AOS-CX 10.12.1020 Release Notes

6300 and 6400 Switch Series

a Hewlett Packard
Enterprise company

December 2023

Edition: 1

Copyright Information

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components 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, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.

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.

Chapter 1
AOS-CX 10.12.1020 release notes

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.

NOTE

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

Product number	Product name	Minimum software version
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
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

Product number	Product name	Minimum software version
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 10.06.0100 or later (including this release) to implement significant improvements to memory usage and prolong the life of the switch.

Starting from AOS-CX 10.12.1010, 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.

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.

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 10.11.0001, the command **route recursive-lookup default-route** has been introduced under the **vrf** context to support BGP route's nexthop resolving to a default route in the Route table. This command is enabled by default.

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.

NOTE

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.

NOTE

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.

For information about Short Supported Releases (SSRs) and Long Supported Releases (LSRs), see https://www.arubanetworks.com/support-services/end-of-life/arubaos-software-release/.

To upgrade to:	Your switch must be running this version or later:
AOS-CX 10.12.xxxx Note: 10.12 is an SSR, recommended release is 10.12.0006	AOS-CX 10.09.0002
AOS-CX 10.11.xxxx Note: 10.11 is an SSR, recommended release is 10.11.0001	AOS-CX 10.08.0001
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

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
10.12.1020	12-12-2023	Released, fully supported, and posted on the Web.
10.12.1010	05-10-2023	Released, fully supported, and posted on the Web.
10.12.1000	02-08-2023	Released, fully supported, and posted on the Web.
10.12.0006	31-05-2023	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)
NetEdit	2.8.0
Aruba Central	2.5.7
Central On-Premises	2.5.6.4
Aruba Fabric Composer	6.5.2
Aruba CX Mobile App	Support coming in future release.
IMC	(708P03) 6410 Switch Series not supported

For more information, see the respective software manuals.

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

PKI	In previous releases, under a certificate configuration context, the key-size or curve-size is a mandatory keyword following a key-type, even when the key-size to configure is the default value. For example:
	`(config-cert01)# key-type rsa key-size 2048`
	`(config-cert01)# key-type ecdsa curve-size 256`
	Starting with AOS-CX 10.12.1020, when the key-curve-size to configure is the default value, the key-size/curve-size keyword is optional and may be omitted. For example, this command
	`(config-cert01)# key-type ecdsa`
	Is equivalent to:
	`(config-cert01)# key-type ecdsa curve-size 256`
	And this command:

Category	Description

	`(config-cert01)# key-type rsa`
	Is equivalent to:
	`(config-cert01)# key-type rsa key-size 2048`

Boot Process	Enhancements in this release allow the switches to display more detailed information about the reason for reboots.

Physical Interfaces	This version of AOS-CX allows you to configure the leader-follower mode for 1000BASE-T, 2.5GBASE-T, 5GBASE-T, and 10GBASE-T on Aruba CX 6300 Switch Series for products, JL659A & JL660A. The leader uses an external clock for generating its clock signals to determine the timing of the transmitter and receiver operations. The follower recovers its clock from the received signal from the leader and uses it to determine the timing of the transmitter operations. As a multiport device, the switch operates as the **preferred-leader** by default.
	NOTE: Configuring both the ends of the link to the same forced leader-follower role will result in the failure to link-up.
	Users can configure the following leader-follower modes for an interface:
	forced-follower: Forces the interface to be the follower.
	forced-leader: Forces the interface to be the leader.
	preferred-follower: Advertises preferences to be the follower.
	preferred-leader: Advertises preferences to be the leader
	The following example configures the preferred-follower mode:
	`switch(config)# interface 1/1/1`
	`switch(config-if)# leader-follower-mode preferred-follower`
	Applying this configuration on interfaces with different technologies like 100BASE-TX and 10BASE-T will have no effect.

Resolved Issues

This section lists fixes found in this branch of the software. The **Symptom** statement describes what a user might experience if this issue 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 chooses 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 section describes the issues resolved in this release.

Category	Bug ID	Description
PKI	283686	**Symptom**: When an X509 certificate profile configuration with an EST profile association is pushed to a switch, it can trigger the EST enrollment two times, causing the EST server to issue two certificates to the switch. **Scenario**: This issue has no functional impact, because only the latest enrolled certificate will take effect.
ASIC SDK -HPE	277504	**Symptom**: A VSF stack breaks apart and a stack member reboots. **Scenario**: This occurs if an invalid client is connected to a downlink or if a counterfeit transceiver is connected to the uplink. **Workaround**: Disable the problematic ports and reboot the switch.
DHCP Snooping	265609	**Symptom:** High CPU utilization is observed on VSX pairs when DHCP snooping is enabled. **Scenario:** When DHCP clients on a VSX move between VLANs/ports, CPU utilization goes up and DHCP services either stop working completely or perform slowly. **Workaround:** Reboot one of the VSX peers or restart the daemon to resolve the issue.
WebUI	279019	**Symptom:** After uploading an invalid PER certificate, the hpe-restd process becomes unstable, the WebUI temporarily stops responding, and all REST API calls from the WebUI fail. **Scenario:** If a user uploads a corrupt PEM certificate file using WebUI certificate management window, selecting the **Upload** button in the WebUI causes the WebUI to stop working completely. To recover from this state, restart hpe-restd from the bash prompt in the command-line interface or restart the switch. **Workaround:** Use the CLI to upload certificates.
SNMP	285540	**Symptom**: If both IPv4 and IPv6 neighbors are used while configuring BGP, the SNMP walk displays incorrect information about IPv4 peer sessions. **Scenario**: This issue occurs when the user configures both IPv4 and IPv6 neighbors. As a result, the SNMP walk displays information about non-existent IPv4 peers.
Central	279046	**Symptom**: A firmware upgrade from Aruba Central will fail. **Scenario**: This issue occurs when switch's connection to the internet is configured using the command **ip source-interface http** or **ip source-interface all**. **Workaround**: Configure the switch to connect to the internet without using an ip source interface.
WebUI	282016	*(For 6300 Switch Series only)* **Symptom**: The **Interface Edit** button on WebUI PoE interface page is disabled when the selected PoE interface's **power enable status** setting is disabled. **Scenario**: This issue occurs when a user accesses the WebUI's PoE Interface page on a PoE switch, edits the PoE configuration of an interface/port, sets the **Power Enable** option to **disabled**, then saves these settings. After this, the **Edit** button for this interface/port on WebUI will not be enabled to reconfigure this interface/port for any other PoE configuration. **Workaround**: Edit the PoE configuration of Interface/Port from the command-line interface or re-enable the **Power Enable** option for the Interface/Port from the CLI to reenable the **Edit** button again in the WebUI.
SNMP	281792	**Symptom**: A desired source IP address is not seen when inform packets are received by the inform receiver. **Scenario**: This issue occurs when a user sets a source IP address for traps.
RADsec	282524	**Symptom**: Client authentication is not successful after a VSF conductor reboot. **Scenario**: This issue occurs when a VSF conductor is rebooted or when the **port-**

Category	Bug ID	Description
		accessd daemon is restarted. **Workaround**: Reconfigure the RADIUS server.

Device-Profile	284093	**Symptom**: The **port-accessd** daemon crashes and generates the following log file message:
		`LOG_EMERG|CDTR|1|PORTACCESS|PORTACCESS_`
		`DEVICEPROFILE|Received a NULL pointer in one`
		`or more function`
		`arguments.`
		Scenario: The issue is observed when a device connected to the switch advertises LLDP information with a TLV value greater than 256 Bytes.

PKI	281380	**Symptom**: When a certificate is validated, the event log did not indicate what CA certificate was used to validate the certificate. A new event is added to this release to provide the CA certificate information. **Scenario**: This issue occurs when validating an Aruba Central server certificate.
PKI	262792	**Symptom**: The hep text for the **crypto pki certificate** command had an additional special character **)** in the default value. **Scenario**: Enter the certificate context to configure a X509 certificate and then type **shift+?** to see the help text.
REST	268051	**Symptom:** The error message, **Unknown string: Class8, valid strings are: class3, class4, class6** is displayed on some interfaces depending on its capability. **Scenario**: This issue occurs when the REST API is used to "Get" a class and Class-8 is obtained. If the returned value of Class-8 configured with 'PUT' function on interfaces which do not support class-8, the error message, **Unknown string: Class8, valid strings are: class3, class4, class6** is displayed. **Workaround:** Issue the **show power-over-ethernet <interface>** command to check the maximum class capability of the interface. Any class that is equal to or lower than the maximum class capability can be configured on the interface.

Physical Interfaces	272070	**Symptom:** Client devices link with the switch at a speed lower than the highest common advertised speed, or link at the highest common advertised speed and then downshift to a lower speed. This issue occurs when the link quality is sub-optimal and it is also possible to downshift from 5G to 100M.
		Scenario: Downshift is expected if there is a non-ideal cabling or high interference in the environment. However, for the products, JL659A and JL660A Smart Rate ports, some devices cause a downshift even when the cabling is good and there is no excessive noise in the environment.
		Workaround: The following workaround applies to the products, JL659A and JL660A, where the downshift is not caused by any environmental issue:
		Limit the speed at the switch can operate with the desired speed using the **speed auto <desired speed>** command in the interface context.
		Set the switch leader-follower mode to **leader-follower-mode preferred-follower** in the interface context.
		`switch(config)# interface 1/1/1`
		`switch(config-if)# leader-follower-mode preferred-`
		`follower`
		If ISSU is used to upgrade the switch, it is required to reboot the switch to configure the **leader-follower-mode** command.

Category	Bug ID	Description
Switch Profiles	288784	**Symptom:** Users who use ZTP for configuration download are unable to change device profiles using the configuration templates. **Scenario:** This issue occurs in a 6400v2 chassis where the user has a mix of both v1 and v2 line cards. This requires the chassis to be placed into the "default" profile setting and the switches must be rebooted and the current configurations must be cleared if the chassis needs be placed into the "default" profile setting. Currently, the safe guards that are in place do not allow the device to be rebooted when the configuration is applied from an unattended source like ZTP, Aruba Central, or NetEdit. This also prevents the device from changing the profile via any unattended configuration download. **Workaround:** Use the CLI to change the device profile.
Transceivers	288993	**Symptom:** Link flap is observed after PMD restart on a transceiver which is already in the final PMD state. **Scenario:** This issue occurs when PMD is restarted during VSF stack formation.
L3 Routes	276730	**Symptom:** After a VSF switchover, the BGP session established over GRE tunnels are stuck in the CONNECT state. **Scenario:** BGP's 3-way TCP handshake fails after a VSF switchover as the ping to the underlying GRE tunnel IP address starts to fail. Hence, the BGP session is stuck in the CONNECT state.

Feature Caveats

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

Feature	Description
L3 Addressing	IPv6 prefixes with a subnet mask between /65 to /127 will not be programmed if there is no other </64 route is programmed for the prefix (including the default). In regular routing scenarios packets are software forwarded, but with VxLAN overlay, the packets will be dropped. It is recommended to use a /128 prefix for a loopback used as an IPv6 VXLAN tunnel source.
REST	The REST v1 API that was deprecated in previous release of AOS-CX is completely deactivated and no longer available in AOS-CX 10.12. For more information on migrating your deployment from the RESTv1API to the RESTv10.xx API, refer to the REST API Migration Quick Start Guide.
REST	When a user configures a RADIUS server via REST with AOS-CX 10.11 or lower, the REST operation fails. A schema change introduced in the RADIUS_Server table in 10.12 is not backward compatible with REST versions 10.11 and lower. A checkpoint restore operation will fail on a switch running 10.12 firmware if the checkpoint is created on a 10.11 or lower release and includes RADIUS server configurations. Use REST version 10.12 to configure RADIUS servers on a switch running AOS-CX 10.12.xxxx. When using checkpoints with RADIUS server configurations, do not restore the checkpoint directly on a switch running 10.12 firmware. Instead, 1. Copy the running-config from the switch running the 10.11 or lower release firmware to a remote server as CLI commands (and not as a JSON file).

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td></td><td>2. Erase the startup-config on the switch.
3. Upgrade without saving the configuration to 10.12.xxxx.
4. Copy the running-config from the remote server, *or* apply the entire configuration from scratch on the switch running the 10.12 firmware.</td></tr>
<tr><td>PIM-SM</td><td>Pim Active-Active is not supported on overlay VXLAN SVIs.</td></tr>
<tr><td>SNMP</td><td>When SNMP is enabled via the switch CLI, it can take between 1-2 minutes for the SNMP daemon to be ready to respond to requests. If a local or external SNMP MIB walk is performed in the interval between when SNMP is first enabled and the SNMP daemon is ready, the MIB walk action will return an error.</td></tr>
<tr><td>Certificates</td><td>When a switch uses a certificate with a legacy certificate name that is not supported in 10.12 because it contains disallowed characters, the information will migrate properly in the upgrade, but that certificate can no longer be edited. For new certificate names, only alphanumeric characters, dots, dashes, and underscores are allowed.</td></tr>
<tr><td>REST</td><td>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.</td></tr>
<tr><td>ACLs</td><td>**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.</td></tr>
<tr><td>Aruba CX Mobile App</td><td>VSF stack formation is blocked when there are reserved autojoin interfaces (25, 26, 49, 50) in the stack topology.</td></tr>
<tr><td>BGP</td><td>In environments with VRRP or VSX peers, 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.</td></tr>
<tr><td>BGP</td><td>The **next-hop-unchanged** option needs to be explicitly configured to</td></tr>
</table>

Feature	Description

	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. To restore a configuration use the procedure documented in Manual configuration restore for 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.
Counters (6400 only)	The "Bytes" counter is not supported in **show interface *<IF-NAME>*** queues output.
EVPN	The 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 at a rate of 100pps if the packets that trigger ICMP redirect.
IGMP/PIM on 6-in-6, Loopback and GRE interfaces	IGMP cannot be enabled on either Loopback or GRE interfaces. IGMP and PIM is not supported on a 6-in-6 Tunnel.
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.

Feature	Description
	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.
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.
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.
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**.
MACsec	MACsec works between a CX device and a Windows VM running AnyConnect with AES-128 cipher. AnyConnect does not support AES-256 in the NAM module (works only for the VPN module).
MACsec	When Cisco AnyConnect is used as dot1x supplicant, it is recommended to configure cak-length to be 16 under dot1x-authenticator mode.
MACsec	Ensure the cipher suite **GCM-AES-128** is configured when AOS-CX is acting as a key server. This is because, by default AOS-CX will use the most secure cipher suite **gcm-aes-xpn-256** for establishing MACsec secure link and Comware/PVOS doesn’t support an XPN cipher suite.
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.
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+.

Feature	Description
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.
VRF	VRF names are limited to 31 characters.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
Traceroute	Traceroute v4/v6 over VXLAN fails to find intermediate next-hop IP information from a source VTEP in Virtual Active Gateway environment (the SVI is the same as theActive Gateway IP).
VRRP	VRRP Preemption Delay Timer (preempt delay minimum) may be ignored after a switch reboot or power cycle.
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.
PTP	*(6300 Switch Series only*) End clients offset might be slightly high when using PTP Default profile 1588v2 with default PTP parameters (1 PPS)

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 additional environment details and trigger summaries. When available, the **Workaround** statement provides a workaround to the issue.

Category	Bug ID	Description
Thermal Manager	228821	**Symptom**: Fans entered a **Fault** state. **Scenario**: All fans in tray three on a 6400 switch can enter a Fault state.
Slot Management	265113	**Symptom**: A Macsec selftest timed out on one port on a 6300 Switch Series R8S89A **Scenario**: This issue is observed on a 6300 Switch Series R8S89A in a VSF stack when issuing the **macsec selftest** command to run a self test for MACsec on all MACsec-capable interfaces.
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

Category	Bug ID	Description
		Conductor/Standby/Member, the convergence time would be lesser and around 70 seconds.
TFTP	272361	**Scenario**: Downloading/uploading the doftware Image via sm ubuntu IPv6 TFTP server fails. **Symptom**: TFTP Software image upload/download transfer operation fails. **Workaround**: Use the **blocksize** option in the copy command with a blocksize of 1375 or less. For example : `copy tftp://[20:1::100];blocksize=1375/image.swi secondary vrf vrf1`
MACsec	240672	**Symptom**: Traffic is dropped for a few seconds on a MACsec channel during a VSF switchover. **Scenario**: When the MACsec channel has data-delay protection enabled, there can be traffic drops for a few seconds on the channel post a VSF switchover due the reset of the MKA session on the interface. **Workaround**: Do not use data-delay protection in a MACsec policy if the system is deployed as a VSF stack.
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.
Internal srvcs: pspo	267398	**Symptom**: VXLAN tunnels go down after removing interfaces with IPv6 address that are the same as the VXLAN VTEP IP addresses. **Scenario**: In an EVPN-VXLAN deployment with an IPv6 tunnel, if any interface (irrespective of the VRF) that has same IP address as the tunnel source IP, it goes down, and then the tunnel interface is brought down **Workaround**: Unconfigure loopback and VXLAN and re-configure them.
Internal srvcs: Security PA infra	275859	**Symptom**: Port-Access security clients not onboarding after the following sequence of configuration change on a port. **Scenario**: This issue can occur if port-access security is enabled on port (802.1X/MAC-Auth/Port-Security/Device profile with security), and the configurations are cleared at port level using the default interface <interface-name> command on the port-access security enabled port. When port-access security is reenabled again at the same port leve, port-access security clients will not be onboarded on the port. **Workaround** Recover from this issue by performing a port flap via the commands **shut** and **no shut**. Perform a port flap (**shut**/**no shut**) at the port level if the command **default interface <interface-name>**" is issued on a port-access security enabled port, then reenable port- access security again on that port.

Upgrade information

AOS-CX 10.12.0006 for the 6300 Switch series uses ServiceOS FL.01.12.0002

AOS-CX 10.12.0006 for the 6400 Switch series uses ServiceOS FL.01.12.0003

NOTE

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.

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.

NOTE

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*.

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
10.09.0001 - 10.09.1050	▪ 10.09.1060 or later 10.09.xxxx release ▪ 10.10.1020 or later 10.10.xxxx release	10.12.0006 or later 10.12.xxx release
10.10.0001 - 10.10.1010	10.10.1020 or later 10.10.xxxx release	10.12.0006 or later 10.12.xxx release

Upgrades requiring one step:

Original Release	Final Upgrade Release
10.09.1060 or later 10.09.xxxx release	10.12.0006 or later 10.12.xxx release
10.10.1020 or later 10.10.xxxx release	10.12.0006 or later 10.12.xxx release

For 6300 and 6400 only: To execute an In-Service Software Upgrade (ISSU) to a 6400 Switch series or a VSF Enhanced Software Upgrade (ESU) for a 6300 Switch series, the switch must be running one of the following supported releases:

From	Supported Versions for Upgrade
10.12.0006	10.12.1000 or later versions
10.12.1000	10.12.1010 or later versions
10.12.1010	10.12.1011 or later versions
10.12.1011	10.12.1020

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.xx.*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 10.12 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.10.11.1010]
2. Secondary Software Image [xx.10.12.1000]

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 2017-2023 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:
```

NOTE

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 10.11 playlist of technical training videos on YouTube: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

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.