. 8. 2 Packet Capture

1. Launch the controller and access a site.
2. Go to Network Tools > Packet Capture.

3. Configure the parameters for packet capture.



Device Type	Select the device type to capture packets.
Sources	Select one or multiple devices to capture packets.
Duration	Specify the duration for packet capture.
Single Packet Size	Specify the size of a single captured packet. It cannot exceed 1 MB.
Packet Capture Filters	(Optional) Enter the filters to capture packets. Supported filters include: host, src, dst, tcp port, tcp src port, tcp dst port, udp port, udp src port, udp dst port, ether host, ether src, ether dst Combination of operators “and”, “or”, “(“ and “)” is supported between multiple filter items. For example: (src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90) (src 192.168.0.1 and tcp src port 80) or (dst 192.168.0.1 and tcp dst port 90) ether src A0:00:00:04:C5:84 and ether dst A0:00:00:04:C5:85 Note: host: host address, src: source, dst: destination, ether: ethernet address (MAC address)

4. Click Start Packet Capture to capture packets. After packets are captured, you can click Download .pcap Files to download them.

Note:

The file will be kept for 10 minutes only and can only be downloaded three times.

8. 8. 3 Terminal

1. Launch the controller and access a site.

1. Go to Network Tools > Terminal.
2. Configure the parameters.



Device Type	Select the device type to run CLI or Shell commands.
Sources	Select one or multiple devices to test.

3. Click Open Terminal. Now you can run CLI or Shell commands.



You can click the Email/Download/Zoom icons above the test result field to email the test logs to a mailbox, download the test logs locally, or zoom in/out the display area.

Chapter 9

Manage Accounts of the SDN Controller

This chapter gives an introduction to different user levels of controller accounts and guides you on how to create and manage them. The chapter includes the following sections:

- 9. 1 Introduction to User Accounts
- 9. 2 Create and Manage Roles
- 9. 3 Create and Manage Local User Accounts
- 9. 4 Create and Manage Cloud User Accounts
- 9. 5 Manage User Accounts Across Controllers

9. 1 Introduction to User Accounts

The SDN Controller offers multiple levels of access available for users: **Owner**, **Super Administrator**, **Administrator**, and **Viewer**. You can also create new account roles and customize their permissions to access different features.

Since the controller can be accessed both locally and via cloud access, users can be further grouped into local users and cloud users.

Multi-level administrative account presents a hierarchy of permissions for different levels of access to the controller as required. This approach ensures security and gives convenience for management.

Moreover, in the user accounts list of the Owner/Super Administrator, all accounts it created will be displayed. The accounts created by each administrator will be hidden by default, making the interface more systematic and to the point.

- **Owner**

The Owner has access to all features.

The account who first launches the controller will be the Owner (used to be recognized as Main Administrator in earlier controller versions). It cannot be changed and deleted.

- **Super Administrator**

The Super Administrator can manage all the other roles (except Owner) and the privileges of most features.

- **Administrator**

Administrators have no permission to some modules, mainly including cloud access, migration, auto-backup and global view logs. They have read-only permission to some modules, such as global view license management and custom account roles.

Administrators can be created and deleted by the Owner/Super Administrator and Administrators.

- **Viewer**

Viewers can view the status and settings of the network, and change the settings in Hotspot Manager.

The entrance to Account page is hidden for viewers, and they can be created or deleted by the administrators.

- **Custom roles**

Custom roles can be configured to access different features.

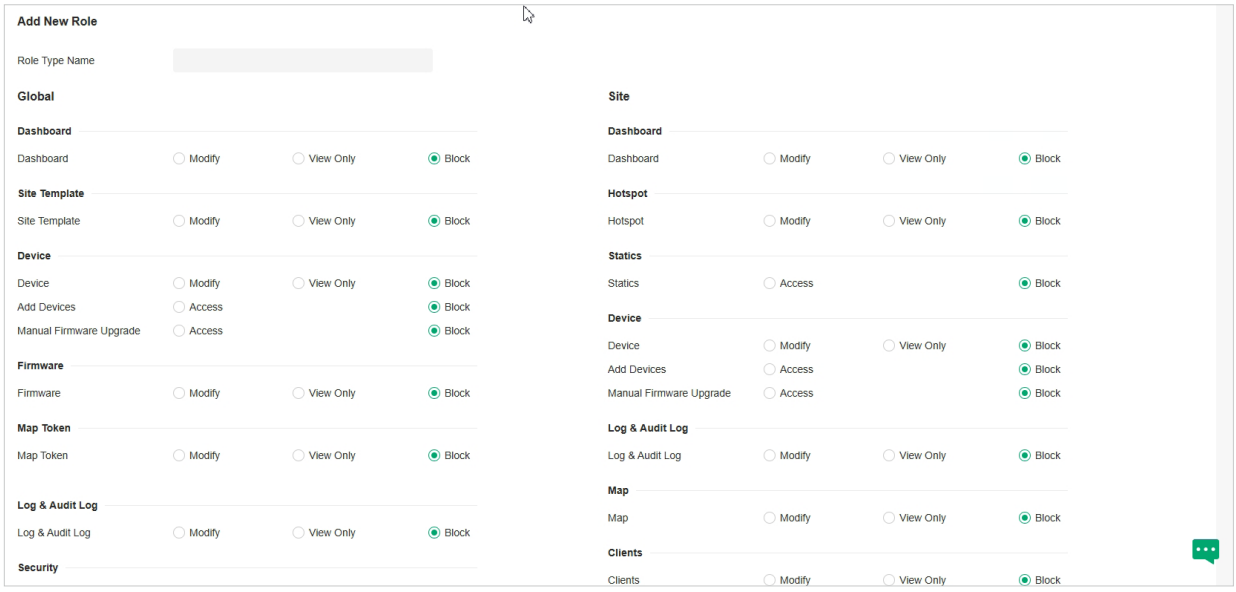
They can be created or deleted only by the Owner/Super Administrator.

Note:

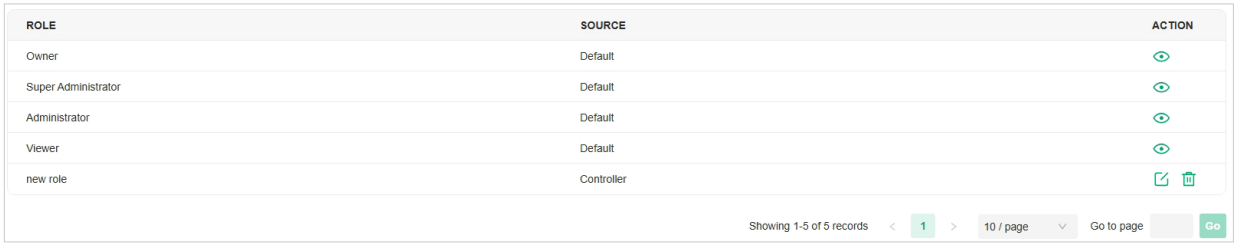
Please upgrade Omada APP to version 4.6 or later, otherwise you may not be able to log in with the accounts bound with customized roles.

9. 2 Create and Manage Roles

1. Launch the controller and access the Global View.
2. Go to Accounts > Role. The SDN Controller offers four levels of default roles: **Owner**, **Super Administrator**, **Administrator**, and **Viewer**.
3. If you want to create a custom role, click Add New Role.



4. Specify the role type name and customize the permissions for the role. Click Create. The new role will be displayed in the role list.



If you want to edit/delete a custom role, click the Edit/Delete icon in the ACTION column.

9. 3 Create and Manage Local User Accounts

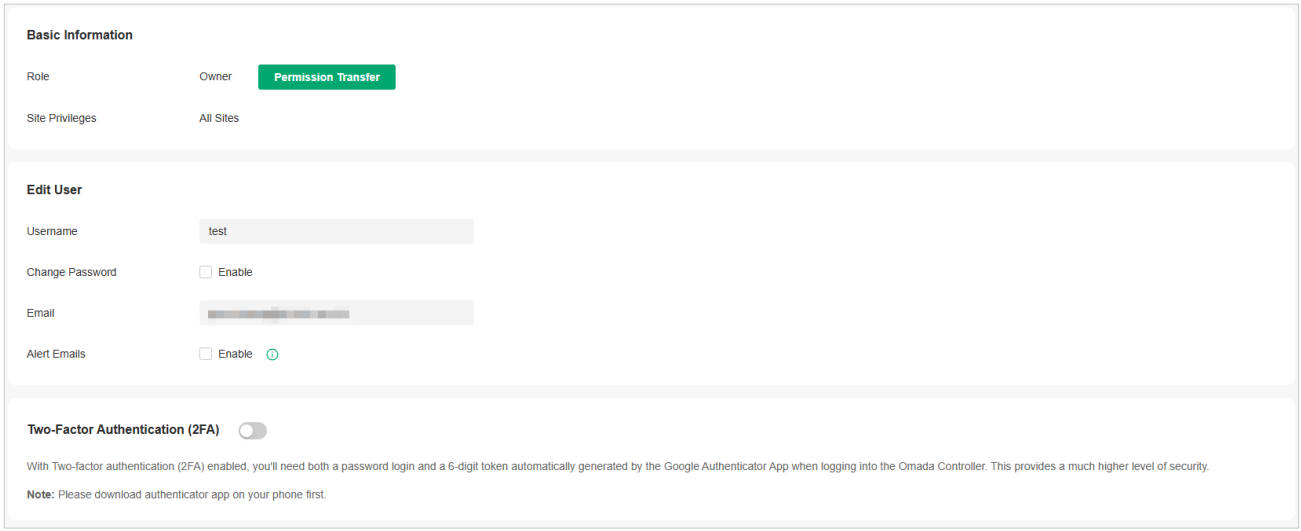
By default, the SDN Controller automatically sets up a local user with the role called Owner as the primary administrator. The username and password of the Owner are the same as that of the controller account by default. The Owner cannot be deleted, and it can create, edit, and delete other levels of user accounts.

9. 3. 1 Edit the Owner Account

To view basic information and edit the Owner account, follow these steps:

1. Launch the controller and access the Global View.

2. Go to Accounts > User.
3. Click the Edit icon in the ACTION column and enter your current password to view or change your account.
4. Check and edit the account information. Click Save.



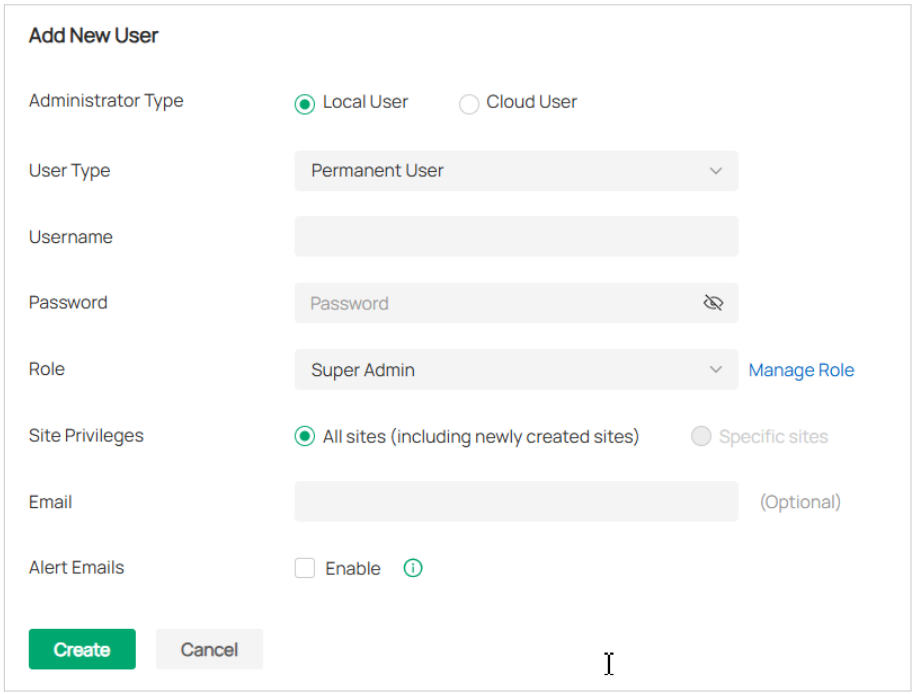
Permission Transfer	Click the button and select a new Owner to transfer the Cloud Owner permissions of the current account to the new account. The current account will be downgraded as Administrator.
Username/Change Password/Email	Change the username, password, or email address if needed.
Alert Emails	Check the box if you want the current user to receive emails about alerts of the privileged sites.
Two-Factor Authentication (2FA)	With Two-factor authentication (2FA) enabled, you'll need both a password login and a 6-digit token automatically generated by the Google Authenticator App when logging into the Omada Controller. This provides a much higher level of security.

9. 3. 2 Create and Manage Other Local Accounts

To create and manage a local user account, follow these steps:

1. Launch the controller and access the Global View.
2. Go to Accounts > User. Click Add New User.

3. Select Local User for the administrator type. Specify the parameters and click Create.



User Type	Set the user type. Permanent User: The user account will have permissions permanently unless modified or deleted. Temporary User: The user account will have permissions only in the Valid Period you set. Note that Temporary Users don't have account-related permissions, including permissions such as User Manager, Roles Manager, SAML Role Manager, SAML Users Manager, and SAML SSO Manager.
Username	Specify the username. The username should be different from the existing ones.
Password	Specify the password.
Role	Select a role for the created user account. Super Administrator: This role can manage all the other roles (except Owner) and the privileges of most features. Administrator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete Owner/Super Administrator. Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself. Custom roles: If you have created custom roles, they will be displayed in the list. To create custom roles, refer to 9. 2 Create and Manage Roles.

Site Privileges	Assign the site permissions to the created local user. All sites (including newly created sites): The created user has device permissions in all sites, including all new-created sites. Specific sites: The created user has device permission in the sites that are selected. Select the sites by checking the box before them.
Email (optional)	Enter an email address for receiving alert emails.
Alert Emails	Check the box if you want the created user to receive emails about alerts of the privileged sites. For detailed configurations, refer to 4. 1. 2 General Config.

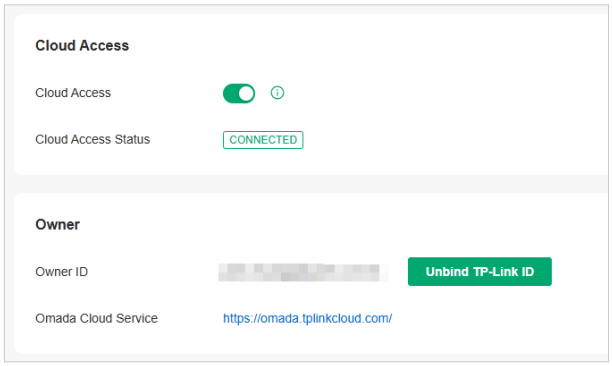
9. 4 Create and Manage Cloud User Accounts

A Cloud-Based Controller enables cloud access by default and automatically sets up the cloud Owner. An on-premise controllers automatically sets up the cloud Owner if you have enabled cloud access and bound the controller account with a TP-Link ID in the quick setup. The username and password is the same as that of the TP-Link ID. The cloud Owner is cannot be deleted, and it can create, edit, and delete other levels of user accounts.

9. 4. 1 Set Up the Cloud Owner Account

For an on-premise controller, if you have not enabled the cloud access and bound the controller with a TP-Link ID in quick setup, you can follow the steps below to set up the cloud Owner:

1. Launch the controller and access the Global View.
2. Go to Settings > Cloud Access to enable Cloud Access and bind your TP-Link ID.



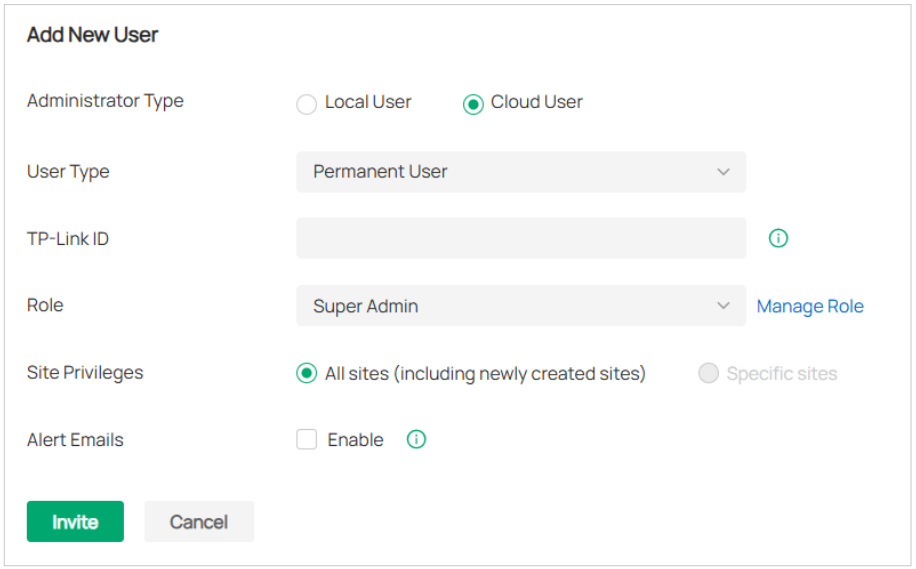
3. Go to Accounts > User. A cloud Owner with the same username as the TP-Link ID will be automatically created. The Cloud Owner cannot be deleted. You can log in with the cloud Owner when the cloud access is enabled.

9. 4. 2 Create and Manage Other Cloud Accounts

To create and manage cloud user account, follow these steps:

1. Launch the controller and access the Global View.

2. Go to Accounts > User. Click Add New User.
3. Select Cloud User for the administrator type. Specify the parameters and click Invite.



User Type	Set the user type. Permanent User: The user account will have permissions permanently unless modified or deleted. Temporary User: The user account will have permissions only in the Valid Period you set. Note that Temporary Users don't have account-related permissions, including permissions such as User Manager, Roles Manager, SAML Role Manager, SAML Users Manager, and SAML SSO Manager.
TP-Link ID	Enter an email address of the created cloud user, and then an invitation email will be sent to the email address. If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. If the email address has not been registered, it will receive an invitation email for registration. After finishing registration, it will automatically becomes a valid cloud user.
Role	Select a role for the created cloud user. Super Administrator: This role can manage all the other roles (except Owner) and the privileges of most features. Administrator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete Owner/Super Administrator and other administrator accounts. Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself. Custom roles: If you have created custom roles, they will be displayed in the list. To create custom roles, refer to 9. 2 Create and Manage Roles.

Site Privileges	Assign the site permission to the created cloud user. All: The created user has permission in all sites, including all new-created sites. Sites: The created user has permission in the sites that are selected. Select the sites by checking the box before them.
Alert Emails	Check the box if you want the created user to receive emails about alerts of the privileged sites. For detailed configurations, refer to 4. 1. 2 General Config.

9. 5 Manage User Accounts Across Controllers

Overview

If you have multiple controller, Account Manager allows you to centrally manage user accounts across controllers, assign users, enforce permissions, and streamline onboarding through Cloud Portal.

To use Account Manager, ensure your controllers meet the following requirements:

Controller Type: Omada On-Premises Networking Controllers only.

Version Required: v5.15.20 or later.

Status: Controllers must be online.

Cloud Access: Must be enabled.

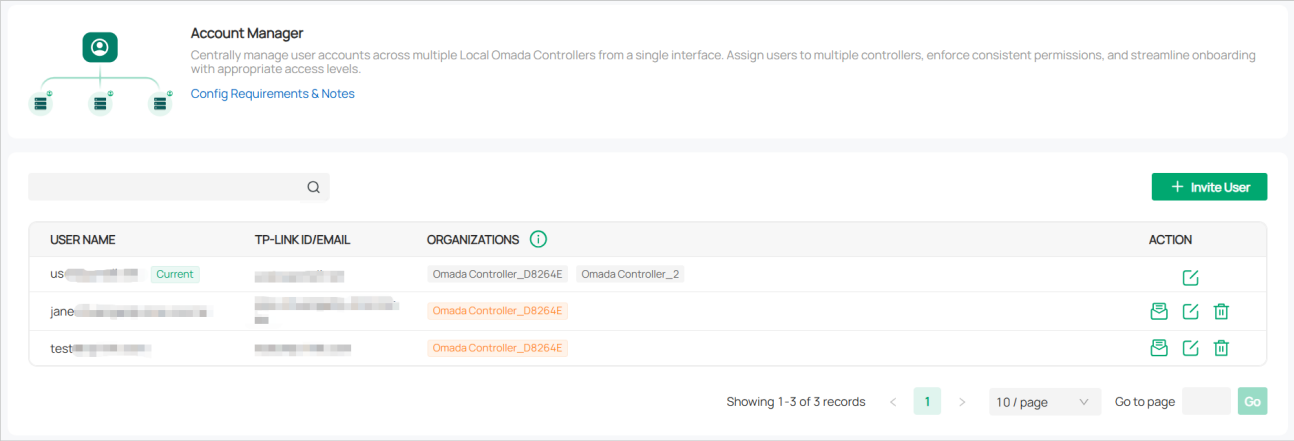
Notes:

- For MSP Controllers, permissions are applied at the MSP level.
- Account Manager currently supports Full Management (Super Admin) and View Only (Viewer) permissions.

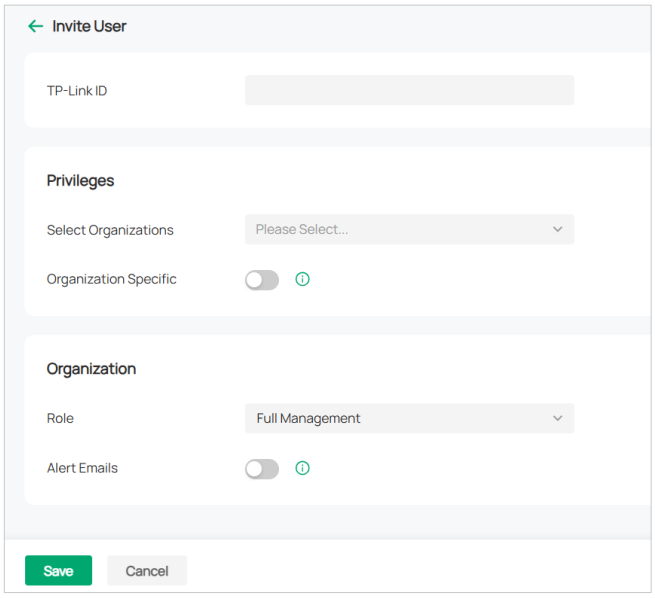
Configuration

1. Launch a web browser and visit https://omada.tplinkcloud.com. Enter your TP-Link ID and password to log in. If you do not have a TP-Link ID, create a TP-Link ID first.
2. Go to Account Manager. The user accounts of all controllers managed by the current TP-Link ID will listed. The organization column displays the status of organization invitation: yellow text indicates

that the user has been invited but not yet agreed, and gray text indicates that the user has agreed to join.



3. If you want to invite a user to help manage a controller organization, click Invite User and configure the parameters.



TP-Link ID	Enter the TP-Link ID of the user you want to invite. If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. If the email address has not been registered, it will receive an invitation email for registration. After finishing registration, it will automatically becomes a valid cloud user.
Select Organizations	Select one or multiple controller organization that the invited user can manage.
Organization Specific	Enable this option if you selected multiple controller organizations and want to configure the roles and alert settings for them separately.
Role	Set the permissions for the user: Full Management (Super Admin) or Viewer (View Only).
Alert Emails	With Alert Emails enabled, the organization will send the user emails about alerts.

Chapter 10

Manage Customer Networks in MSP Mode

MSP (Managed Service Provider) mode allows you to know the status of your customers at a glance, and manage customers in the Omada platform.

- **Customer Monitoring**

  Keep you informed of accurate, real-time status of every customer.

- **Customer Management**

  Manage all customers to deploy the whole network.

- **Account Settings**

  Manage all administrative accounts.

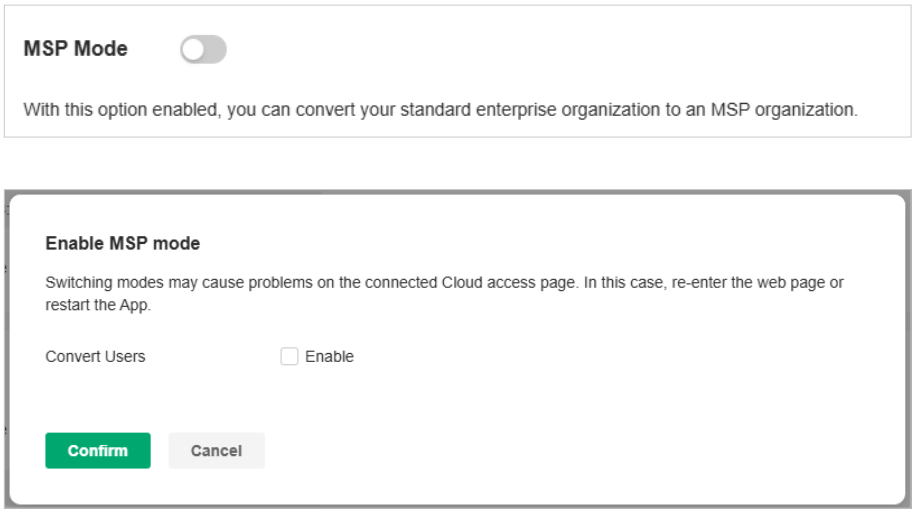
This chapter will introduce how to enable MSP mode and manage customer networks in MSP view.

- 10. 1 Quick Start
- 10. 2 Add and Manage MSP Accounts

10. 1 Quick Start

10. 1. 1 Enable the MSP Mode

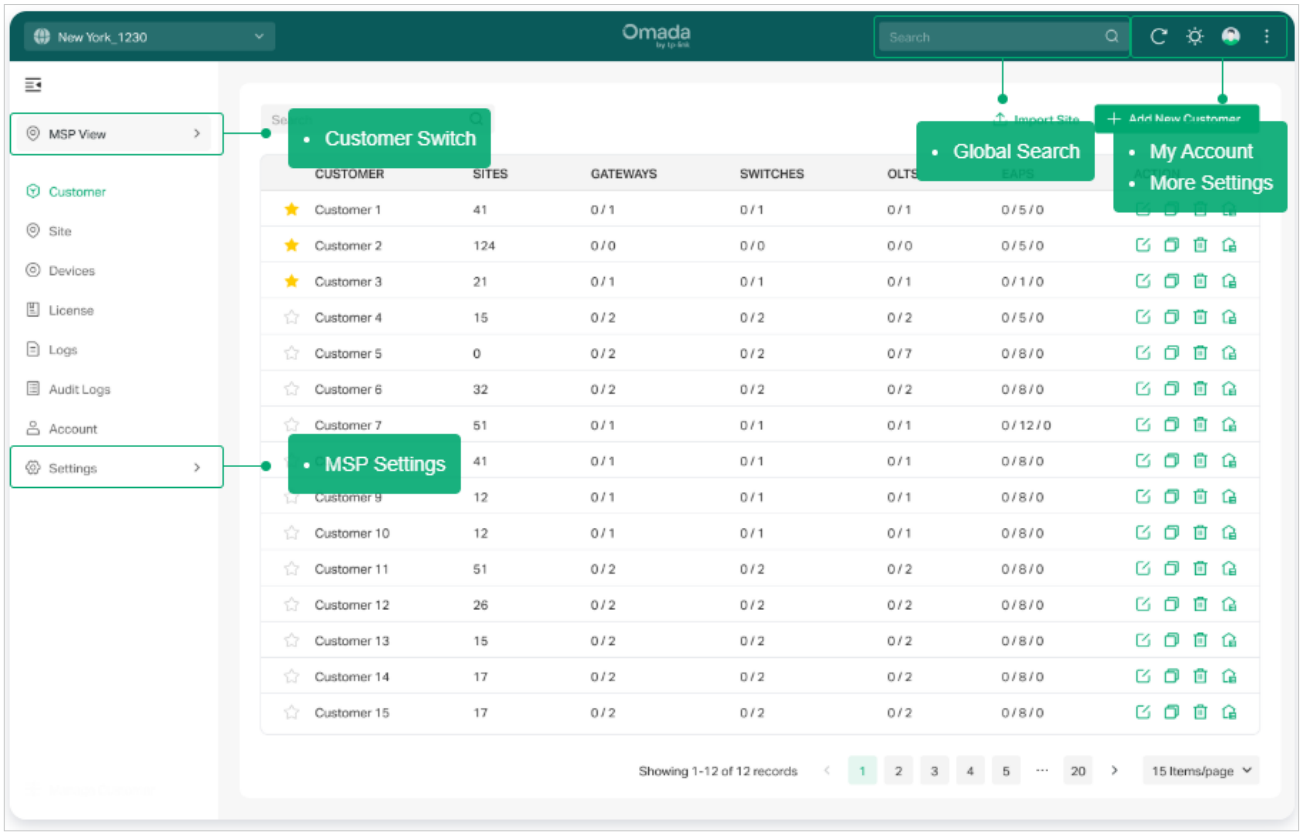
1. Launch the controller and access the Global View.
2. Go to Settings > Controller Settings. Enable MSP Mode and confirm the action to convert your standard controller system to an MSP system.



Note:

Enabling or disabling MSP mode may cause problems on the connected Cloud access page. In this case, re-enter the web page.

You will enter the MSP view.

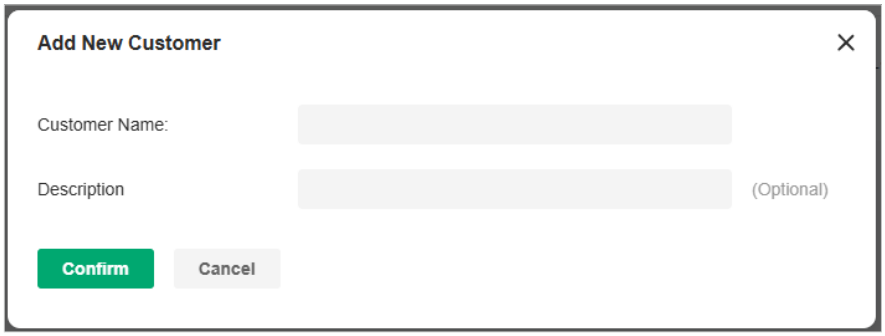


10. 1. 2 Add and Manage Customers

1. In MSP View, go to the Customer page.
2. Add customers by using one of the following methods:

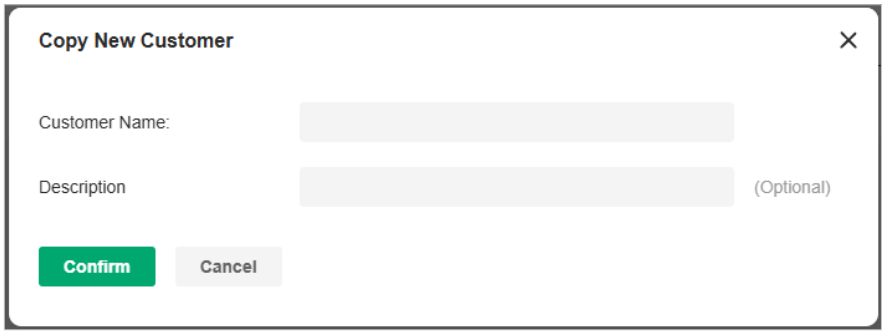
   - **Add a new customer**

     Click Add New Customer above the customer list. Specify the customer name and enter a description. Then save the settings.



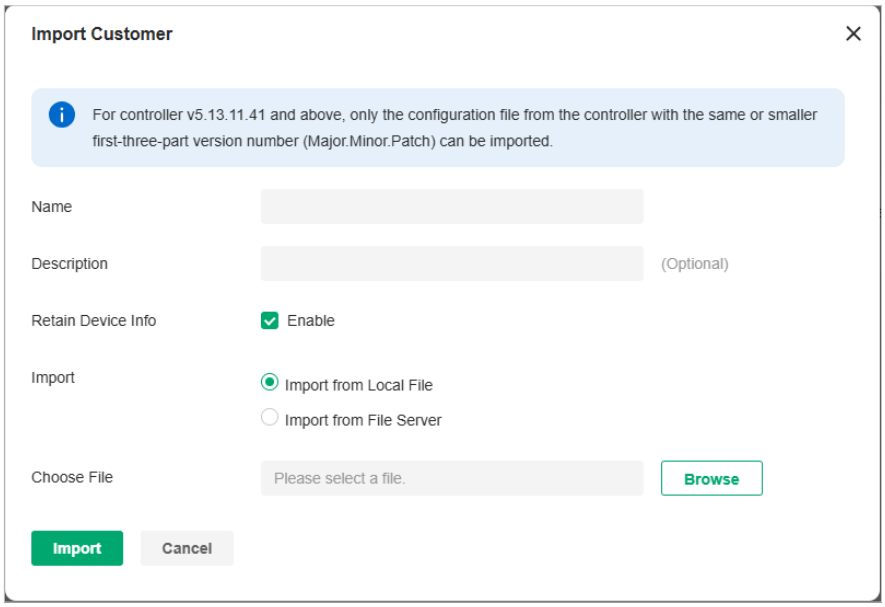
- **Copy an existing customer**

  Click the Copy icon of a customer entry. Specify the customer name and enter a description. Then save the settings.



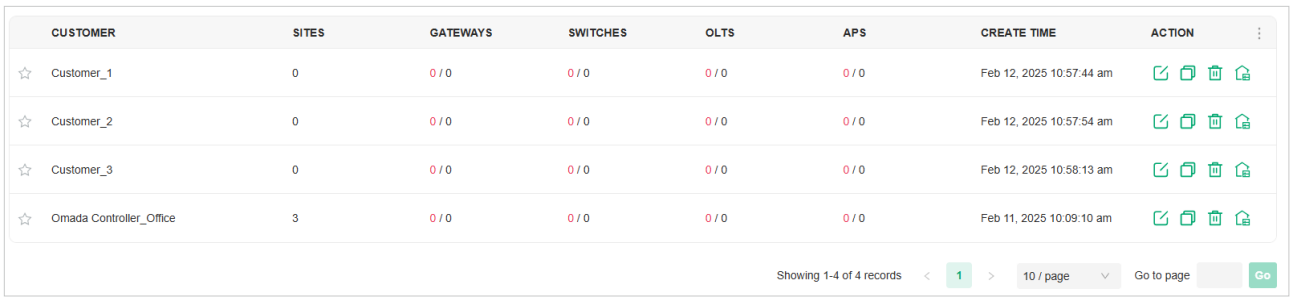
- **Import customers from another controller**

  Click Import Customer above the customer list. Specify the customer name and enter a description. Determine whether to retain device info according to your needs. Then import customer from a local file or from a file server.



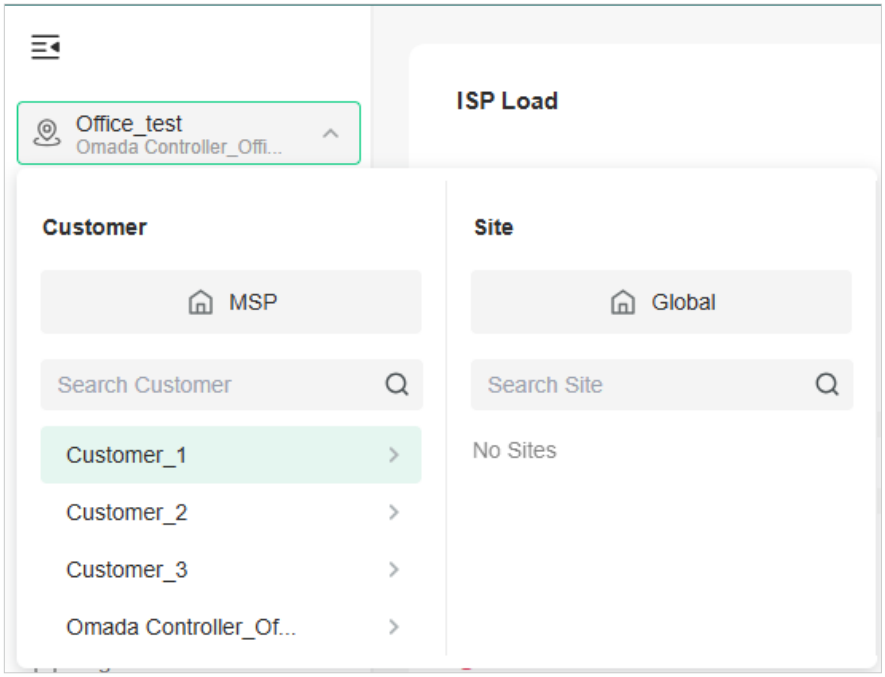
3. The new customers will be added to the customer list and the drop-down list of Customers.

   In the customer list, you can view the customer information, and click the icons in the ACTION column to manage customer entries and launch the controller of each customer.



10. 1. 3 Add Sites and Devices

1. Select a customer then click Global from the Customer drop-down list in the left of the page.



2. Add sites and adopt devices by referring to 3 Get Started with Your Network on Omada SDN Controller.

10. 2 Add and Manage MSP Accounts

Similar as a common controller, the controller in MSP mode offers multiple levels of access available for users: **MSP Owner**, **MSP Super Administrator**, MSP **Administrator**, and MSP **Viewer**. You can also create new account roles and customize their permissions to access different features.

You can use the MSP roles and user accounts on a controller in MSP mode in the same way as using the roles and user accounts on a standard controller. For more information, refer to 9 Manage Accounts of the SDN Controller.

Chapter 11

Configure Platform Integration and SAML SSO

This chapter will introduce how to configure Platform Integration and SAML SSO.

- 11. 1 Open API
- 11. 2 Webhooks
- 11. 3 SAML SSO

11. 1 Open API

Overview

Omada's Open API supports the REST API of most Controller services. This feature allows Omada users to write custom applications, embed APIs, or combine their own applications. The REST API supports HTTP GET and POST operations by providing specific URLs for each query, and the output of these operations is returned in JSON format.

To access the API securely, the Omada API framework supports the OAuth protocol for authentication and authorization, and supports the authorization code mode and client mode.

Access Token provides temporary and secure access to the API. For security reasons, Access Token has a limited lifespan. Access Token in authorization code mode uses the refresh API to obtain a new Access Token, and client mode obtains a new token through clientKey and clientSecret.

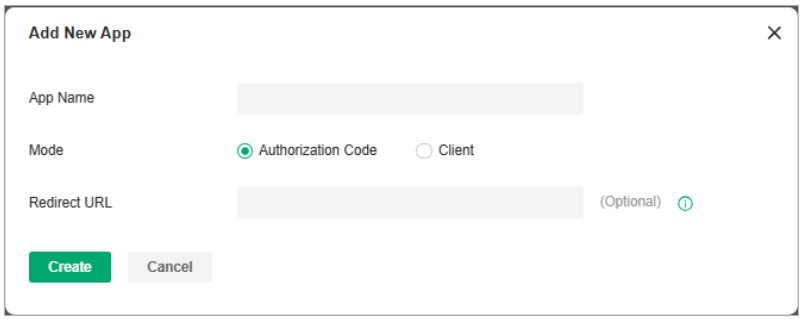
To use the Open API function, first create a new application, the smallest API access unit, which can be specified as client mode or authorization code mode. After creation, you can configure your own application for Open API access.

Configuration

1. In Global View or MSP View, go to Settings > Platform Integration > Open API.
2. Click Add New App.
3. Specify the App name, choose the access mode and configure the parameters.

   - **Authorization code mode**

   The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients. Since this is a redirection-based flow, the client must be capable of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server.

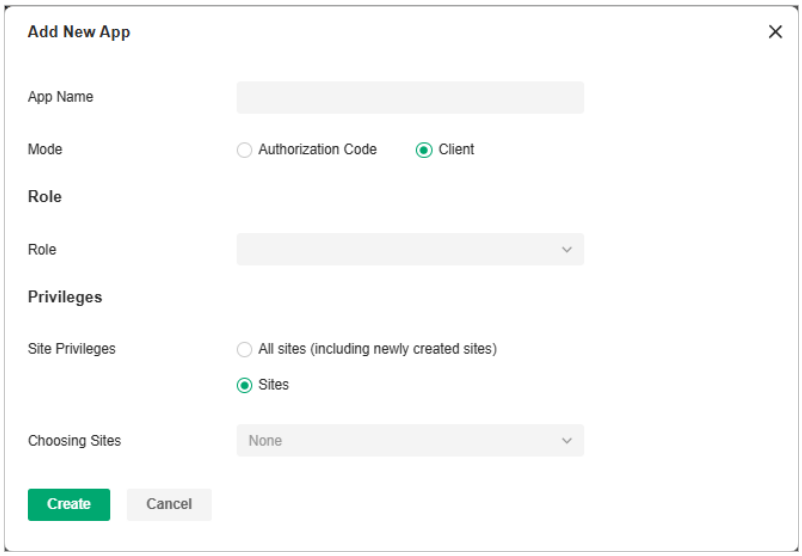


Redirect URL	Specify the redirect URL for Oauth2.0 authorization flow.

   - **Client mode**

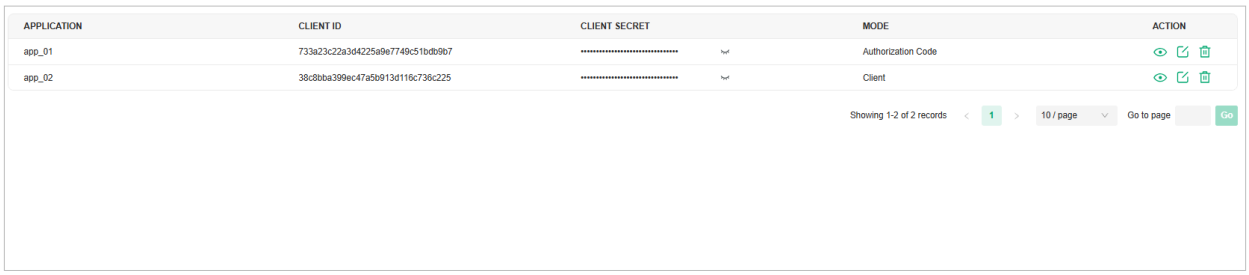
   The client can request an access token using only its client credentials (or other supported means of authentication) when the client is requesting access to the protected resources under its control,

or those of another resource owner that have been previously arranged with the authorization server (the method of which is beyond the scope of this specification).



Role	Specify the authority role of the client through the Open API.
Site Privileges	Specify the site privileges of the client through the Open API.

4. Apply the settings. The application will be added for Open API access.



For more instructions, click Online API Document in the upper right corner of the page to get the Open API Access Guide.

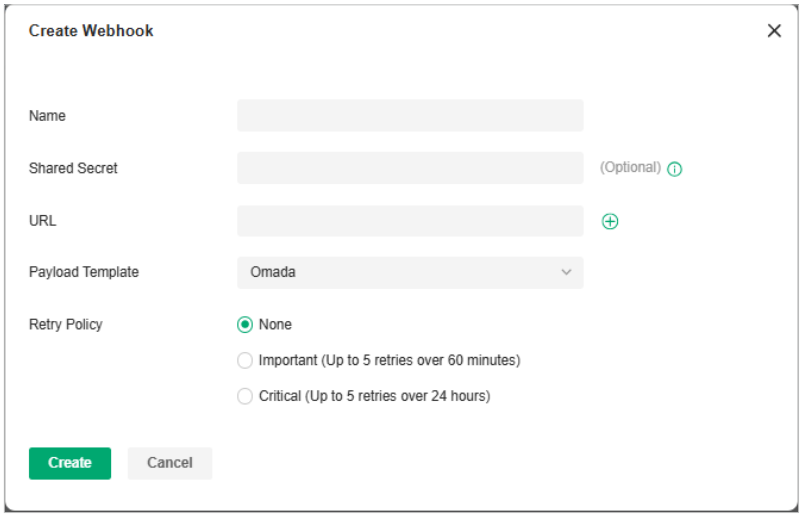
11. 2 Webhooks

Overview

Webhook is an API concept and one of the usage paradigms of microservice APIs. It is also called a reverse API, that is, the front end does not actively send requests, but is completely pushed by the back end. In Omada, Webhook is used for the active push function of messages such as alerts.

Configuration

1. In Global View or MSP View, go to Settings > Platform Integration > Webhooks.
2. Click Create New Webhook.



Name	Specify the Webhook entry name.
Shared Secret	Specify the authentication secret key. If it is not filled in, the system will automatically generate a key. If it is manually cleared, the system will no longer generate a key.
URL	Specify the Webhook URL address.
Payload Template	Select a template for message push.
Retry Policy	Specify the Webhook retry policy: None (no retry), Important (up to 5 retries over 60 minutes), and Critical (up to 5 retries over 24 hours).

3. Save the settings. The webhook entry will be added.



You can click the icon in the ACTION column to test the connectivity, view the dispatch logs, and edit, or delete the Webhook entry.

11. 3 SAML SSO

Overview

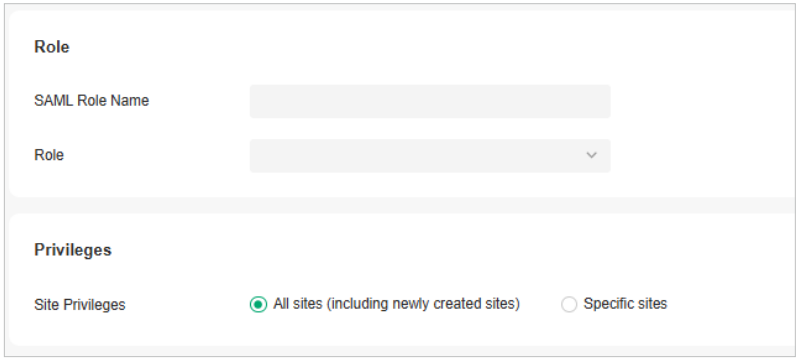
SAML (Security Assertion Markup Language) SSO (Single Sign On) enables clients to access multiple web applications using one set of login credentials. To complete the SAML SSO interconnection, the system administrator needs to configure the IdP (identity provider) information when the current system serves as the SP (service provider), or configure the SP information when the current system serves as the IdP.

Prerequisites

- This chapter takes the configuration of the current system as an example to explain the operation. Other systems also need to be configured. SAML SSO works only after all systems are configured.
- If you need to connect with other systems that serve as the IdP, please obtain the metadata file of the IdP first, then configure the SP.
- If you need to connect with a third-party IdP, please configure the third-party IdP first and obtain its metadata file.

Configuration

1. Configure the SAML role.
   a. In Global View or MSP View, go to Account > SAML Role.
   b. Click Add New SAML Role. Configure the parameters and click Create.



SAML Role Name	Specify the role name.
Role	Specify the authority role of the account.
Site Privileges	Specify the site privileges of the client through the Open API.

2. Configure the IdP.
   Use a third-party system as the IdP and follow the steps below to configure the parameters:
   a. Create an IdP. Fill in the initial information except the name.

b. Use the IdP metadata information for SP configuration on the Controller.

c. Edit the IdP information, including Entity ID, Sign-On URL, and Relay State.

Note:

- The above three parameters use the information of View SAML Attribute in SP configuration.
- Relay State is base64(resourceId_omadaId).

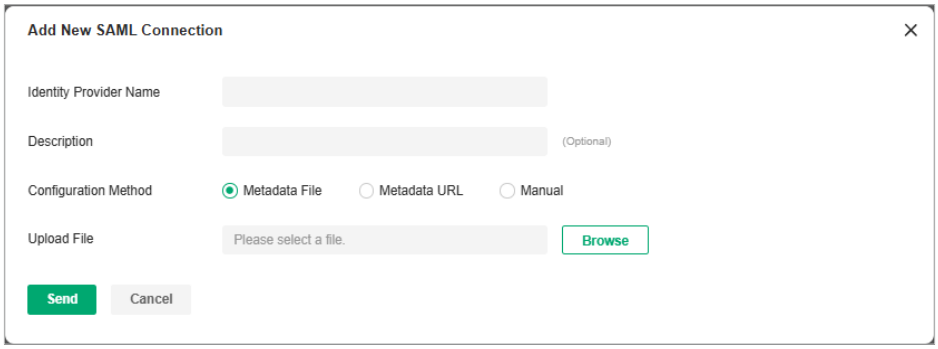
d. Edit the Attribute, and configure the username and usergroup_name. The usergroup_name is the SAML Role Name you configured in step 1.

3. Configure the SP.

Use the Controller as the SP and follow the steps below to configure the parameters:

a. In Global View or MSP View, go to Settings > SAML SSO.

b. Click Add New SAML Connection.



Identity Provider Name	Specify the IdP name.
Description	Enter a description for identification.
Configuration Method	Configure the metadata. You can upload the metadata file, use URL parsing, or manually fill in the information.

c. Click View SAML Attribute to view the SP configuration. This will be used for IdP configuration on the third-party system.

Subsequent Processing

After configuring all systems, verify whether the SAML SSO configuration is successful as follows:

1. In the configured IdP system, find the SP login entry and click to log in.
2. On the login page, enter the Username and Password to log in.
3. Go to the SP system and verify that the user has logged in.

Chapter 12

Configure SD-WAN

This chapter will introduce how to configure SD-WAN.

Overview

SD-WAN, or Software-Defined Wide Area Network, allows you to easily connect multiple gateways together without complicated VPN configuration. It helps reduce wide area network expenses, improve network connection flexibility, and provide secure and reliable interconnection services for enterprise networks and data center networks scattered across a wide geographical range.

Omada Controller implements SD-WAN networking based on the Hub-Spoke mode, which allows you to quickly establish network connections between multiple sites; it also supports setting up direct channels between specified sites to improve communication efficiency.

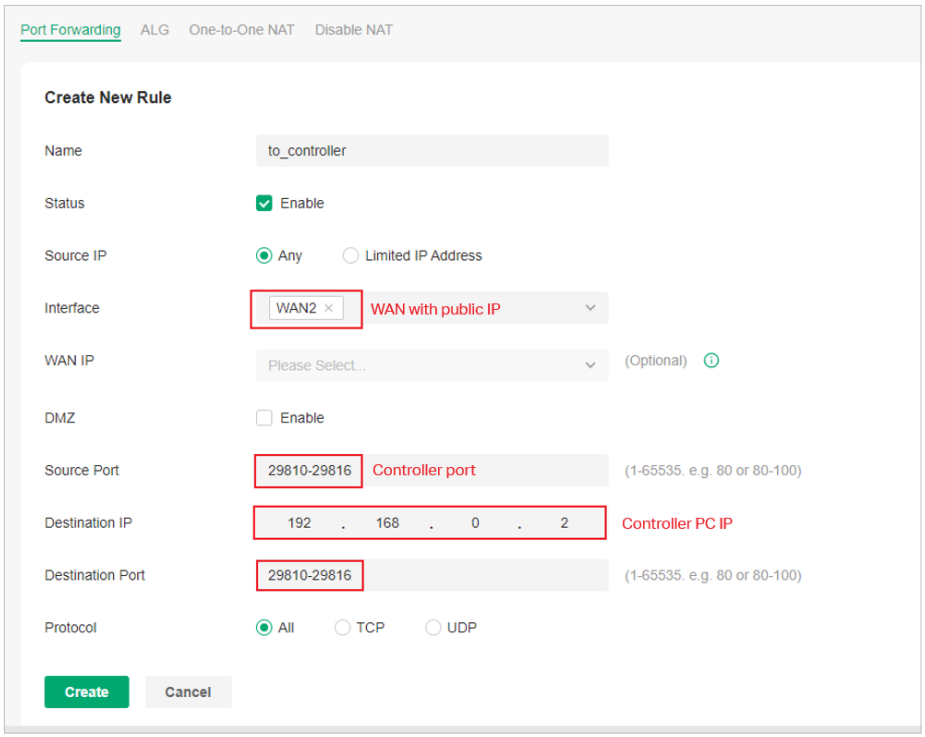
Requirements

To use SD-WAN, ensure the following:

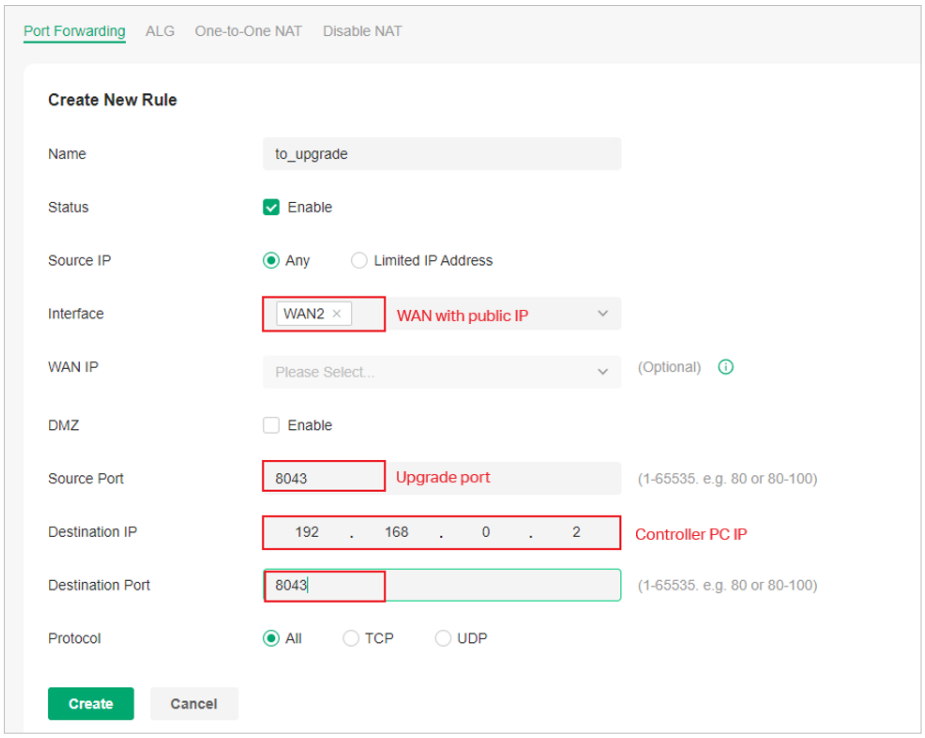
- At least one gateway in your network has a public IP address.
- The WAN networks of the gateways have not enable DMZ.
- The network segments in the network do not conflict with each other or the LAN of other sites.

Configuration

1. Adopt the gateway that has a public IP address through the LAN side.
2. Configure port forwarding on the adopted gateway for adoption of other gateways.
   a. Go to Settings > Transmission > NAT > Port.
   b. Add a Port Forwarding rule for the controller port, as shown in the following figure:

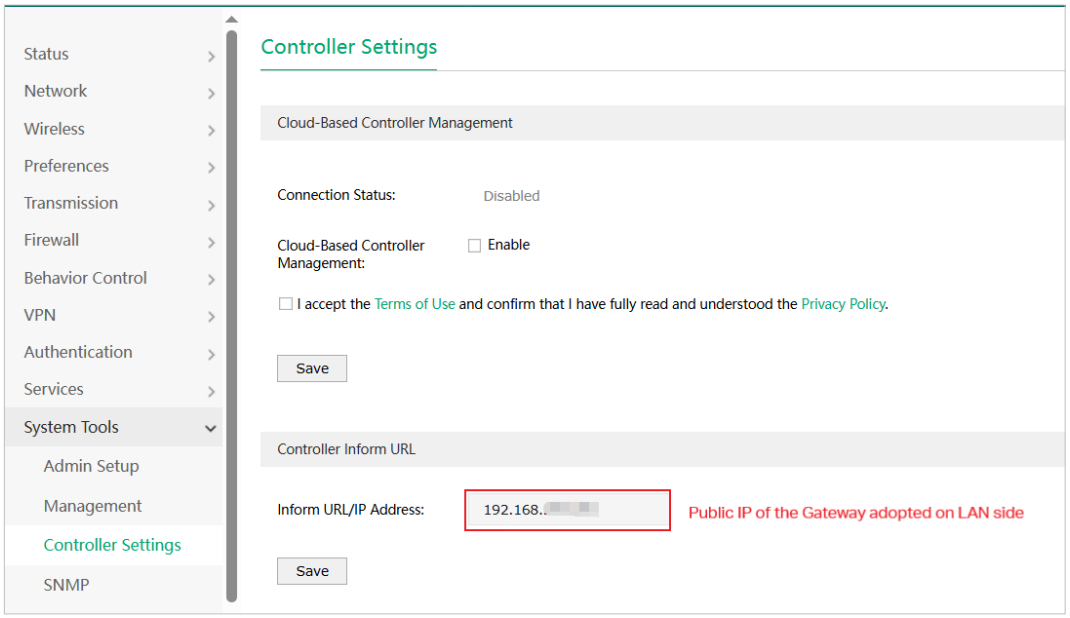


c. If you need to upgrade devices through the controller, add a port forwarding rule for upgrade port 8043, as shown in the following figure:



3. Adopt other gateways through the WAN side.

a. On the standalone page of each gateway, set the Controller Inform URL/IP to the public IP of the gateway adopted on the LAN side, as shown in the following figure:

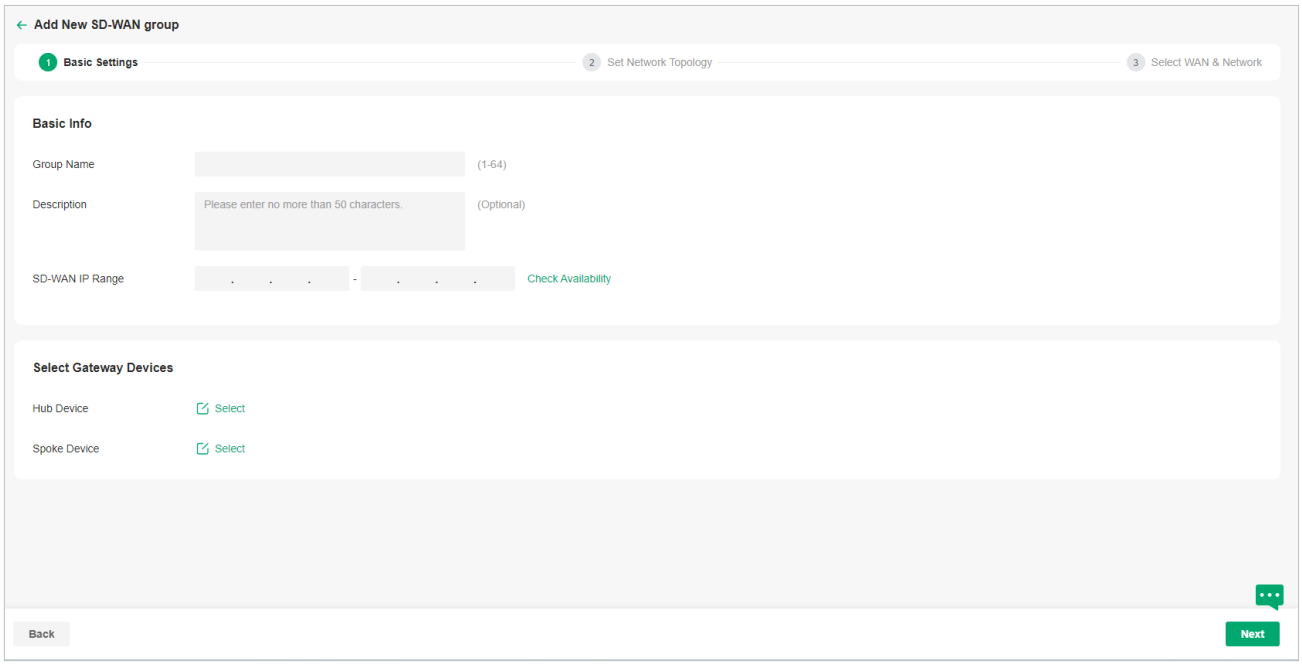


b. On the controller page, create a site for each gateway and adopt them to the sites.

4. Configure SD-WAN.

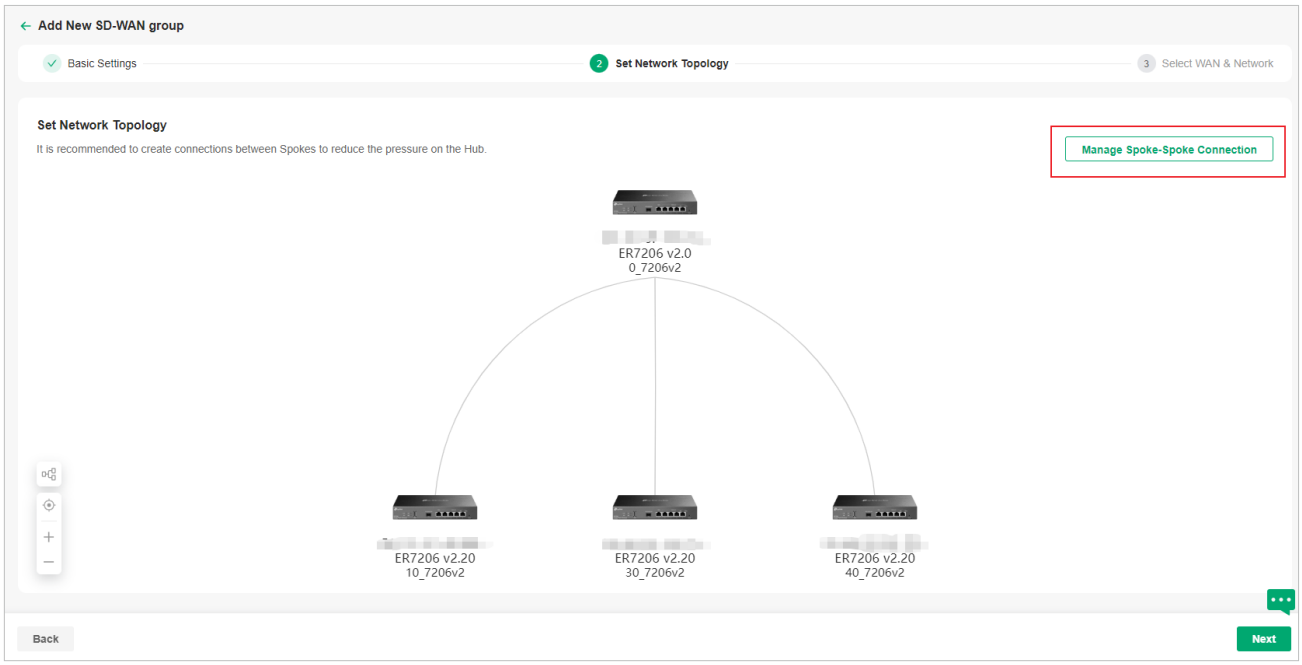
a. In Global View, go to SD-WAN. Click Create SD-WAN Group.

b. Configure basic settings, then click Next.



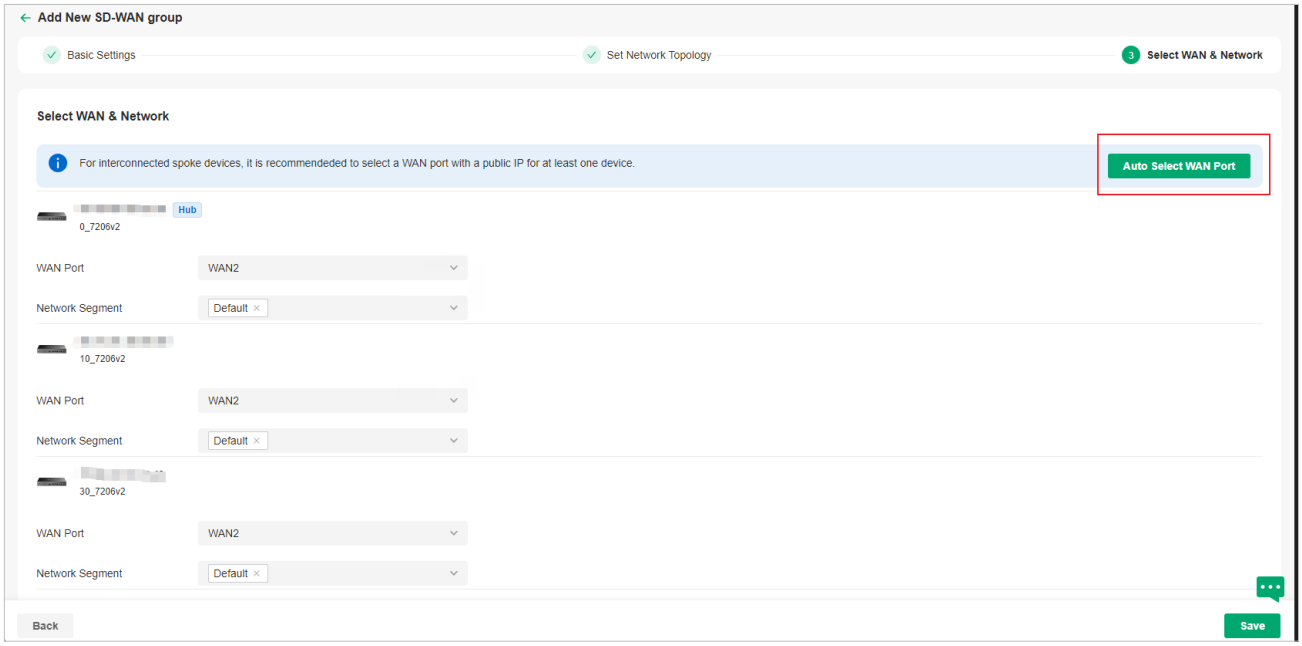
Group Name	Specify the name of the group.
Description	Enter a description for identification.
SD-WAN IP Range	Specify the IP range for the controller to assign virtual IP addresses to VPN interfaces. Ensure the IP range contains at least 16 IP addresses. After filling in the information, click Check Availability to perform conflict detection on the IP range.
Hub Device	Click to select a hub device from the listed gateways. Only the gateways with public IP addresses will be listed.
Spoke Device	Click to select spoke devices from the listed gateways.

c. Set the network topology. It is recommended to click Manage Spoke-Spoke Connection to create connections between spokes to reduce the pressure on the hub. Click Next.

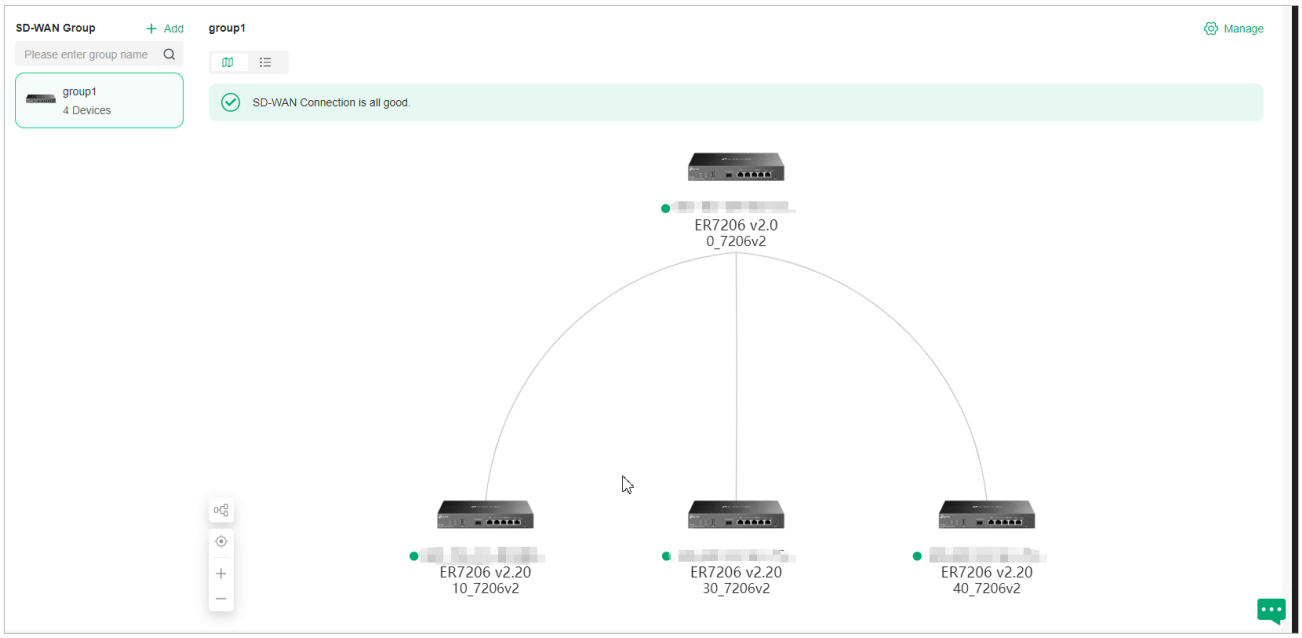


d. Select WAN and network. Then click Next.

WAN Port	Click Auto Select WAN Port and the controller will automatically select a WAN with a public IP or a WAN with the smallest number of ports and an IP for each gateway. You can also customize the configuration for each gateway.
Network Segment	This controller automatically adds the Default LAN of each gateway to the Network Segment. You can also customize the configuration for each gateway. Ensure all network segments in the network do not conflict with LANs in other sites.



e. Save the settings. The SD-WAN group will be added.


SD-WAN Group
Add
Please enter group name
group1
4 Devices
group1
Manage
SD-WAN Connection is all good.
ER7206 v2.0
0_7206v2
ER7206 v2.20
10_7206v2
ER7206 v2.20
30_7206v2
ER7206 v2.20
40_7206v2

Chapter 13

Configure Multi-Controller Clusters

This chapter will introduce how to configure multi-controller clusters.

13. 1 Introduction to Multi-Controller Clusters

A multi-controller cluster is a group of interconnected controllers that work together as a single system to enable high availability and can be recognized as a Cluster System. Each controller (node) in the cluster works on a part of the task. If one controller fails, others will take over tasks, preventing system interruptions. This reduces the impact of controller failures on authentication and other online services and facilitates centralized management across multiple controllers.

Omada Controller supports two cluster modes:

- **Hot-Standby Backup Mode**

In this mode, there is a primary node and a secondary node. Generally, the primary node is responsible for network management and process running, while the secondary node synchronizes data with the primary node. If the primary node goes down, the secondary node will take over network and clients management. During the failover, the devices will go offline for a short time, then they will reconnect to the new primary node when the devices get connected again, all services will run normally. If the previous primary node recovers from failover, it will continue to run as a secondary node.

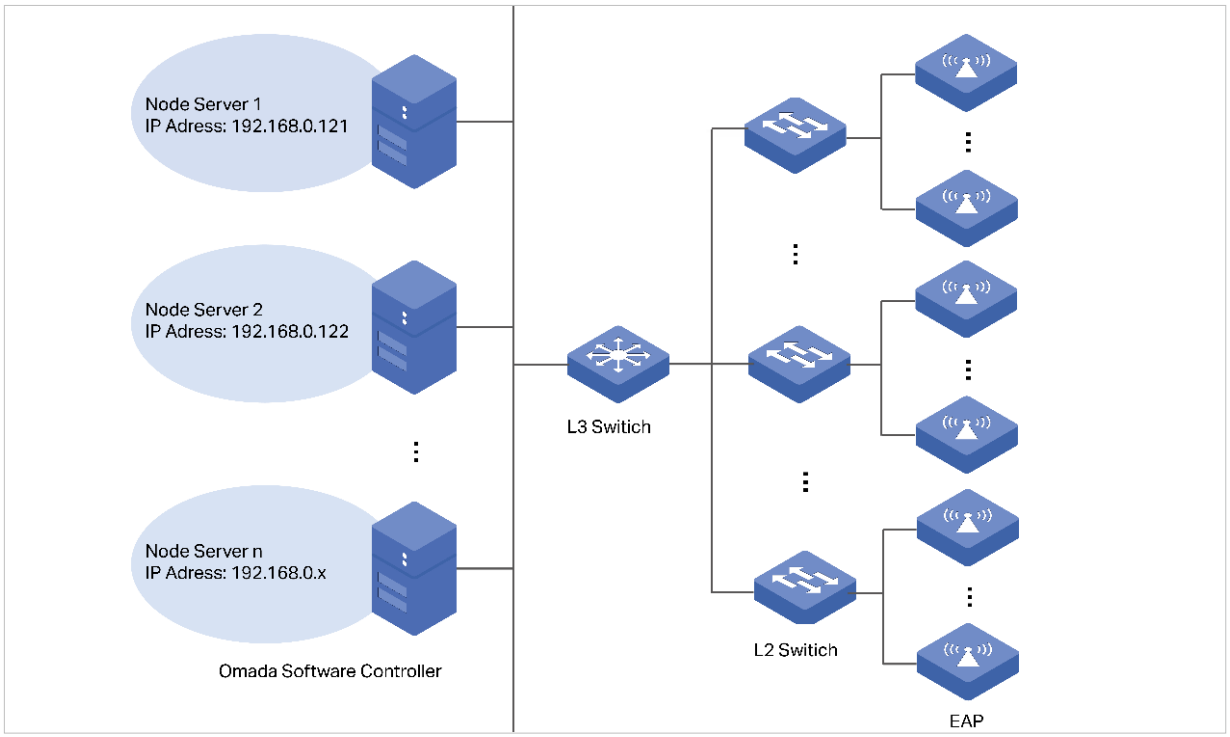
Notes:

- For OC300, the management scale will be reduced to half its original size after enabling Hot-Standby Backup Mode.
- For Linux system, ensure the primary node and secondary node server configurations are the same. The new primary node after switching nodes will remain unchanged until the next switch.

- **Distributed Cluster Mode.**

In this mode, multiple nodes collaborate to manage Omada devices. This collaborative approach not only significantly increases the upper limit of the number of devices that the Controller can manage, but also, through the coordinated operation of multiple nodes, ensures the high - availability of the entire network. If a node failure occurs, automatic load balancing will be triggered, and the services of the failed node will be taken over by other nodes. During the failover period, the devices under the site managed by the original failed node will be briefly offline and then automatically reconnect to other nodes. Once the devices resume the “Connected” state, all services will operate normally.

Below is a typical distributed cluster deployment topology, where multiple nodes (three nodes or more) can jointly manage Omada devices.



13. 2 Configure Hot-Standby Backup Mode on Omada Controllers

Requirements

- Omada Software Controller(Linux, v5.15.20 and above)/Omada Hardware Controller(OC300 / OC400, Built-in Controller v5.15.20 and above)
- Linux System(Ubuntu 20.04/22.04, Debian 8/9/10/11/12)

Prerequisites and Precautions

- Ensure the JDK and MongoDB versions are consistent across all nodes.
- Set static IP addresses for your controllers. For Linux Controller, it is recommended to set static IP before enabling Cluster Mode to avoid abnormalities in the connections between nodes due to dynamic IP changes. For Hardware Controller, it's a mandatory requirement that the IP of nodes should be static under Cluster Mode.
- It is recommended to deploy all nodes within the same network segment.
- The original data of the secondary node will be overwritten by the data of the primary node. The settings will take effect after rebooting. This process involves data synchronization and may take a long time.
- If you are using hardware controller, during startup, the secondary node needs to successfully connect to the primary node before it can continue to startup, and the web page of Hardware

Controller may be unresponsive for a long time.

Configuration

1. (For Linux Controller) Modifying the handle count of the system is a prerequisite for using the Controller Hot-Standby Backup Mode. Edit **/etc/security/limits.conf**, add the following parameters, save the file, log out and log back in to make the changes take effect.

   *** soft nofile 65535**

   *** hard nofile 65535**

   Note: The methods of modifying handle number may vary by Linux version. Please modify the handle number according to Linux version.

2. Set static IP addresses for your controllers, and keep them in the same subnet.

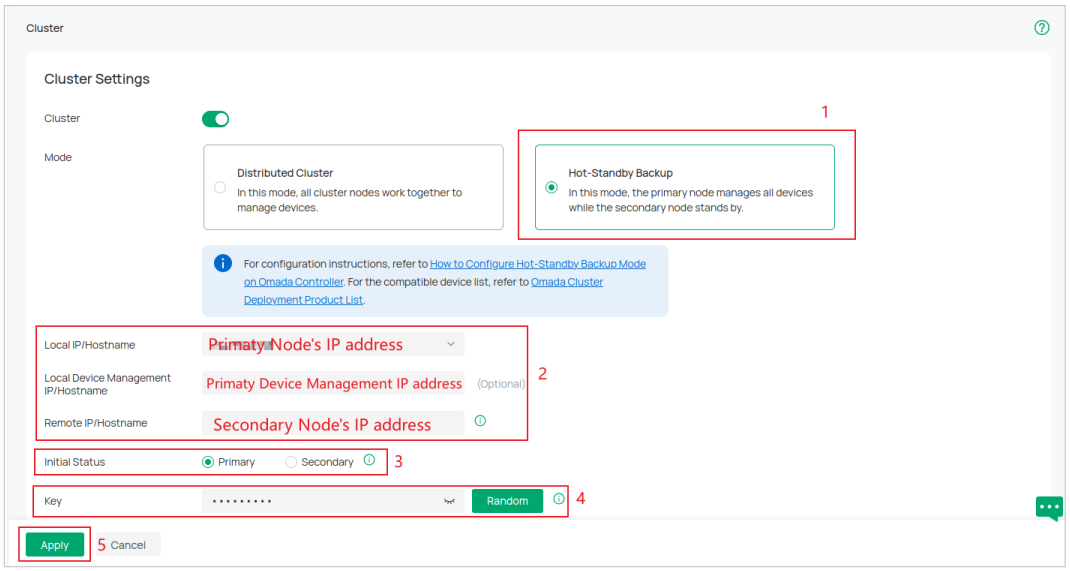
   • For Linux Controller, it is recommended to set static IP before enabling Cluster Mode to avoid abnormalities in the connections between nodes due to dynamic IP changes.

   • For Hardware Controller, it's a mandatory requirement that the IP of nodes should be static under Cluster Mode.

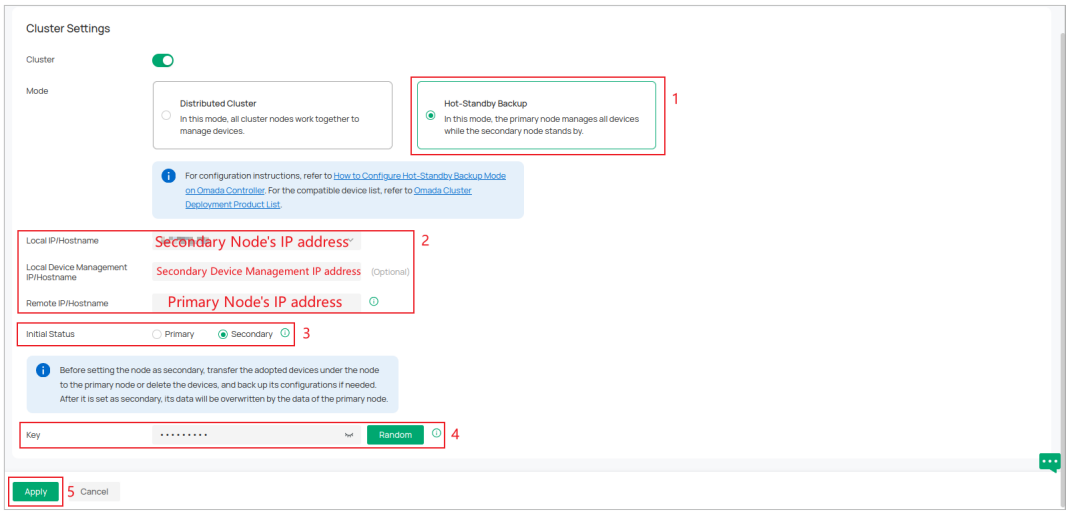
3. Configure cluster settings.

   a. In Global View, go to Settings > Cluster, and enable Cluster.

   b. For the primary node, select the mode as Hot-Standby Backup. Input the IP address of the primary node in the Local IP/Hostname field and the IP address of the secondary node in the Remote IP/Hostname field. Choose Primary as Initial Status. Customize the Key and remember it.



   c. For the secondary node, select the mode as Hot-Standby Backup. Input the IP address of the secondary node in the Local IP/Hostname field and the IP address of the primary node in the Remote IP/Hostname field. Choose Secondary as Initial Status. Input the same Key as the primary node's.



Note: If you are going to set one running controller as the secondary node, migrate all the devices of this controller to the primary node or forget them all. It is recommended to back up your configuration before cluster configuration. After it's set as secondary node, its data will be overwritten by the data of the primary node.

4. Reboot the primary node and the secondary node.
   - For Hardware Controller, just reboot the Controller with the Reboot feature.
   - For Linux Controller, use the **sudo tpeap restart** command on your Linux System:

   The cluster will be established after the nodes reboot.

For more instructions and related FAQs, refer to How to Configure Hot-Standby Backup Mode on Omada Controller.

13. 3 Configure Distributed Cluster Mode on Linux Controllers

Requirements

- Omada Software Controller
- Ubuntu 22.04
- JAVA17
- Mongodb v7.0

Prerequisites and Precautions

- The Distributed cluster mode requires at least three nodes. Prepare to deploy at least three controllers before setting it up.
- Installing the distributed cluster mode requires Java 17. Use the **sudo apt install openjdk-17-jre-headless** command to install Java 17.
- Modifying the handle count of the system is a prerequisite for using the Controller distributed cluster mode. Edit **/etc/security/limits.conf**, add the following parameters, save the file, log out and

log back in to make the changes take effect.

*** soft nofile 65535**

*** hard nofile 65535**

- The methods of modifying handle number may vary by Linux version. Please modify the handle number according to Linux version.
- Ensure the system time of each node is consistent, with a time difference of less than 20 seconds.
- Ensure the JDK and MongoDB versions are consistent across all nodes.
- Node IPs only support static IPs. If you need to modify the IP/port, you will need to re-initialize.
- It is recommended to deploy all nodes within the same network segment.

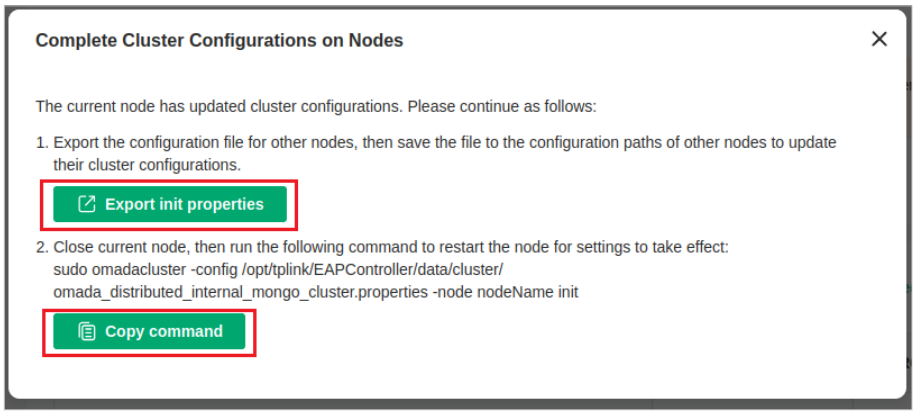
13. 3. 1 Configure an Existing Controller via Web

1. In Global View, go to Settings > Cluster and enable Cluster. Then select the mode as Distributed Cluster.
2. Click Add Node to add at least three nodes. Input these nodes' NAME and NODE MANAGEMENT HOSTNAME/IP. Here, IPs and hostnames should correspond to different servers. Please specify the IP address of the management device in DEVICE MANAGEMENT HOSTNAME/IP. This IP address will be used to establish a connection and communicate with the device. If it is not specified, NODE MANAGEMENT HOSTNAME/IP will be used by default. Then click Apply.

   After that, Controller will pop up a prompt window and the init properties file. Download the init properties file and reboot the Controller for the settings to take effect.

   Notes:

   - Please reboot nodes as soon as possible to prevent device disconnection or other problems.
   - Nodes added offline will be considered down - state nodes, which will affect the disaster recovery capability. Please initiate them as soon as possible.



3. Replace the properties file you downloaded at each node respectively. The path to the properties file is:

   /opt/tplink/EAPController/data/cluster/omada_distributed_internal_mongo_cluster.properties

4. Execute the initialization command on each node respectively. When initializing nodes, set the

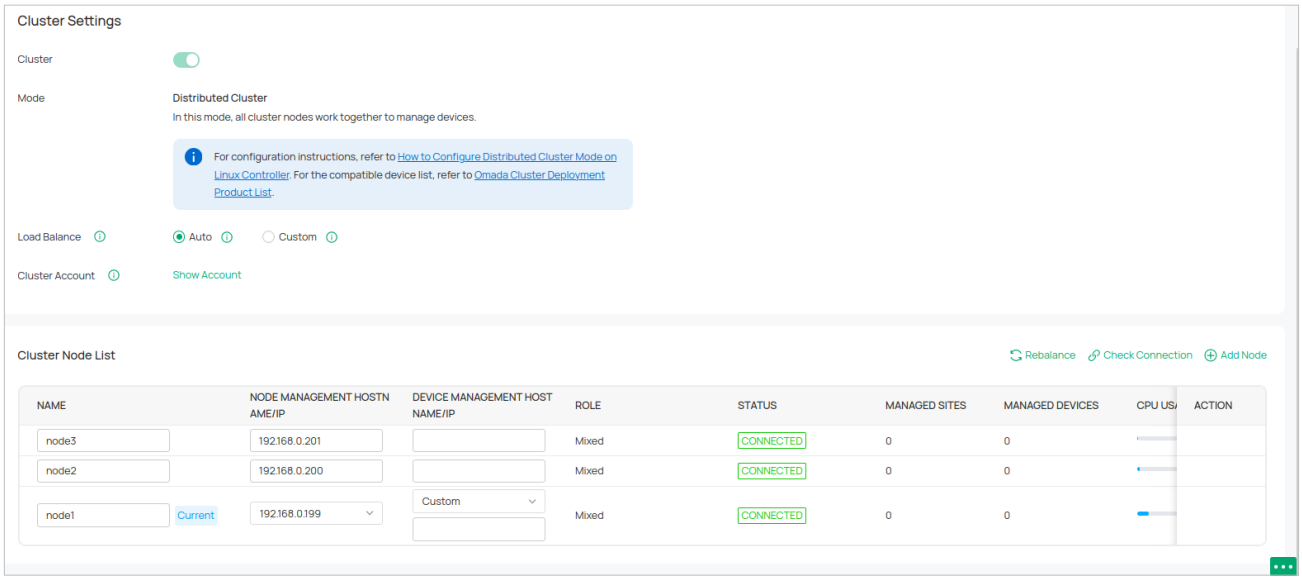
account and password for all nodes. When initializing nodes, first initialize the primary node (the one exporting init properties). Otherwise, initialization may fail.

sudo omadacluster -config

/opt/tplink/EAPController/data/cluster/omada_distributed_internal_mongo_cluster.properties -nodeName init

```
root@node1-VirtualBox:/home/node1# sudo omadacluster -config /opt/tplink/EAPController/data/cluster/omada_distributed_internal_mongo
_cluster.properties -node node1 init
check omada
Omada Controller is already running.
Stopping Omada Controller
Stop successfully.
Number of mixed members: 3
Check node ips: 192.168.0.121 192.168.0.122 192.168.0.123
Please enter your cluster username: admin
Please enter your cluster password: You have entered cluster username: admin, password: Tplink123 . Are you sure? (y/n): y
```

5. After the deployment is successful, go to the Cluster page to confirm. And when the distributed cluster mode is running properly, you can access the Controller through any node.



13. 3. 2 Configure a New Controller via Commands

1. Select cluster mode installation (does not automatically start after installation).

   - Install using deb

   echo "omadac omadac/init-cluster-mode boolean true" | sudo debconf-set-selections

   sudo dpkg -i /path/to/controller_installation_package

```
root@node3-VirtualBox:/home/node3# echo "omadac omadac/init-cluster-mode boolean true" | sudo debconf-set-selections
root@node3-VirtualBox:/home/node3# dpkg -i omada_v5.15.20.7_linux_x64_20250113193653.deb
```

   - Install using tar.gz

   After decompression, deploy the cluster mode via the shell installation script. Enter **./install.sh init - cluster – mode**, the system will not start automatically after installation, and relevant prompt information for setting up the cluster will be printed.

```
root@node3-VirtualBox:/home/node3/Omada_SDN_Controller_v5.15.20.7_x64# sudo ./install.sh init-cluster-mode
```

2. Start installing the Controller and edit the properties file as prompted.

```
root@node1-VirtualBox:/home/node1# dpkg -i omada_v5.15.20.10_linux_x64_20250119195257.deb
Selecting previously unselected package omadac.
(Reading database ... 160648 files and directories currently installed.)
Preparing to unpack omada_v5.15.20.10_linux_x64_20250119195257.deb ...
Start controller distributed cluster mode.
Cannot locate Java Home
Unpacking omadac (5.15.20.10) ...
Setting up omadac (5.15.20.10) ...
Start controller distributed cluster mode.
Install Omada Controller succeeded!
=========================
current data is empty
Before enabling the cluster mode, first configure the system environment by referring to the Cluster UG(https://www.omadanetworks.com/en/support/faq/4347/). Th
en please edit the properties file that specifies the cluster mode in directory /opt/tplink/EAPController/data/cluster and use command 'sudo omadacluster -conf
ig <properties_path> -node <node_name> init' to initialize the cluster node.
Controllers that have not completed cluster initialization will still start in normal mode.
Usage: /usr/bin/omadacluster [<option> ...] <command>

Commands:
  help                                              - this screen
  -config <properties_file> -node <node_name> init  - Initialize a specific cluster node using a specified configuration file

Options:
  -config                                           - cluster properties file
  -node                                             - node name

======================
Processing triggers for systemd (245.4-4ubuntu3.20) ...
```

Modify each node's properties file **/opt/tplink/EAPController/data/cluster/omada_distributed_internal_mongo_cluster.properties**

```
## local cluster config
# Cluster mode, distributed: Distributed Cluster
omada.cluster.mode=distributed
# internal: internal mongodb server
omada.cluster.distributed.mongo.mode=internal

## Distributed Cluster Config
## Please edit:
omada.cluster.distributed.mongo.replset.name=omadaReplSet
# Cluster member names list
omada.cluster.distributed.names=node1,node2,node3

# To preserve the data node, if not configured, it defaults to 'node1'.
# It can only be a node with a mixed node role.
omada.cluster.distributed.primary.data.node=node1
omada.cluster.distributed.node1.host=192.168.0.121
# node1.role:mixed or service. mixed: node that provides service with data(At least 3 mixed nodes); service: node that only provides service without data
omada.cluster.distributed.node1.role=mixed

omada.cluster.distributed.node2.host=192.168.0.122
omada.cluster.distributed.node2.role=mixed

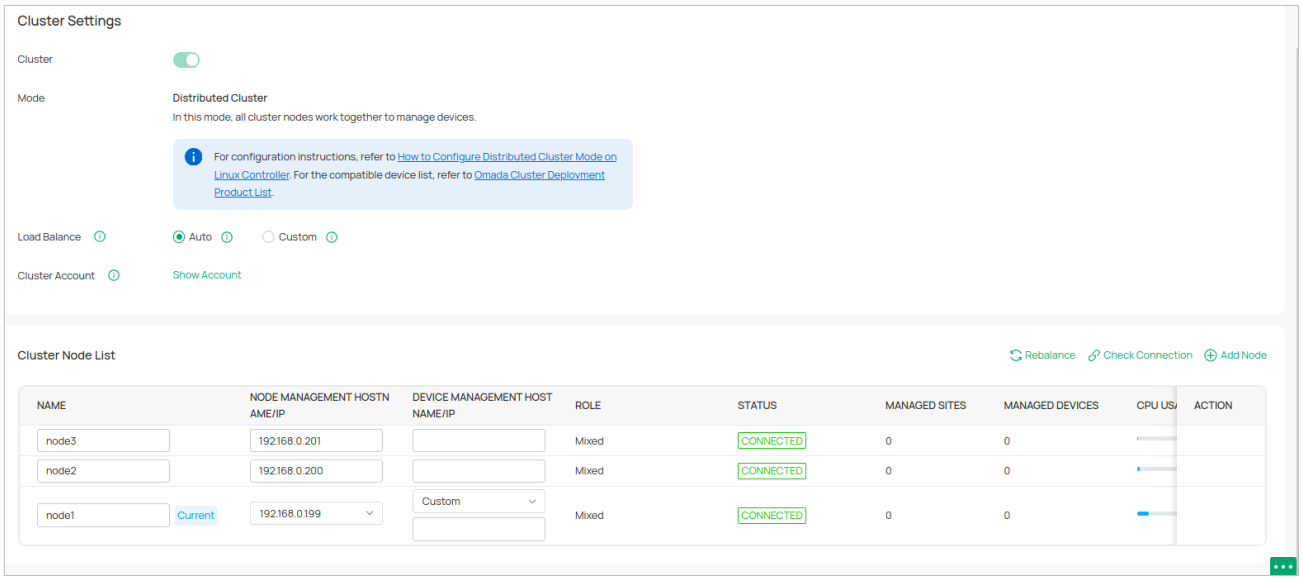
omada.cluster.distributed.node3.host=192.168.0.123
omada.cluster.distributed.node3.role=mixed
```

3. Execute the initialization command on each node respectively.

   sudo omadacluster -config /opt/tplink/EAPController/data/cluster/omada_distributed_internal_mongo_cluster.properties -node <nodeName> init

4. After the deployment is successful, log in to the Controller and set the username and password, and other nodes will synchronize the username and password.

   Then go to the Cluster page to confirm. And when the distributed cluster mode is running properly, you can access the Controller through any node.



For more instructions and related FAQs, refer to How to Configure Distributed Cluster Mode on Linux Controller.