

AOS-CX 10.14.1000 Release Notes

9300 Switch Series



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.

This release applies to the 9300 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 following 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
S0F81A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Front-to-Back 6xFan 2xAC TAA Bundle	10.14.0005
S0F82A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Front-to-Back 6xFan 2xAC Bundle	10.14.0005
S0F83A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Back-to-Front 6xFan 2xAC TAA Bundle	10.14.0005
S0F84A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Back-to-Front 6xFan 2xAC Bundle	10.14.0005
S0F85A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Front-to-Back 6xFan 2xDC TAA Bundle	10.14.0005
S0F86A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Front-to-Back 6xFan 2xDC Bundle	10.14.0005
S0F87A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Back-to-Front 6xFan 2xDC TAA Bundle	10.14.0005
S0F88A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Back-to-Front 6xFan 2xDC Bundle	10.14.0005
S0F95A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G TAA Switch	10.14.0005
S0F96A	HPE Aruba Networking 9300S 32p QSFP28 100G 8p QSFP-DD 400G Switch	10.14.0005

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 configuration, files, databases, scripts, and so forth.

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.

AOS-CX 10.14 is a Short Supported Release (SSR).

- SSRs are short lived releases where Aruba will introduce new features and new hardware. This release will not be the last major release supported for any hardware model.
- AOS-CX SSR support period: Initial Release + 1 year.
- The End of Maintenance (EOM*) and End of Support (EOST) will be the same date.

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/>.

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 HPE Aruba Networking, unless noted in the table.

Version number	Release date	Remarks
10.14.1000	31 July 2024	Released, fully supported, and posted on the Web.
10.14.0001	29 May 2024	Initial release.

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	113
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	Refer to the AOS-CX and NetEdit Compatibility Matrix .
Aruba Central	2.5.8
Aruba Fabric Composer	7.0.2
Aruba CX Mobile App	Support for version 2.9.3 or later.



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 for 9300 Switches in AOS-CX 10.14.1000

This section describes the enhancements introduced in this release.

Category	Description
Transceivers	(For 9300-32D Switch Series only) Support for 400G-LR4 QDD 10Km SMF transceiver S3N96A - HPE ANW 400G LR4 QDD LC SMF XCVR

Category	Description
Transceivers	(For 9300S Switch Series only) Support for QSFP28 LR1 transceiver S3N89A - HPE ANW 100G LR QSFP28 LC SMF XCVR
Underlay Fabric	Support for IP-MTU and IP-TCP MSS on GRE tunnel interfaces
Underlay Fabric	IP unnumbered interfaces
Underlay Fabric	eBGP and OSPF point-2-point peering over IP unnumbered interface
Underlay Fabric	LLDP TLV for IP unnumbered interface
Feature Pack / Observability	In-band flow analyzer and telemetry support
Infrastructure Management and Usability	AOS-CX support for SNMP read-only MIB for transceivers
Infrastructure Management and Usability	Secure image transfer using HTTPS and MTLS between server and client (Firmware Site Distribution)

Resolved Issues for 9300 Switches in AOS-CX 10.14.1000

This section describes the issues resolved in this release.

Category	Bug ID	Description
REST	302889	<p>Symptom: Growth in the boot.log file file size may lead to an increase in RAM utilization.</p> <p>Scenario: This issue can be triggered by a high rate of unauthorized or wrong requests to the REST HTTPS server, which could occur during malicious attacks or vulnerability tool tests.</p>
VSX-Sync	309500	<p>Symptom: VSX sync is no longer syncing after a configuring BGP to redistribute to OSPF with a route map.</p> <p>Scenario: This issue can occur on a pair of switches in a VSX configuration that are syncing for BGP when a user configures redistribution for BGP to OSPF with a route map on the primary switch. VSX sync will not sync the redistribution configuration or any other new configuration.</p> <p>Workaround: Disable BGP syncing or remove the redistribution for BGP to OSPF with a route map.</p>
ARP	315962	<p>Symptom: Some hosts may experience connectivity issues.</p> <p>Scenario: In an EVPN environment with ARP suppression enabled, random hosts could experience connectivity issues due to missing the associated ARP entry</p> <p>Workaround: Temporarily add andremove a static ARP entry using the following commands</p> <pre>interface vlan <vlan_id> arp ipv4 <IPV4_ADDR> mac <MAC_ADDR> no arp ipv4 <IPV4_ADDR> mac <MAC_ADDR></pre>

Feature Caveats

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

Feature	Description
Central	When a switch is able to connect to Aruba Central but is not registered in the Aruba Central inventory or does not have a proper license, the switch will get disconnected. This connect/disconnect process will continue until the switch is properly registered in Aruba Central. To avoid this unnecessary reconnection cycle, best practices is to disable Aruba Central until the switch is registered in Aruba Central, or a license is obtained for that device.
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 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.
Hot Patch	When a hot-patch file download is triggered using the switch WebUI, log messages can incorrectly state that the file is added to the database with a missing status. This is a temporary state, and will correctly change to Not applied once the download is completed.
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.
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 there is chance of unexpected behaviors from these services. Best practices is to use unique port for each service across system.
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	WAN MACsec with a custom ether type will not be established between CX devices when there are PVOs switches in the bypass.
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

Feature	Description
	updated in the output of the show macsec status detailed command.
MACsec	In an environment with Cisco devices, when the GCM-AES-XPB-128 or GCM-AES-XPB-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	Multicast traffic cannot be run under GRE, 6in4, or 6in6 tunnels,
PFC	Priority-based flow control (PFC) is not supported on a split port.
PIM-SM	Pim Active-Active is not supported on overlay VXLAN SVIs.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
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.
Traceroute	Issuing the traceroute command with the ip-option loosesourceroute parameter fails in an overlay EVPN-VxLAN deployment.
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 the Active Gateway IP).
VXLAN	VXLAN must be configured prior to configuring VSX.

Known Issues

There are no known issue in this release.

PTP	301728	<p>Symptom: With the switch is configured with PTP protocol on multiple ports (both physical and lag) and user were to remove or add lag port to a clock source port, the sink port could flap.</p> <p>Scenario: In most cases, any PTP-related configuration changes will cause PTP services in the system to restart, which affects all the ports. Adding or removing a LAG port, can also cause PTP services to restart. There is a potential risk of of data traffic being miss-classified as PTP protocol packets for a very short window (milliseconds) and with enough of this traffic type, the PTP service will encounter the condition as if there were no sync packets from the grand source device. As a result, the PTP sink port will flap to re-establish the PTP protocol. However, even with the PTP sink port flap, the system can converge quickly and should not cause high offsets to downstream PTP clients.</p> <p>Workaround: Best practices is to implement PTP configuration changes during network downtime or a maintenance window.</p>
-----	--------	--

Upgrade information



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.



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 software 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 10.14 Fundamentals Guide](#).



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.10.13.1000]
2. Secondary Software Image [xx.10.14.0001]

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 2017-2024 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
- AOS-CX technical training videos on YouTube: 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 to initiate a subscription to receive future Aruba Security Bulletin alerts via email.