AOS-CX 10.14.0001 Release Notes

8400 Switch Series

May 2024
Edition: 1

Copyright Information

© Copyright 2024 Hewlett Packard Enterprise Development LP.

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

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

Notices

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

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

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

Acknowledgments

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

Chapter 1
AOS-CX 10.14.0001 Release Notes

This release applies to the 8400 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 below table, no minimum software version is required.

Product number	Product name	Minimum software version
JL366A	Aruba 8400X 6-port 40GbE/100GbE QSFP28 Advanced Module	10.00.0006
JL363A	Aruba 8400X 32-port 10GbE SFP/SFP+ with MACsec Advanced Module	10.00.0006
JL687A	Aruba 8400X-32Y 32p 1/10/25G SFP/SFP+/SFP28 Module	10.04.2000

Important information for 8400 Switches

Aruba switches covered by this release note use eMMC or SSD storage. This is non-volatile memory for persistent storage of config, files, databases, scripts, and so forth. Aruba recommends updating to version 10.06.0100 or later (including this release) to implement significant improvements to memory usage and prolong the life of the switch.

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Clear the browser cache after upgrading to this version of software before logging into the switch using a Web UI session. This will ensure the Web UI session downloads the latest changes.

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
10.14.0001	21 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	2.11.0
Aruba Central	2.5.8
Aruba Fabric Composer	7.0.2
Aruba CX Mobile App	Support for version 2.9.3 or later.
IMC	(708P03)

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 8400 Switches in AOS-CX 10.14.0001

This section describes the enhancements introduced in this release.

Category	Description
EVPN	EVPN routes can be matched against additional **evpn-type** values: ▪ evpn-type-2 MAC/IP Advertisement Route ▪ evpn-type-3 Inclusive Multicast Ethernet Tag Route ▪ evpn-type-5 IP Prefix route
Classifier	In previous releases, the ACL Logging text could display a value of **unknown** for either the sequence number or the list type. This issue could occur if an ACL is configured with the **log** keyword *and* the switch is are using QoS or VSX features. Starting with AOS-CX 10.14.0001, the logging message includes source and destination addresses and protocol. The **unknown** value no longer appears if there is no sequence number to display.
Overlay Fabric	Multicast anycast RP/MSDP for IPv4 multicast routing in the VXLAN overlay fabric design.
Overlay Fabric	Multi-fabric Route-Server for BGP peering for EVPN-AF for provisioning VXLAN tunnels between border VTEPs in a multi-fabric design.
Underlay Fabric	Increased range of the OSPF process ID from 1-63 to 1- 65535
Underlay Fabric	VRF support for non-VRF/Namespace aware container applications
Underlay Fabric	Port-mapping for container private IP reachability in a DNAT configuration
Underlay Fabric	Fix for setting multiple communities and extended communities in a route-map. Ability to set multiple and extended communities per prefix in a route-map used by BGP for both IPv4 and IPv6 address families.
Containers	Multiple container infrastructure hardening features to increase overall system stability
OSPF	Ability to configure a different AD for multiple OSPF process in a VRF
Infrastructure Management and Usability	Visibiity into configuration history from previous sessions
Infrastructure Management and Usability	Local switch WebUI connections over IPv6

Category	Description
Infrastructure Management and Usability	SNMPv3 enablement without any SNMPv2 or community configured
Infrastructure Management and Usability	Ability to display all the deprecated CLI commands and new version of those commands in the CLI
Infrastructure Management and Usability	Output of the show interfacecommand now displays how long the interface has been down
Infrastructure Management and Usability	AOS-CX introduces support for NAE-Lite
Infrastructure Management and Usability	SNMP trap filter per host
Infrastructure Management and Usability	SNMP read extended interface MIB for reporting

Resolved Issues for 8400 Switches in AOS-CX 10.14.0001

This section describes the issues resolved in this release.

Component	Summary	Description
Central	294122	**Symptom**: Some hpe-restd core dumps may be generated after the switch reboots.This will not interrupt the normal switch operation. **Scenario**: This can occur every time the switch reboots. **Workaround**: The hpe-restd core dumps generated after after the switch is rebooted have no impact to switch operation, and can be ignored
IGMP	215677	**Symptom**: IGMP/MLD configuration changes do not take effect when the **hpe-mgmdd** process is flooded with IGMP/MLD control packets. **Scenario**: In a situation where IGMP or MLD control packets (Joins or Leaves) are part of a loop, or if misbehaving clients send continuous streams of IGMP/MLD control packets, the **hpe-mgmdd** daemon's packet queue can become continuously full. **Workaround**: Restart the MGMD daemon using the command **systemctl restart hpe-mgmdd**.
DNS	230380	**Symptom:** The switch experiences high CPU utilization . **Scenario:** High CPU utilization occurs when SNMP invokes DNS resolution, due to access of source IP which causes CPU overhead.
BGP	285540	**Symptom:** When both IPv4 and IPv6 neighbors are configured in BGP, an SNMP walk displays incorrect information on IPv4 peer sessions. **Scenario:** If the customer configures both IPv4 and IPv6 neighbors, the SNMP walk output will include information on non-existent IPv4 peers. The IPv6 peer information displays

Component	Summary	Description
		as expected.
DHCP Relay	291742	**Symptom:** DHCP relay does not change the source IP address of the DHCP discover frame **Scenario:** This issue occurs if the DHPCP client does not use **0.0.0.0** as the source IP, for example. when the DHCP packet is generated by the client with a valid private IP as source IP. **Workaround:** Use the source interface configuration.
BGP	295703	**Symptom**: When the **show bgp vrf info** command is run, the , vtysh session is logged out. **Scenario:** This issue occurs when VRF is configured with export RT (Route Target). **Workaround:** Use the command **show running-config vrf** to prevent the vtysh session from logging out.
LEDs - Buttons	297812	**Symptom:** Port LEDs remain off even when link is established and traffic is flowing. **Scenario:** This issue can occur if the **no module** command is issued on a line card. **Workaround:** Check the CLI for link status and health, as the CLI can deliver the same information provided by the port LEDs.
VSX-Sync	299838	**Symptom**: An Interface VLAN configuration is not getting synced to secondary switch. **Scenario**: This issue can occur n a pair of switches in VSX configuration, when the user creates an Interface VLAN with VSX-Sync configuration in primary switch, then the user creates the same Interface VLAN on secondary, but the configuration is not synced. **Workaround**: Once VSX-Sync has been enabled on primary Interface VLAN, wait ~15 seconds before creating the Interface VLAN on the secondary interface. Another workaround is to first create the Interface VLAN on the secondary and then enable VSX-Sync on the primary Interface VLAN. (There is no need to wait in this second workaround).
VSX	299851	**Symptom:** The VSX software upgrade software version is not properly validated when upgrading using TFTP. **Scenario:** When upgrading using TFTP, it is possible to load mismatched software versions, resulting in a VSX upgrade failure and a VSX software mismatch between the primary and secondary VSX nodes. **Workaround:** Confirm that software image versions are compatible. Software upgrades using boot banks rather than TFTP will perform a proper version check before completing the upgrade.
SNMP	303650	**Symptom**: The snmpd process crashes and SNMP polling stops for a few seconds. **Scenario**: This issue can occur when polling by SNMP (snmpwalk), and simultaneously performing a snmpget/snmpbulkget on a non-existent OID. The SNMP process will recover itself after the crash.
CX-Licensing	TMA-4234	**Symptom:** The switch advanced feature pack shows as

Component	Summary	Description
		expired. **Scenario:** This issue occurs if the switch is configured with non-UTC time. After installing a feature pack to enable the advanced features on the switch, the feature pack expiration date is incorrectly flagged as expired **Workaround:** Set the switch to UTC time to activate the feature pack.

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.
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.
PIM-SM	Pim Active-Active is not supported on overlay VXLAN SVIs.
SNMP	When SNMP is enabled via the switch CLI, it can take between 1-2 minutes for the SNMP daemon to be ready to respond to requests. If a local or external SNMP MIB walk is performed in the interval between when SNMP is first enabled and the SNMP daemon is ready, the MIB walk action will return an error.
Certificates	When a switch uses a certificate with a legacy certificate name that is not supported in 10.12 because it contains disallowed characters, the information will migrate properly in the upgrade, but that certificate can no longer be edited. For new certificate names, only alphanumeric characters, dots, dashes, and underscores are allowed.
REST	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.
BGP	In environments with VRRP or VSX peers, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch will install both routes as ECMP instead of preferring the leaked route. Use route-maps to give lower/higher preference to the routes received from an iBGP peer. For example: `!`

Feature	Description
	`` route-map rmap permit seq 10 set local-preference 50 ! router bgp 100 vrf red neighbor 1.1.1.2 remote-as 100 address-family ipv4 unicast neighbor 1.1.1.2 activate neighbor 1.1.1.2 route-map rmap in exit-address-family ``` In the above example, since a lower value of local-preference (i.e. 50, whereas default value is 100) has been set to the routes received from iBGP peer, the leaked routes get preferred and get installed as best routes.
BGP	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 neighbor 1.1.1.1 send-community extende exit-address-family ```
Classifiers	Classifier policies, IPv6 and MAC ACLs are not supported on egress.
Classifiers	DSCP remarking is performed only on routed packets.
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	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters	Classifier Counters: Max number Classifier entries with count action: JL363A=32K, JL365A=32K, JL366A=16K.
Counters	Counters are shared between ACL and Layer 3 ports. The Max number of ACL entries with count action plus Layer 3 counters is: JL363A=24K, JL365A=24K, JL366A=8K. Enabling counters on a Layer 3 port consumes 6 ACL counter entries.
Counters	Layer 3 Route-only port counters are not enabled by default. Enabling them will remove them from the counter resources shared with ACLs.
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.

Feature	Description
	DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.
DHCP Server, DHCP Relay, and DHCP Snooping	DHCPv4 Snooping and DHCPv4 Server cannot co-exist on the same switch. DHCPv6 Snooping and DHCPv6 Server cannot co-exist on the same switch.
EVPN	The iBGP split-horizon rule is not followed between different address families. Use route-map to block the routes getting advertised to the iBGP peer.
IP-SLA	Reserved ports or ports used by other applications/services with in 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.
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)	After management module failover, up to 5 minutes of alert history could be lost.
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 Analects 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.
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.
RADIUS	Authorization by means of HPE VSAs is not supported.
REST	REST supports the 'admin' and 'operator' roles but does not work with

Feature	Description
	TACACS+ command authorization.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RIP/RIPng	RIP/RIPng metric configuration support is not available.
RPVST+ and MSTP	Spanning Tree can only run in MSTP or RPVST+ mode.
RPVST+ and MVRP	RPVST+ is mutually exclusive with MVRP.
sFlow and Mirroring	sFlow and port mirroring are mutually exclusive per port. A port cannot support both sFlow and mirroring at the same time.
UDLD	For a UDLD-enabled interface to not lose traffic during a failover operation, the result of multiplying 'interval' and 'retries' should be at least 8 seconds. The default values are 7000 ms (interval) x 4 (retries) = 28 seconds.
VRF	VRF names are limited to 31 characters.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
Traceroute	Issuing the **traceroute** command with the i**p-option loosesourceroute** parameter fails inan 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 theActive Gateway IP).
VRRP	VRRP Preemption Delay Timer (preempt delay minimum) may be ignored after a switch reboot or power cycle.
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.
VSX and Static VXLAN	Static VXLAN on VSX configuration is not supported. Use VSX and EVPN or VSX and HSC.
VXLAN	DSCP-enabled packets carried in a VXLAN tunnel are treated as best-effort traffic.
VXLAN	IPv6 traffic does not work over static VXLAN.

Known Issues

There are no known issue in this release.

Upgrade information

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software.
To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where <*VLAN_ID*> is the native VLAN ID configured on the trunk interface.
If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

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.

Some Network Analytics Engine (NAE) scripts may not function properly after an upgrade. Aruba recommends deleting existing NAE scripts before an upgrade and then reinstalling the scripts after the upgrade. For more information, see the *Network Analytics Engine Guide*.

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, XL.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.

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 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.