

# **AOS-CX 10.12.1000 Release Notes**

## **9300 Switch Series**



a Hewlett Packard  
Enterprise company

January 2024

Edition: 1

## Copyright Information

© Copyright 2024 Hewlett Packard Enterprise Development LP.

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.

### Products Supported

This release applies to the 9300Switch 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
R9A29A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Front-to-Back 6 Fans 2 AC PSU Bundle	10.10.1000
R9A30A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Back-to-Front 6 Fans 2 AC PSU Bundle	10.10.1000
R8Z96A	Aruba 9300-32D 32-port 100/200/400G QSFP-DD 2-port 10G Switch	10.10.1000

### Important information for 9300 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.

---

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.

---

---

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 `CL.10.0x.yyy`).

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

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
10.12.1000	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.



---

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
RPVST-Auto enable during VLAN creation	This version of AOS-CX supports automatic enabling/disabling of RPVST when a VLAN is created, and can be triggered either explicitly or automatically for the non-configured range, either with or without priority values. AOS-CX supports a maximum of 254 RPVST-enabled VLANs.
TACACS over VXLAN tunnel (IPv6 underlay)	TACACS enables centralized AAA services for network devices. In a complex VXLAN deployments, TACACS over VXLAN is required to ensure secure log on to the devices. This release of AOS-CX introduces support for TACACS over VXLAN with IPv6 underlay, an enhancement from previous releases which supported VXLAN with IPv4 underlay only.
ACLs	Control plane ACL behavior is changed in 10.12.1000. In previous releases, multicast packets were skipped from control plane ACL filters. Starting with this release, the implicit deny rule is taken into effect. After an upgrade to 10.12.1000, a control plane ACL configured in the default VRF could cause a multicast flood due to this behavior change. To avoid this issue, add an ACL rule to allow a multicast source IP in the existing control plane ACL (which is applied in default VRF).
TACACS improvements	The following TACACS enhancements are addressed in the release. <ul style="list-style-type: none"><li>Other management users (and not just admin users) can change a password for the next login.</li><li>A fail-through mechanism is triggered in when RADIUS/TACACS server response are corrupted. This fail-through mechanism also prevents local access for users whose authentication was rejected.</li><li>Commands <b>[no] aaa authorization allow-fail-through</b> and <b>[no] aaa accounting allow-fail-through</b> are introduced to support for authorization and accounting fail-through.</li><li>A limit to login attempts is configurable for local users even when TACACS or RADIUS is enabled.</li><li>TACACS/RADIUS FQDN retries are now configurable</li></ul>
Syslog over VXLAN tunnel	Syslog support over VXLAN tunnel is supported in this release, providing a mechanism to log events in centralized servers reachable over VXLAN tunnels.
DHCPv6 Relay over VXLAN tunnel	In complex VXLAN deployments, the DHCP relay support over VXLAN is required to relay DHCP messages across L2 domains. In previous CX releases, DHCPV4 relay over VXLAN tunnel is supported. This release of AOS-CX introduces support for , DHCPV6 relay over VXLAN to relay DHCP messages across L2 domains in the same VRF,an enhancement from previous releases, which supported only DHCPV4 relay over a VXLAN tunnel.
IPv6 Multicast over VXLAN tunnel	AOS-CX introduces support for IPv6 Multicast routing over VLXAN tunnel in a single fabric.

Category	Description
Source interface – SFTP client SSH Server/client	A source interface is configurable for SFTP clients, SSH Server and SSH Client, all for IPv4 and IPv6.
Connected host route – redistribution(BGP)	Connected Host route enhancements redistribute the Dynamic, IVRL and Static ARP/ND entries to BGP V4/V6 unicast address families.
VRF export route-map	This enhancement allows network administrators to control which routes are exported from a VRF, this option is supported under IPV4 and IPV6 address families
SLA over HTTPS	This release includes IP-SLA support over HTTPS. This feature helps measure a service level agreement (SLA) for the HTTPS protocol.

## 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 9300 switches, refer to the [AOS-CX Release Notes Portal](#).




---

The Bug ID is used for tracking purposes.

---

## Resolved issues

This section describes the issues resolved in this release.

Category	Bug ID	Description
OSPFv2	272233	<p><b>Symptom:</b>Creating a new OSPF process or restarting hpe-routing can change the Administrative Distance (AD) for all the OSPF process in same VRF.</p> <p><b>Scenario:</b> If OSPF processes have multiple configured Administrative Distance (ADs), this can cause unexpected behavior, as the last applied AD will be operational AD for all the OSPF processes.</p> <p><b>Workaround:</b> To avoid this issue, configure the same AD on all OSPF processes. If a new OSPF process need to be created, configure it via the REST API so the new OSPF process has the correct distance.</p>
MSTP	266777	<p><b>Symptom;</b> Integer overflow caused the PVST root to fluctuate for some VLANs, which caused checks to fail and SIP row addition to occur frequently.</p> <p><b>Scenario:</b> The switch had a high uptime (545 days in one instance), which led to an integer overflow that triggered repeated port additions in particular VLANs.</p> <p><b>Workaround</b> - Disable and then reenale STP for affected VLANs.</p>
OSPFv3	266040	<p><b>Symptom:</b> AN OSPFv3 session will not come up a 6-in-6 tunnel.</p>

Category	Bug ID	Description
		<b>Scenario:</b> This issue occurs when configuring OSPFv3 in a 6-in-6 tunnel interface.
BGP	268873	<p><b>Symptom:</b> SNMP incorrectly reports BGP peering sessions as idle</p> <p><b>Scenario:</b> This issue occurs when validating an BGP Session usingr snmpwalk output.</p> <p><b>Workaround:</b> Use the <b>show bgp</b> commands in the command-line interface and event logs output to view BGP status.</p>

## Feature Caveats

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

Feature	Description
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 <a href="#">REST API Migration Quick Start Guide</a> .
REST	<p>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.</p> <p>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,</p> <ol style="list-style-type: none"> <li>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).</li> <li>2. Erase the startup-config on the switch.</li> <li>3. Upgrade without saving the configuration to 10.12.xxxx.</li> <li>4. Copy the running-config from the remote server, <i>or</i> apply the entire configuration from scratch on the switch running the 10.12 firmware.</li> </ol>
PIM-SM	Pim Active-Active is not supported on overlay VXLAN SVIs.
SNMP	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.
Certificates	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



Feature	Description
	edited. For new certificate names, only alphanumeric characters, dots, dashes, and underscores are allowed.
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	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
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.
Multicast and VXLAN	<ul style="list-style-type: none"> <li>▪ VXLAN must be configured prior to configuring VSX.</li> <li>▪ IPv6 multicast is not supported for VXLAN overlay.</li> <li>▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details.</li> </ul>
PFC	Priority-based flow control (PFC) is not supported on a split port.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
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).

## 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
Internal svcs: pspo	267398	<p><b>Symptom:</b> VXLAN tunnels go down after removing interfaces with IPv6 address that are the same as the VXLAN VTEP IP addresses.</p> <p><b>Scenario:</b> 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</p> <p><b>Workaround:</b> Unconfigure loopback and VXLAN and re-configure them.</p>

## Upgrade information

AOS-CX 10.12.0006 uses ServiceOS CL.01.12.0002.



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.

---

## 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, CL.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:
```



---

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

---

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](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](https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS)

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](https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com) to initiate a subscription to receive future Aruba Security Bulletin alerts via email.