AOS-CX 10.12.1010 Release Notes

10000 Switch Series

a Hewlett Packard
Enterprise company

November 2023
Edition: 2

Copyright Information

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

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

Notices

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

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

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

Acknowledgments

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

Chapter 1
AOS-CX 10.12.1010 release notes

Products Supported

This release applies to the 10000 Switch Series. The following table lists any applicable minimum software versions required for that model of switch.

NOTE

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

Product number	Product name	Minimum software version
R8P14A	Aruba CX 10000-48Y6C Distributed Services Back-to-Front Bundle	10.10.0002
R8P13A	Aruba CX 10000-48Y6C Distributed Services Front-to-Back Bundle	10.10.0002

Important information for 10000 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.

NOTE

AOS-CX BGP implementations support resolving a BGP route's nexthop to a default route (0.0.0.0/0). However, this is not generally recommended in network deployments. Considering the default route to be the last resort route, resolving the BGP route's nexthop to a default route can cause potential routing loops in the network, if they are not properly designed and monitored. Route flaps and/or traffic drops may be observed in such cases.

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

NOTE

To restore a previous configuration when downgrading to a previous version of software, follow these steps:

1. Use the `show checkpoint` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the `Image Version` column in the output of the command, for example .10.0*x.yyyy*).

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.

2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

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

To upgrade to:	Your switch must be running this version or later:
AOS-CX 10.12.xxxx Note: 10.12 is an SSR, recommended release is 10.12.0006	AOS-CX 10.09.0002
AOS-CX 10.11.xxxx Note: 10.11 is an SSR, recommended release is 10.11.0001	AOS-CX 10.08.0001
AOS-CX 10.10.xxxx Note: 10.10 is an LSR, recommended release is 10.10.10xx.	AOS-CX 10.06.0110

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
10.12.1010	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
Pensando Policy and Services Manager (PSM)	1.62.3-T
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

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 10000 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
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

Category	Bug ID	Description
		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.
Internal srvs: Security PA Infra	278954	**Symptom:** Clients, that onboard on an interface with concurrent on-boarding enabled and with default priority, are onboarded with lower authentication method. Also, the authentication requests are not seen for higher authentication methods. **Scenario:** This issue occurs when auth-precendence is configured on the switches. When concurrent on-boarding is enabled with default priority and when auth-precedence is configured with non-default precedence on a port, the clients that onboard take an incorrect authentication priority. **Workaround:** Configure the authentication priority again on the port and then onboard the clients.
Health Monitor	TMA-3674	**Symptom:** Switches reboot unexpectedly. **Scenario:** Switches reboot unexpectedly with an error message similar to **PCI access failed**.
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 Rotation Of Logs.** **Scenario:** This issue occurs when the logrotate service and ops-gen-logrotate.service are unable to restart.
Management Module	TMA-3574	**Symptom:** In rare circumstances, switches may reboot unexpectedly with an error message, **Critical service fault (DSM port failure).** **Scenario:** This issue is rarely observed on switches running AOS-CX versions prior to 10.12.1010. If you are running previous AOS-CX versions, it is recommended to upgrade the switch to AOS-CX 10.12.1010.
NTP	271587	**Symptom:** The NTP conductor will not be available for NTP clients.

Category	Bug ID	Description
		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	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.
WebUI	269716	**Symptom:** NAE graphs render multiple incorrect variations. **Scenario:** NAE graphs refresh every 10 days and users observe variations in the graph rendering due to missing data.

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,

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td></td><td>

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.

</td></tr>
<tr><td>PIM-SM</td><td>Pim Active-Active is not supported on overlay VXLAN SVIs.</td></tr>
<tr><td>SNMP</td><td>When SNMP is enabled via the switch CLI, it can take between 1-2 minutes for the SNMP daemon to be ready to respond to requests. If a local or external SNMP MIB walk is performed in the interval between when SNMP is first enabled and the SNMP daemon is ready, the MIB walk action will return an error.</td></tr>
<tr><td>Certificates</td><td>When a switch uses a certificate with a legacy certificate name that is not supported in 10.12 because it contains disallowed characters, the information will migrate properly in the upgrade, but that certificate can no longer be edited. For new certificate names, only alphanumeric characters, dots, dashes, and underscores are allowed.</td></tr>
<tr><td>Port Access</td><td>Port Access (802.1x, MAC Authentication, Device Profile), Port Security, IPv4/v6 Source Lockdown, Dynamic ARP Inspection and/or DHCPv4/v6 Snooping configurations are mutually exclusive with PSM stateful firewall policies.</td></tr>
<tr><td>Subinterfaces</td><td>BFD sessions are not supported on sub interfaces. Use a switch virtual interfaces (SVI) to configure a BFD session.</td></tr>
<tr><td>REST</td><td>Boundary values for **match vni** and **set local preference** in a route-map system cannot be set via the REST API and must be manually configured on the switch via the CLI.</td></tr>
<tr><td>Stateful L4 firewall</td><td>For locally-switched and routed flows on the switch, the traffic from the host is subject to policy processing only once and only egress policy is enforced on the traffic egressing the workload and entering the switch.</td></tr>
<tr><td>Stateful L4 firewall</td><td>Stateful services for VRFs, where route leaking is enabled, are not supported.</td></tr>
<tr><td>Stateful L4 firewall</td><td>Port-access (802.1x, MAC authentication, Device Profile), Port-security, DHCP v4/v6 snooping, Dynamic ARP Inspection and/or IPv4/v6 Source Lockdown configurations are mutually exclusive with PSM Stateful firewall policies</td></tr>
<tr><td>BGP</td><td>

The **next-hop-unchanged** option needs to be explicitly configured to preserve nexthop while advertising routes to eBGP peers, in the L2VPN EVPN address-family. For example:

```
 router bgp 1
neighbor 1.1.1.1 remote-as 2
      address-family l2vpn evpn
         neighbor 1.1.1.1 activate
neighbor 1.1.1.1 next-hop-unchanged
```

</td></tr>
</table>

Feature	Description

	`      neighbor 1.1.1.1 send-community extended`
	`   exit-address-family`
	`!`

Classifiers	Classifier policies, IPv6 and MAC ACLs are not supported on egress.
Classifiers	Egress ACL logging is not supported.
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	IPv4 egress ACLs can be applied only to route-only ports.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	Automatic downgrade of the startup–config is not supported during a software downgrade.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters	Layer 3 Route-only port counters are not enabled by default. Enabling them will reduce ipv4 route scale to 80K.
ICMP Redirect	The switch may incorrectly duplicate an IP frame that triggers ICMP redirect.
IGMP/PIM on 6-in-6, Loopback and GRE interfaces	IGMP cannot be enabled on either Loopback or GRE interfaces. IGMP and PIM is not supported on a 6-in-6 Tunnel.
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.
MVRP and VSX	MVRP is mutually exclusive with VSX.
Network Analytics Engine (NAE)	Agents monitoring a resource that has column type enum with a list of strings (as opposed to a single string enum) is not supported.
Network Analytics Engine (NAE)	Network Analytics Engine (NAE) agents execute Command Line Interface (CLI) actions as 'admin' user, so they have permission to run any command by default. However, when the authentication, authorization and accounting (AAA) feature is enabled, the same restrictions applied to 'admin' will also apply to NAE agents. When using AAA, make sure to give the admin user the permissions to run all commands needed by enabled NAE agents. Otherwise, some CLI commands may be denied and their outputs won't be available. Actions other than CLI won't be affected and will execute normally. Also, NAE agents won't authenticate, thus the AAA service configuration must not block authorization for unauthenticated 'admin' user. ClearPass doesn't support such configuration, so it cannot be used as a TACACS+ server.

Feature	Description
Network Analytics Engine (NAE)	The following tables are not supported for NAE scripts: OSPF_Route, OSPF_LSA, OSPF_Neighbor, BGP_Route.
OSPF	OSPFv2 and OSPFv3 do not support detailed LSA **show** commands.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RPVST+ and MSTP	Spanning Tree can only run in MSTP or RPVST+ mode.
RPVST+ and MVRP	RPVST+ is mutually exclusive with MVRP.
VRF	VRF names are limited to 31 characters.
VRRP	The same virtual link-local address cannot be used across different VRFs.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
Traceroute	Traceroute v4/v6 over VXLAN fails to find intermediate next-hop IP information from a source VTEP in Virtual Active Gateway environment (the SVI is the same as theActive Gateway IP).
VRRP	VRRP Preemption Delay Timer (preempt delay minimum) may be ignored after a switch reboot or power cycle.
DHCP Server, DHCP Relay, and DHCP Snooping	DHCP Relay and DHCP Snooping can co-exist on the same switch. DHCP Snooping and DHCP Server cannot co-exist on the same switch. DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.

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
VXLAN	T-1223	**Symptom**: North-South or South-North traffic cannot be inspected. **Scenario**: This issue occurs on 10000 Series switches that support VRF to VRF traffic with firewall inspection. **Workaround**: Leak the inter-vrf traffic on borders (without firewall enabled) and inspect them on non-border VTEPs.
VXLAN	T-1245	**Symptom**; fLocal proxy ARP cannot be disabled per VLAN. **Scenario**: Deployments that require local proxy ARP.
Port	T-1013	**Symptom**: A port with AOC15 SFP might not link up after a link flap. **Scenario**: If AOC15 SFP is used, and there are multiple port flaps, then

Category	Bug ID	Description
		there is a chance that the port might not link up. **Workaround**: Recover from this issue by issuing the commands **shut** and **no shut** on the port.
IPSEC	T-3412	**Symptom**: DSCP classification will not work with IPSec. Scenario: This issue is observed in a deloyment with anIPSec tunnel is configured between two 10000 Switch series in *no_ha* mode.
L3 addressing	T-3012	**Syymptom**: There may be a delay in the programming of IPsec tunnels after a switch reboot. **Scenario**: A Higher SVI scale with IPsec tunnel may increase traffic convergence time upon system reboot.
Core	T-454	**Symptom**: The **show core-dump all** command does not show cores from DSM. **Scenario**: Core dumps from DSM are not shown in the output of `show core-dump all` command in AOS-CX.

Upgrade information

AOS-CX 10.12.0006 uses ServiceOS DL.01.11.0001.

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, DL.10.xx.*yyyy*).

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.
2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

Performing the upgrade

For additional upgrade and downgrade scenarios, including limitations of automatic upgrade and downgrade scenarios provided by the Configuration Migration Framework (CMF), refer to the **AOS-CX 10.12 Fundamentals Guide**.

CAUTION

This version may contain a change of BootROM from the current running version. A BootROM update is a non-failsafe update. Do not interrupt power to the switch during the update process or the update could permanently damage the device.

1. Copy the new image into the non-current boot bank on the switch using your preferred method.
2. Depending on the version being updated, there may be device component updates needed. Preview any devices updates needed using the `boot system <BOOT-BANK>` command and entering `n` when asked to continue.

   For example, if you copied the new image to the secondary boot bank and no device component updates are needed, you will see this:

   ```
   switch# boot system secondary
   Default boot image set to secondary.
   Checking if the configuration needs to be saved...

   Checking for updates needed to programmable devices...
   Done checking for updates.

   This will reboot the entire switch and render it unavailable
   until the process is complete.
   Continue (y/n)? n
   ```

   In this example, three device updates will be made upon reboot, one of which is a non-failsafe device:

   ```
   switch# boot system secondary
   Default boot image set to secondary.
   Checking if the configuration needs to be saved...

   Checking for updates needed to programmable devices...
   Done checking for updates.

   2 device(s) need to be updated during the boot process.
   The estimated update time is between 2 and 3 minute(s).
   There may be multiple reboots during the update process.

   1 non-failsafe device(s) also need to be updated.
   Please run the 'allow-unsafe-updates' command to enable these updates.

   This will reboot the entire switch and render it unavailable
   until the process is complete.
   Continue (y/n)? n
   ```

3. When ready to update the system, if a non-failsafe device update is needed, make sure the system will not have any power interruption during the process. Invoke the `allow unsafe updates` command to allow updates to proceed after a switch reboot. Proceed to step 4 within the configured time.

```
switch# config
switch(config)# allow-unsafe-updates 30

This command will enable non-failsafe updates of programmable devices for
the next 30 minutes.  You will first need to wait for all line and fabric
modules to reach the ready state, and then reboot the switch to begin
applying any needed updates.  Ensure that the switch will not lose power,
be rebooted again, or have any modules removed until all updates have
finished and all line and fabric modules have returned to the ready state.

WARNING: Interrupting these updates may make the product unusable!

Continue (y/n)? y

    Unsafe updates      : allowed (less than 30 minute(s) remaining)
```

4. Use the `boot system <BOOT-BANK>` command to initiate the upgrade. On the switch console port an output similar to the following will be displayed as various components are being updated:

```
switch# boot system secondary
Default boot image set to secondary.
Checking if the configuration needs to be saved...

Checking for updates needed to programmable devices...
Done checking for updates.

3 device(s) need to be updated during the boot process.
The estimated update time is between 2 and 3 minute(s).
There may be multiple reboots during the update process.


This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.

Looking for SVOS.

Primary SVOS:  Checking...Loading...Finding...Verifying...Booting...

ServiceOS Information:
    Version:          <serviceOS_number>
    Build Date:       yyyy-mm-dd hh:mm:ss PDT
    Build ID:         ServiceOS:<serviceOS_number>:6303a2a501ba:202006171659
    SHA:              6303a2a501bad91100d9e71780813c59f19c12fe

Boot Profiles:

0. Service OS Console
1. Primary Software Image [xx.10.11.1010]
2. Secondary Software Image [xx.10.12.1000]

Select profile(secondary):

ISP configuration:
    Auto updates        : enabled
    Version comparisons : match (upgrade or downgrade)
    Unsafe updates      : allowed (less than 29 minute(s) remaining)

Advanced:
    Config path         : /fs/nos/isp/config [DEFAULT]
    Log-file path       : /fs/logs/isp [DEFAULT]
    Write-protection    : disabled [DEFAULT]
    Package selection   : 0 [DEFAULT]

3 device(s) need to be updated by the ServiceOS during the boot process.
The estimated update time by the ServiceOS is 2 minute(s).
There may be multiple reboots during the update process.


MODULE 'mc' DEVICE 'svos_primary' :
    Current version  : '<serviceOS_number>'
    Write-protected  : NO
    Packaged version : '<version>'
    Package name     : '<svos_package_name>'
    Image filename   : '<filename>.svos'
    Image timestamp  : 'Day Mon dd hh:mm:ss yyyy'
    Image size       : 22248723
    Version upgrade needed

Starting update...

Writing...    Done.
Erasing...    Done.
Reading...    Done.
Verifying...  Done.
Reading...    Done.
Verifying...  Done.


Update successful (0.5 seconds).

reboot: Restarting system
```

Multiple components may be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

```
 (C) Copyright 2017-2023 Hewlett Packard Enterprise Development LP

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

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at: https://asp.arubanetworks.com

switch login:
```

NOTE

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

Chapter 2
Other resources

Aruba is committed to ensuring you have the resources you need to be successful. Check out these learning and documentation resources:

- AOS-CX switch software documentation portal: https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
- AOS-CX 10.11 playlist of technical training videos on YouTube: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

Chapter 3
Aruba security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/security-bulletins/. You can sign up at https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com to initiate a subscription to receive future Aruba Security Bulletin alerts via email.