AOS-CX 10.10.1120 Release Notes

6300, 6400 Switch Series

a Hewlett Packard Enterprise company

April 2024
Edition: 1

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Products Supported

This release applies to the 6300 and 6400 Switch Series. The following table lists any applicable minimum software versions required for that model of switch.

If your product is not listed in the below table, no minimum software version is required.

Product number	Product name	Minimum software version
S0E91A	HPE Aruba Networking 6300M 48p SR10 1G/2.5G/5G/10G PTP/AVB Class8 PoE and 4p 100G MACsec Switch	10.13.1000
S0X44A	HPE Aruba Networking 6300M 48p SR10 1G/2.5G/5G/10G PTP/AVB Class8 PoE 4p 100G MACsec TAA Switch	10.13.1000
R8S89A	Aruba 6300M 24p SR10 10Gbase-T, PTP/AVB, 60W Class6 PoE with 2 x 50G and 2 x 25G MACsec Switch	10.10.0002
R8S90A	Aruba 6300M 48p SR5 (up to 5G), PTP/AVB, 90W Class 8 PoE with 2 x 50G and 2 x 25G MACsec Switch	10.10.0002
R8S91A	Aruba 6300M 48p SR5 (up to 5G) 60W Class6 PoE with 12p 90W Class 8 PoE with 2x 50G and 2x10G LRM/MACsec Switch	10.10.0002
R8S92A	Aruba 6300M 24p SFP+ 10G LRM support and 2 x 50G and 2 x 25G MACsec Switch	10.10.0002
JL658A	Aruba 6300M 24-port SFP+ and 4-port SFP56 Switch	10.04.3000
JL659A	Aruba 6300M 48-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 Switch	10.04.3000
JL660A	Aruba 6300M 24-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 Switch	10.04.3000
JL661A	Aruba 6300M 48-port 1GbE Class 4 PoE and 4-port SFP56 Switch	10.04.3000
JL662A	Aruba 6300M 24-port 1GbE Class 4 PoE and 4-port SFP56 Switch	10.04.3000
JL663A	Aruba 6300M 48-port 1GbE and 4-port SFP56 Switch	10.04.3000
JL664A	Aruba 6300M 24-port 1GbE and 4-port SFP56 Switch	10.04.0001
JL762A	Aruba 6300M 48-port 1GbE and 4-port SFP56 Power-to-Port 2 Fan Trays 1 PSU Bundle	10.04.3000

Product number	Product name	Minimum software version
JL665A	Aruba 6300F 48-port 1GbE Class 4 PoE and 4-port SFP56 Switch	10.04.0001
JL666A	Aruba 6300F 24-port 1GbE Class 4 PoE and 4-port SFP56 Switch	10.04.0001
JL667A	Aruba 6300F 48-port 1GbE and 4-port SFP56 Switch	10.04.0001
JL668A	Aruba 6300F 24-port 1GbE and 4-port SFP56 Switch	10.04.0001
R0X31A	Aruba 6400 Management Module	10.04.1000
R0X38B	Aruba 6400 48-port 1GbE Class 4 PoE Module	10.04.1000
R0X38C	Aruba 6400 48-port 1GbE Class 4 PoE v2 Module	10.09.1000
R0X39B	Aruba 6400 48-port 1GbE Class 4 PoE and 4-port SFP56 Module	10.04.1000
R0X39C	Aruba 6400 48-port 1GbE Class 4 PoE and 4-port SFP56 v2 Module	10.09.1000
R0X40B	Aruba 6400 48-port 1GbE Class 6 PoE and 4-port SFP56 Module	10.04.1000
R0X40C	ruba 6400 48-port 1GbE Class 6 PoE and 4-port SFP56 v2 Module	10.09.1000
R0X41A	Aruba 6400 48-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 Module	10.04.1000
R0X41C	Aruba 6400 48-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 v2 Module	10.09.1000
R0X42A	Aruba 6400 24-port 10Gbase-T and 4-port SFP56 Module	10.04.1000
R0X42C	R0X42C Aruba 6400 24-port 10Gbase-T and 4-port SFP56 v2 Module	10.09.1000
R0X43A	Aruba 6400 24-port SFP+ and 4-port SFP56 Module	10.04.1000
R0X43C	Aruba 6400 24-port SFP+ and 4-port SFP56 v2 Module	10.09.1000
R0X44A	Aruba 6400 48-port 10/25GbE SFP28 Module	10.04.2000
R0X44C	Aruba 6400 48-port 1G/10G/25GbE SFP28 v2 Extended Tables Module	10.09.1000
R0X45A	Aruba 6400 12-port 40/100GbE QSFP28 Module	10.04.2000
R0X45C	Aruba 6400 12-port 40/100GbE QSFP28 v2 Extended Tables Module	10.09.1000
R0X26A	Aruba 6405 Switch	10.05.0021
R0X27A	Aruba 6410 Switch	10.05.0001
JL741A	Aruba 6410 96-port 1GbE Class PoE 4 and 4-port SFP56 Switch	10.05.0001

Important information for 6300 and 6400 Switches

Aruba switches covered by this release note use eMMC or SSD storage. This is non-volatile memory for persistent storage of config, files, databases, scripts, and so forth. Aruba recommends updating to version 10.05.0060 or 10.06.0100 or later (including this release) to implement significant improvements to memory usage and prolong the life of the switch.

Starting from AOS-CX 10.10.1090, switches will only support TLSv1.2 ciphers and curves approved by the NIAP on all supported applications such as Secure RADIUS (RadSec), Captive Portal, and EAP-TLS clients. It is advised to upgrade your Secure RADIUS server to a version that supports the NIAP approved ciphers and curves and disable the unsupported ciphers from your EAP-TLS clients. NIAP approved ciphers and curves are DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, secp521r1, secp384r1, and prime256v1.

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Diffie-Helman algorithm is no longer enabled by default for key exchange. To enable using Diffie-Helman for key exchange, use the command `ssh key-exchange-algorithms <KEY-EXCHANGE-ALGORITHM-LIST>`."

Switch fans will run at full speed when a fault is detected with the temperature sensors in the switch. This is normal behavior to ensure overheating does not occur. Should the fans run at full speed at unexpected times, check the output of `show environment temperature` and `show environment fans`, then contact support for further assistance.

AOS-CX BGP implementations support resolving a BGP route's nexthop to a default route (0.0.0.0/0). However, this is not generally recommended in network deployments. Considering the default route to be the last resort route, resolving the BGP route's nexthop to a default route can cause potential routing loops in the network, if they are not properly designed and monitored. Route flaps and/or traffic drops may be observed in such cases.

In a future release, AOS-CX will not support the BGP route's nexthop resolving to a default route in the Route table. To avoid this problem and to be prepared for the update, Aruba recommends configuring a more specific static route (or host route) for BGP nexthops that are multihops away that are resolving via the default route.

If using the Web UI, you should clear the browser cache after upgrading to this version of software before logging into the switch using a Web UI session. This will ensure the Web UI session downloads the latest changes. Do not upgrade to 10.11 using REST API or WebUI unless your switch is running 10.09.1060, 10.10.1020 or later versions of these releases.

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software.
To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where <*VLAN_ID*> is the native VLAN ID configured on the trunk interface.
If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

If the switch has the always-on PoE feature enabled, during the upgrade from a version of software prior to 10.05.0001 to this version of software, PoE Powered Devices (PDs) will lose power from the switch as the switch will power cycle during the update. Plan a time for upgrading the switch when loss of power to the PDs attached to the switch can be mitigated.

To restore a previous configuration when downgrading to a previous version of software, follow these steps:

1. Use the `show checkpoint` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the `Image Version` column in the output of the command, for example FL.10.0*x*.*yyyy*).

   

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.
2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

To upgrade to:	Your switch must be running this version or later ***
AOS-CX 10.10.xxxx Note: 10.10 is an LSR, recommended release is 10.10.10xx.	AOS-CX 10.06.0110
AOS-CX 10.09.xxxx Note: 10.09 is an SSR, recommended release is 10.09.10xx.	AOS-CX 10.06.0110
AOS-CX 10.08.xxxx Note: 10.08 is an SSR, recommended release is 10.09.10xx.	AOS-CX 10.05.0001
AOS-CX 10.07.xxxx Note: 10.07 is an SSR, recommended release is 10.09.10xx.	AOS-CX 10.04.0001

To upgrade to:	Your switch must be running this version or later ***
AOS-CX 10.06.xxxx Note: 10.06 is an LSR, recommended release is 10.06.10xx.	AOS-CX 10.03.0001

*** *Note that all switch models may not support this minimum upgrade version.*

Refer to the Approved Product Lists sites for the Common Criteria, FIPS 140-2 and DoDIN APL to obtain the product certification details. Products should be used as evaluated and defined in the respective configuration guides.

- Common Criteria: https://www.niap-ccevs.org/Product/
- FIPS 140-2: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search
- DoDIN APL: https://aplits.disa.mil/processAPList.action

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

```
Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
U.S.A.
```

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at: https://hpe.com/software/opensource

Version history

All released versions are fully supported by Aruba, unless noted in the table.

Version number	Release date	Remarks
10.10.1120	2024-04-09	Released, fully supported, and posted on the Web.
10.10.1111	2024-03-14	Released, fully supported, and posted on the Web.
10.10.1110	2024-02-22	Released, fully supported, and posted on the Web.
10.10.1100	2023-12-12	Released, fully supported, and posted on the Web.
10.10.1090	2023-10-05	Released, fully supported, and posted on the Web.

Version number	Release date	Remarks
10.10.1080	2023-08-10	Released, fully supported, and posted on the Web.
10.10.1071	2023-07-20	Released, fully supported, and posted on the Web.
10.10.1070	2023-06-21	Released, fully supported, and posted on the Web.
10.10.1060	2023-05-04	Released, fully supported, and posted on the Web.
10.10.1050	2023-03-17	Released, fully supported, and posted on the Web.
10.10.1040	2023-02-08	Released, fully supported, and posted on the Web.
10.10.1030	2022-12-08	Released, fully supported, and posted on the Web.
10.10.1020	2022-11-07	Released, fully supported, and posted on the Web.
10.10.1010	2022-09-22	Released, fully supported, and posted on the Web.
10.10.1000	2022-08-14	Released, fully supported, and posted on the Web.
10.10.0002	2022-06-21	Initial release of AOS-CX 10.10. Released, fully supported, and posted on the Web.

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	56
Safari (MacOS)	12
Safari (iOS)	10 (Version 12 is not supported)

Internet Explorer is not supported.

Recommended versions of network management software for switches found in this release note:

Management software	Recommended version(s)
AirWave	8.2.15.1(R8Sxxx SKUs for 6300M Switches not supported)
NetEdit	2.10.0
Aruba Fabric Composer	6.2.0

Management software	Recommended version(s)
Aruba CX Mobile App	2.7.9 (or later)
Aruba Central	2.5.5
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40
IMC	7.3 (E0706P11) 6410 Switch Series not supported

NOTE

For more information, see the respective software manuals.

NOTE

To upgrade software using NetEdit, make sure to upgrade to the above version of NetEdit first and then execute the switch software upgrade on devices discovered by this version of NetEdit.

Enhancements

This section describes the enhancements introduced in this release.

Category	Description
AAA	(For 6300 Switch Series Only) RADIUS command authorization support is achieved in AOS-CX by sending the Aruba-Admin-Role VSA along with the RADIUS ACCEPT packet during RADIUS authentication. The Aruba-Admin-Role holds the user-group for the user and hence, it should be configured in the switch. For example, if a RADIUS ACCEPT packet is received with the Aruba-Admin-Role VSA with value **grp1**, the user-group **grp1** should be configured in switch.

Fixes

This section lists released builds that include fixes found in this branch of the software. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

For a list of issues resolved in the previous releases of 6300 and 6400 switches, refer to the AOS-CX Release Notes Portal.

NOTE

The Bug ID is used for tracking purposes.

Resolved Issues

This topic describes the resolved issues in this release.

Category	Bug ID	Description
Diagnostics	279303	(For 6300 Switch series only) **Symptom:** Cable diagnostic test incorrectly reports cables as faulty. **Scenario:** The cable diagnostic test will show the output pairs as open.
Port Access	290068	**Symptom:** The port-accessd process crashes unexpectedly. **Scenario:** This issue occurs when clients are frequently moved between ports on the same switch. **Workaround:** Do not frequently move clients between ports on the same switch.
Interface Persona	291435	**Symptom:** The interface persona is brought down when it is configured using the **aaa authentication port-access dot1x authenticator enable** or **aaa authentication port-access mac-auth enable** commands, and while attaching the same to a physical interface. **Scenario:** This issue occurs when the interface persona is configured with the **aaa authentication port-access dot1x authenticator enable** or **aaa authentication port-access mac-auth enable** commands. **Workaround:** Do not configure the interface persona using the **aaa authentication port-access dot1x authenticator enable** or **aaa authentication port-access mac-auth enable** commands.
VSX	291905	**Symptom:** Packet drop is observed and packets are not redirected to the other VSX member if the ISL LAG is reconfigured while the local MCLAG is down. **Scenario:** If the local MCLAG port on a VSX member is down and the MCLAG on the other VSX member is up, then traffic should be redirected over ISL to the VSX partner. If the ISL LAG is reconfigured, the redirection will fail, causing packets headed toward that MCLAG to be dropped. **Workaround:** Remove and re-configure the ISL LAG and assign port membership before setting the LAG as ISL.
IGMP/MLD	292078	**Symptom:** The event message, Event ID 2628: "**IGMP/MLD internal queue limit exceeded. Needs admin intervention**" is logged multiple times. **Scenario:** This issue is observed in VXLAN overlay networks that do not have any multicast configuration. **Workaround:** Enable IGMP snooping on each VLAN carried in the overlay on all switches acting as VTEPs. Alternatively, use the **logging filter** command to deny log messages with the Event ID 2628.
Link Aggregation	294783	(For 6400 Switch series only) **Symptom:** LACP remains in blocked state after a few changes in the line module configuration. **Scenario:** This behavior can be observed in rare circumstances where a user issues **no module** command on a line card slot and immediately issues a configuration command for the same line card. **Workaround:** Allow some time for the configuration changes to be applied before configuring further changes.
Captive Portal Using Aruba CPPM	296004	**Symptom:** The chrome browser displays an error message, **404: page not found**. **Scenario:** This issue is observed in a captive portal profile when multiple clients access the login page at the same time using the Chrome browser. **Workaround:** Refresh the web page.
Port Access	297755	**Symptom:** Traffic to existing clients on a VLAN drops if a new client with the MAC address of a DUT system onboards an authentication enabled port. **Scenario:** This issue is observed when a packet with a MAC address which is same as the MAC address of a DUT system is received on the authentication enabled port. **Workaround:** Shut down and re-enable the VLAN interface to resume traffic flow

Category	Bug ID	Description
		for the clients.
VSX Sync	299838	**Symptom:** The interface VLAN configuration did not synchronize on the secondary switch. **Scenario:** This issue is observed in a pair of switches where the user configures an interface VLAN with **vsx-sync** configuration on the primary VSX and then creates the same interface VLAN on the secondary switch. **Workaround:** When **vsx-sync** is enabled on the interface VLAN of the primary VSX member, it is recommended to wait for at least 15 seconds before configuring the same on the secondary switch. Alternatively, configure the interface VLAN on the secondary switch and then enable **vsx-syn**c on the primary switch.

User Based Tunnel	300802	**Symptom:** UBT clients connected to the newly replaced backup controller are unable to receive the IP address.
		Scenario: This issue occurs when a newly replaced controller has the same IP address of the old controller in the cluster and has been assigned the role of a leader.
		Workaround: Remove the UBT configuration using the **no ubt** command and add the UBT configuration again using the following commands:
		`switch(config) # ubt zone <zone name> vrf <vrf name>`
		`switch(config-ubt-<zone name>)# primary-controller ip <IP address>`
		`switch(config-ubt-<zone name>)# backup-controller ip <IP address>`
		`switch(config-ubt-<zone name>)# enable`

Feature caveats

The following are feature caveats that should be taken into consideration when using this version of the software.

Feature	Description
User Based Tunnel	In the event of of license issues when onboarding an DUT to primary or backup mobility conductor, the DUT will not try to bootstrap to other mobility conductor where a license is available. For example, a if mobility conductor ▪ does not have a have license to on-board the DUT but mobility conductor. ▪ does have adequate licenses, if both mobility conductors are reachable then UBT will be down, and the DUT will not attempt to bootstrap to the backup controller. However, if the primary mobility conductor is not reachable, the DUT gets tunneled to the standby/backup mobility conductor. Once the primary mobility conductor reachable by the DUT once again, the DUT will not automatically bootstrap back to the primary. Network administrators should manually disable and enable UBT on the DUT to re-establish the tunnel to the primary mobility conductor.
IP-SLA	Reserved ports or ports used by other applications/services within the system are not recommended to be used for other services. When two services use the same port, users might observe some unexpected behaviors from these services. The best practice is to use unique port for each service across the system.

Feature	Description
SNMP	The traps from the **hpe-routing, hpe-vsxd, hpe-cardd, SNMP, hpe-config, hpe-vrrpd, intfd, fand, tempd, hpe-eventlog,** and **powerd** daemons have been migrated to the New-Trap infra and will have the correct PDU type in the SNMPv1 traps. All the other daemons will have the PDU set to coldstart.
EVPN	Next-hop-self is not supported for EVPN on an RR+VTEP device. As a workaround, issue the **route-map** command, then use the commands **set ip nexthop** and set **extcommunity router-mac**.
BGP	If a route-map is applied and none of the routes satisfy the match condition(s) in any of the route-map entries, then all routes are dropped.
TFTP	Blocksize greater than 1480 is not supported in 4100i, 6100 and 6000 Switch series.
VRRP	The same virtual link-local address cannot be used across different VRFs.
VRRP	MD5 authentication interoperation is not supported with Comware-based switches
REST	Boundary values for **match vni** and **set local preference** in a route-map system cannot be set via the REST API and must be manually configured on the switch via the CLI.
ACLs	**NOTE:** Applies only to the Aruba 6300 Switch Series. In a VSF stack, the switch may fail to log events for the matching access-list entries. ACL functionality is not impacted; access-list entries are applied properly and only the logging is incorrectly generated.
Aruba CX Mobile App	VSF stack formation is blocked when there are reserved autojoin interfaces (25, 26, 49, 50) in the stack topology.

BGP	In multi-VRF environments, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch will install both routes as ECMP instead of preferring the leaked route. Use route-maps to give lower/higher preference to the routes received from an iBGP peer. For example:
	`!`
	`route-map rmap permit seq 10`
	`  set local-preference 50`
	`!`
	`router bgp 100`
	`  vrf red`
	`  neighbor 1.1.1.2 remote-as 100`
	`  address-family ipv4 unicast`
	`  neighbor 1.1.1.2 activate`
	`  neighbor 1.1.1.2 route-map rmap in`
	`  exit-address-family`
	In the above example, since a lower value of local-preference (i.e. 50, whereas default value is 100) has been set to the routes received from iBGP peer, the leaked routes get preferred and get installed as best routes.

DHCP Server DHCP Relay DHCP Snooping	Note the following caveats for these features: ▪ DHCP Relay and DHCP Snooping can co-exist on the same switch. DHCP

Feature	Description
	Snooping and DHCP Server cannot co-exist on the same switch. ■ DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.

BGP	The **next-hop-unchanged** option needs to be explicitly configured to preserve nexthop while advertising routes to eBGP peers, in the L2VPN EVPN address-family. For example:
	`router bgp 1`
	`neighbor 1.1.1.1 remote-as 2`
	`address-family l2vpn evpn`
	`neighbor 1.1.1.1 activate`
	`neighbor 1.1.1.1 next-hop-unchanged`
	`neighbor 1.1.1.1 send-community extended`
	`exit-address-family`
	`!`

Classifiers	For Classifier policy modifications to be secure, Aruba strongly encourages modifications be done as a three-step process: Bring down the port, modify, and bring the port back up.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	Automatic downgrade of the startup–config is not supported during a software downgrade.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters (6400 only)	Bytes/errors/drops count in **show interface <*IF-NAME*>** and **show interface <*IF-NAME*>** queues can have up to 10% deviation. This will manifest mainly when running at line rate with small packet sizes and after a port goes up/down.
EVPN	iBGP split-horizon rule is not followed between different address families. Use route-map to block the routes getting advertised to the iBGP peer.
Flow control (6400 only)	Flow control is not supported.
ICMP Redirect	The switch may only software forward an 100pps IP frame that triggers ICMP redirect.
Line module Hot Swap and Reboot (6400 only)	Concurrent physical hot insert/removal or reboot of a line-module is not supported. Subsequent insert/removal or reboot of a line-module must be initiated only after preceding attempts have been completely processed by the system. For hot insert you must wait until the preceding line-module has reached the "ready" state before inserting subsequent line-modules. For hot removal you must wait until the line-module is no longer present in the system. See the CLI command **show module** for line-module status information. Aruba recommends line-modules be gracefully shut down before removal. Use the CLI config command **module <*SLOT-ID*> admin-state [diagnostic | down | up]** to change the administrative state of the line-module. Line module reboot and hot removal is not a hitless operation. Up to 2 seconds of traffic loss may be expected when any module is rebooted or removed from the system. Hot insert does not result in any traffic loss.

Feature	Description
MACsec	In an environment with a Cisco device, the Cisco device must be designated as the key server. Designating the AOS-CX as the key server results in complete traffic loss.
MACsec	In an environment with Cisco and FlexFabric or H3C devices, do not update confidentiality-offset on the live channel. There can be complete traffic loss for an extended period on the MACsec channel when confidentiality-offset is updated on both ends. When deriving the connectivity association key (CAK) from an EAP-TLS session, AOS-CX always derives a 32-byte CAK. This is true for both the authenticator and supplicant. But during the interop tests with Cisco devices/software (AnyConnect), it is observed that the derived CAK is only 16 bytes in length. To enable interop with devices that generate a 16 byte CAK for EAP-TLS MACsec, a new configuration is added to allow the user to select the size of the CAK to generate for both authenticator and supplicant.
MACsec	MACsec uses a software-based implementation to track start and stop times for secure channels and secure associations. As the implementation is software-based, the stop times for MACsec secure channel and secure associations are only updated when they are deleted and therefore never updated in the output of the **show macsec status detailed** command. When a 802.1X supplicant transmits an EAPoL frame, it uses the MAC address of the interface on which the supplicant is running as the source MAC in EAPoL frames. But there are certain vendors (for example, Cisco), when running as 802.1X authenticator do not support the use of EAP MACsec in **device-mode**, that is, the client being authenticated is an infrastructure device that must be profiled in **client-mode** to be able to use EAP MACsec over that channel. Since an AOS-CX supplicant uses the interface MAC address in 802.1X EAPoL frames by default, after authentication and MKA, any packet sourced from the switch or routed from the switch will be dropped by the peer since the MAC in such frames is the system MAC and not the interface MAC which is authenticated on the peer. A new configuration inside the 802.1X supplicant policy allows a user to configure the MAC address to use for EAPoL frames based on deployment needs. The supported options are a. Interface MAC (Default) b. System MAC
MACsec and UDLD	In an environment with devices running AOS-Switch, do not enable UDLD on the same link. The UDLD session can toggle between up and down continuously when both MACsec and UDLD is enabled on the same link.
MACsec	In an environment with Cisco devices, when the GCM-AES-XPN-128 or GCM-AES-XPN-256 cipher suite is used for establishing the MACsec channel, the MKA policy on the Cisco device must be configured with **ssci-based-on-sci**.
Multicast and VXLAN	▪ VXLAN must be configured prior to configuring VSX. ▪ IPv6 multicast is not supported for VXLAN overlay. ▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details.
Priority queues (6400 only)	A maximum of four (4) priority queues is supported.
RADIUS	Authorization by means of HPE VSAs is not supported.

Feature	Description
Reduction in TCAM entries (6400 only)	On some line cards, a small number (~200) of TCAM entries are used for internal purposes.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RIP/RIPng	RIP/RIPng metric configuration support is not available.
SFTP	When the path to the SFTP server crosses segments with different MTU frame sizes, file transfers will fail. Configure the same MTU on all nework segments on the path to the SFTP server to use SFTP to transfer files.
Sub-interface	BFD is not supported on a sub-interface. A sub-interface as underlay for EVPN-VXLAN is not supported
Tunnels	When configuring tunnels (VXLAN/IP tunnels) with the underlay as a static route, the next-hop IP should be an SVI or ROP IP and not configured as the Active-Gateway.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.

Known Issues

The following are known open issues with this branch of the software. The **Symptom** statement describes what a user might experience if this is seen on the network. The **Scenario** statement provides environment details and trigger summaries. When available, the **Workaround** statement provides a workaround to the issue.

Category	Bug ID	Description
L3 Routes	207077	**Symptom**: Traffic convergence takes approximately two minutes when VSF switchover is performed. **Scenario**: This issue occurs when traffic is flowing through the switch using the uplink on the conductor. Performing a VSF switchover causes the standby to become the new conductor, and it takes approximately 2 minutes for traffic to resume using the uplink of the new conductor. **Workaround**: If the Uplink from the VSF is a LAG with members in Conductor/Standby/Member, the convergence time would be lesser and around 70 seconds.
CLI Infra	211466	**Symptom**: The user session does not timeout. **Scenario**: When the switch console is left idle, with a CLI command output in progress, waiting for user input to display the next page, the user session does not timeout when the configured timer expires. **Workaround**: The session idle timeout counts when CLI command is completed and the switch is idle at the switch prompt.
GRE Tunnels	279874	**Symptom:** BGP sessions go down. **Scenario:** This issue occurs after traffic is sent over two tunnels. However, BGP session does not go down if there's no traffic.

Upgrade information

AOS-CX 10.10.1120 uses ServiceOS FL.01.11.0001

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software.
To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

NOTE

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where <*VLAN_ID*> is the native VLAN ID configured on the trunk interface.
If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

CAUTION

Each VSX switch in a pair must run the same version of AOS-CX. If a primary VSX switch is upgraded to 10.10.xxxx, the secondary VSX switch must be immediately upgraded to that same version. If the ISL link is disabled and enabled on VSX switches that are running different versions of AOS-CX, a VSX secondary switch running an older version of AOS-CX may be unable to synch information from the VSX primary, which can cause the port state to become blocked and lead to traffic loss.

NOTE

Do not interrupt power to the switch during this important update.

Due to an image size issue, a one-step upgrade from some versions of AOS-CX using the WebUI is not supported. This limitation only affects upgrades performed using the switch WebUI, and does not impact upgrades performed using the command-line interface or Aruba Central.

Upgrades requiring two steps:

Original Release	Intermediate Upgrade Release	Final Upgrade Release
10.08.xxxx	▪ 10.09.1060 or later 10.09.xxxx release ▪ 10.10.1020 or later 10.10.xxxx release	10.10.1020 or later 10.10.xxxx release
10.09.0001 - 10.09.1050	▪ 10.09.1060 or later 10.09.xxxx release ▪ 10.10.1020 or later 10.10.xxxx release	10.10.1020 or later 10.10.xxxx release

Upgrades requiring one step:

Original Release	Final Upgrade Release
10.09.1060 or later 10.09.xxxx release	10.10.1020 or later 10.10.xxxx release
10.10.1020 or later 10.10.xxxx release	10.10.1020 or later 10.10.xxxx release

Some Network Analytics Engine (NAE) scripts may not function properly after an upgrade. Aruba recommends deleting existing NAE scripts before an upgrade and then reinstalling the scripts after the upgrade. For more information, see the *Network Analytics Engine Guide*.

For 6400 only: To execute an In Service Software Upgrade (ISSU) to your switch must be running one of the following supported releases:

From	Supported Versions for Upgrade
10.10.0002	10.10.1000 or later versions
10.10.1000	10.10.1010 or later versions
10.10.1010	10.10.1020 or later versions
10.10.1020	10.10.1030 or later versions
10.10.1030	10.10.1040 or later versions
10.10.1040	10.10.1050 or later versions
10.10.1050	10.10.1060 or later versions
10.10.1060	10.10.1070 or later versions
10.10.1070	10.10.1080 or later versions
10.10.1080	10.10.1082 or later versions
10.10.1082	10.10.1090 or later versions
10.10.1090	10.10.1100 or later versions
10.10.1100	10.10.1110 or later versions
10.10.1110	10.10.1120

Manual configuration restore for software downgrade

To restore a previous configuration when downgrading to a previous version of software, follow these steps:

1. Use the **show checkpoint** command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version. (See the **Image Version** column in the output of the command, for example, FL.10.10.*yyyy*)

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.

2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

Performing the upgrade

For additional upgrade and downgrade scenarios, including limitations of automatic upgrade and downgrade scenarios provided by the Configuration Migration Framework (CMF), refer to the **AOS-CX 10.10 Fundamentals Guide**.

CAUTION

This version may contain a change of BootROM from the current running version. A BootROM update is a non-failsafe update. Do not interrupt power to the switch during the update process or the update could permanently damage the device.

1. Copy the new image into the non-current boot bank on the switch using your preferred method.
2. Depending on the version being updated, there may be device component updates needed. Preview any devices updates needed using the `boot system <BOOT-BANK>` command and entering `n` when asked to continue.

   For example, if you copied the new image to the secondary boot bank and no device component updates are needed, you will see this:

```
switch# boot system secondary
Default boot image set to secondary.
Checking if the configuration needs to be saved...

Checking for updates needed to programmable devices...
Done checking for updates.

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? n
```

   In this example, three device updates will be made upon reboot, one of which is a non-failsafe device:

```
switch# boot system secondary
Default boot image set to secondary.
Checking if the configuration needs to be saved...
```

```
Checking for updates needed to programmable devices...
Done checking for updates.

2 device(s) need to be updated during the boot process.
The estimated update time is between 2 and 3 minute(s).
There may be multiple reboots during the update process.

1 non-failsafe device(s) also need to be updated.
Please run the 'allow-unsafe-updates' command to enable these updates.

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? n
```

3. When ready to update the system, if a non-failsafe device update is needed, make sure the system will not have any power interruption during the process. Invoke the `allow unsafe updates` command to allow updates to proceed after a switch reboot. Proceed to step 4 within the configured time.

```
switch# config
switch(config)# allow-unsafe-updates 30

This command will enable non-failsafe updates of programmable devices for
the next 30 minutes.  You will first need to wait for all line and fabric
modules to reach the ready state, and then reboot the switch to begin
applying any needed updates.  Ensure that the switch will not lose power,
be rebooted again, or have any modules removed until all updates have
finished and all line and fabric modules have returned to the ready state.

WARNING: Interrupting these updates may make the product unusable!

Continue (y/n)? y

    Unsafe updates      : allowed (less than 30 minute(s) remaining)
```

4. Use the `boot system <BOOT-BANK>` command to initiate the upgrade. On the switch console port an output similar to the following will be displayed as various components are being updated:

```
switch# boot system secondary
Default boot image set to secondary.
Checking if the configuration needs to be saved...

Checking for updates needed to programmable devices...
Done checking for updates.

3 device(s) need to be updated during the boot process.
The estimated update time is between 2 and 3 minute(s).
There may be multiple reboots during the update process.


This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.

Looking for SVOS.
```

```
Primary SVOS:  Checking...Loading...Finding...Verifying...Booting...

ServiceOS Information:
    Version:          <serviceOS_number>
    Build Date:       yyyy-mm-dd hh:mm:ss PDT
    Build ID:         ServiceOS:<serviceOS_number>:
6303a2a501ba:202006171659
    SHA:              6303a2a501bad91100d9e71780813c59f19c12fe

Boot Profiles:

0. Service OS Console
1. Primary Software Image [xx.10.10.1030]
2. Secondary Software Image [xx.10.10.1040]

Select profile(secondary):

ISP configuration:
    Auto updates        : enabled
    Version comparisons : match (upgrade or downgrade)
    Unsafe updates      : allowed (less than 29 minute(s) remaining)

Advanced:
    Config path         : /fs/nos/isp/config [DEFAULT]
    Log-file path       : /fs/logs/isp [DEFAULT]
    Write-protection    : disabled [DEFAULT]
    Package selection   : 0 [DEFAULT]

3 device(s) need to be updated by the ServiceOS during the boot process.
The estimated update time by the ServiceOS is 2 minute(s).
There may be multiple reboots during the update process.


MODULE 'mc' DEVICE 'svos_primary' :
    Current version  : '<serviceOS_number>'
    Write-protected  : NO
    Packaged version : '<version>'
    Package name     : '<svos_package_name>'
    Image filename   : '<filename>.svos'
    Image timestamp  : 'Day Mon dd hh:mm:ss yyyy'
    Image size       : 22248723
    Version upgrade needed

Starting update...

Writing...    Done.
Erasing...    Done.
Reading...    Done.
Verifying...  Done.
Reading...    Done.
Verifying...  Done.


Update successful (0.5 seconds).

reboot: Restarting system
```

Multiple components may be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

```
 (C) Copyright 2017-2022 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
 Confidential computer software. Valid license from Hewlett Packard Enterprise
 Development LP required for possession, use or copying. Consistent with FAR
 12.211 and 12.212, Commercial Computer Software, Computer Software
 Documentation, and Technical Data for Commercial Items are licensed to the
 U.S. Government under vendor's standard commercial license.

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at: https://asp.arubanetworks.com

switch login:
```

Aruba recommends waiting until all upgrades have completed before making any configuration changes.

Chapter 2
Other resources

Aruba is committed to ensuring you have the resources you need to be successful. Check out these learning and documentation resources:

- AOS-CX switch software documentation portal: https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
- AOS-CX 10.10 playlist of technical training videos on YouTube: https://www.youtube.com/playlist?list=PLsYGHuNuBZcZmHTZQC9LuivtrVecOx5vk

Chapter 3
Aruba security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/security-bulletins/. You can sign up at https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com to initiate a subscription to receive future Aruba Security Bulletin alerts via email.