AOS-CX 10.12.1020 Release Notes

9300 Switch Series

a Hewlett Packard Enterprise company

December 2023
Edition: 1

Notices

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

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

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

Acknowledgments

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

Chapter 1
AOS-CX 10.12.1020 release notes

Products Supported

This release applies to the 9300Switch 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
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

NOTE

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.

NOTE

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.

NOTE

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.10.0*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

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)

NOTE

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.

NOTE

For more information, see the respective software manuals.

NOTE

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

Enhancements

This section describes the enhancements introduced in this release.

Category	Description

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

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.

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.
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.
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.

BGP	285425	**Symptom:** Aruba Central and NetEdit is unable to synchronize new configuration changes to a device. Aruba Central MultiEdit will display the following- warning message:
		`neighbor 1.1.1.1 remove-private-AS]`
		`Incomplete command or invalid parameters`
		A device validation failure will display the following- warning message:
		`Neighbor 1.1.1.1 does not exist`
		Scenario: A configuration synchronization failure will occur while using the NetEdit or Aruba Central MultiEdit to modify a switch configuration that has the BGP configuration **neighbor**

Category	Bug ID	Description
		remove-private-AS in the current running-config. **Workaround:** Manually configure the switch from the switch command-line interface.
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.

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 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). 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.
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

Feature	Description
	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 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	▪ 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.
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 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.

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.

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.