AOS-CX 10.11.1050 Release Notes

9300 Switch Series

a Hewlett Packard
Enterprise company

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 10.11.1050 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

Starting from AOS-CX 10.11.1050, 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

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

NOTE

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

For additional 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 10.11.xxxx Note: 10.11 is an SSR, recommended release is 10.11.10xx	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

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

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

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

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

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

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

Version history

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

Version number	Release date	Remarks
10.11.1050	2023-10-05	Released, fully supported, and posted on the Web.
10.11.1041	2023-09-08	Released, fully supported, and posted on the Web.
10.11.1040	2023-08-10	Released, fully supported, and posted on the Web.

Version number	Release date	Remarks
10.11.1030	2023-06-21	Released, fully supported, and posted on the Web.
10.11.1021	2023-05-12	Released, fully supported, and posted on the Web.
10.11.1010	2023-03-28	Released, fully supported, and posted on the Web.
10.11.1005	2023-03-03	Released, fully supported, and posted on the Web.
10.11.0001	2022-11-30	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	2.7.0
Aruba Central	Support in an upcoming Central upgrade (to be announced).
Aruba Fabric Composer	6.4.1
Aruba CX Mobile App	2.7.9 (or later)
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40

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

There are no new enhancements introduced in this release.

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 topic describes the resolved issues in this release.

Category	Bug ID	Description
Aruba Central	265125	**Symptom:** Switches are unable to establish connection with Aruba Central. **Scenario:** The **show aruba-central** command displays the **Central source connectionstatus** as **connection_failure**.
BGP	274060	**Symptom:** Traffic loss is observed on a few selective BGP networks. **Scenario:** This issue might occur when the BGP route is relearned when a connected BGP experiences a port flap. Also, a few BGP routes fail to get programmed. **Workaround:** Add a static route for the failed BGP route.
CLI Infra	269871	**Symptom:** High CPU utilization is observed on the **system-socket proxyd** process. **Scenario:** This issue occurs when the user leaves a vtysh console waiting at the user-input/page-prompt. **Workaround:** Provide an input at the page break.
Credential Manager	266007	**Symptom:** The **hpe-restd** process crashes unexpectedly. **Scenario:** This issue is observed due to rare timing issues that occur during the initialization and teardown phases of certificate validation requests from multiple modules which would lead to crashes in the REST daemon process. **Workaround:** Reboot the switch.
L3 Routes	274371	**Symptom:** Switches forward traffic to incorrect tunnel points. **Scenario:** This issue occurs either when the switch is rebooted, when the BGP sessions are cleared using the **clear bgp** command, or when the tunnel bounces. **Workaround:** Disable the tunnel where the traffic is being incorrectly forwarded and re-enable the tunnel when the switch forwards the traffic to the correct tunnel points.
Logging	TMA-3668	**Symptom:** The critical severity syslog messages continuously log the message, **systemd[1]: Failed to start Automatic**

Category	Bug ID	Description
		Rotation Of Logs. **Scenario:** This issue occurs when the logrotate service, ops-gen-logrotate.service are unable to restart.
NTP	271587	**Symptom:** The NTP conductor will not be available for NTP clients. **Scenario:** This issue occurs on VRF when both the NTP conductor and client are configured on the same VRF with a source interface on that VRF. As a result, the conductor will listen only to the configured source interface. **Workaround:** Configure the conductor on a separate VRF.
PKI	272227	**Symptom:** The **hpe-restd** process crashes unexpectedly. **Scenario:** This issue is observed due to rare timing issues that occur during the initialization and teardown phases of certificate validation requests from multiple modules which would lead to crashes in the REST daemon process. **Workaround:** Reboot the switch.
sFlow	269486	**Symptom:** sFLow encounters for some interfaces display zero and negative values intermittently. **Scenario**: This issue occurs when the OVSDB is overloaded on a system with large number of ports.
VLANS	271762	**Symptom**: The CLI process crashes on the switch with interface persona configured. **Scenario**: This issue occurs when the **show vlan** command is issued.
WebUI	269716	**Symptom:** NAE graphs render multiple incorrect variations. **Scenario:** NAE graphs referesh every 10 days and users observe variations in the graph rendering due to missing data.
WebUI	265798	**Symptom:** NAE graphs render multiple incorrect variations. **Scenario:** NAE graphs refresh every 10 days and users observe variations in the graph including an incorrect depiction of high CPU utilization.

Feature caveats

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

Feature	Description
PIM-SM	Pim Active-Active not supported on overlay VXLAN SVIs.
BGP	If a route-map is applied and none of the routes satisfy the match condition(s) in any of the route-map entries, then all routes are dropped.
SNMP	If 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.

Feature	Description
Certificates	When a switch uses a certificate with a legacy certificate name that is not supported in 10.11 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.
Config Mgmt	Configurations in JSON format may not be successfully imported from a previous release as a result of schema changes between software releases.
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 Loopback and GRE interfaces	IGMP cannot be enabled on either Loopback or GRE interfaces. IGMP and PIM is not supported on 6-in-6 Tunnel . PIM can be enabled only on Loopback interfaces.
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.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.

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

DHCP	230087	**Symptom**: A DHCPv6 server does not accept valid ASCII values or hex values for its dhcp-server options.
		Scenario: A DHCPv6 server does not accept valid ASCII values or hex values for its dhcp-server options **ascii** and **hex** .
		Example:
		`switch(config)# dhcpv6-server vrf default`
		`switch(config-dhcpv6-server)# pool vlan100`
		`switch(config-dhcpv6-server-pool)# option 10 ascii abc`
		`Invalid input: abc`
		`switch(config-dhcpv6-server-pool)# option 11 hex aa`
		`Invalid config: bad IPv6 address`

DHCP	239710	**Symptom**: A DHCP server does not accept an ASCII string for its dhcp-server options.

Category	Bug ID	Description

		Scenario: The DHCP server does not accept an ASCII string for its dhcp-server options if it has both an IPaddress and a special character (a comma), and the command returns the error "Invalid config: bad IPv4 address".
		Example:
		`switch(config)# dhcp-server vrf default`
		`switch(config-dhcp-server)# pool vlan100`
		`switch(config-dhcp-server-pool)# option 108 ascii "57003,10.1.2.3"`
		`Invalid config: bad IPv4 address.`

L3 routes	240831	**Symptom**: Route takes 180 seconds to get learn completely or stabilized when the CLI command **route recursive default route** is disabled during the Route flap. **Scenario**: Route flap is observed upon any uplink failover scenarios when the nexthop of BGP routes tries to resolve via default route . In order to avoid the flap, route recursive default route ipv4 or ipv6 should be disabled. if the CLI is disabled during the issue state. Route learning takes 180 seconds for learning it completely. CLI command **Route recursive default route ipv4 or ipv6** needs to be disabled first. **Workaround**: Issue the command **clear bgp ***.

Upgrade information

AOS-CX 10.11.xxxx uses ServiceOS CL.01.11.0005

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.10.11.*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 10.11 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.10.10.1040]
2. Secondary Software Image [xx.10.11.1010]
```

```
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.