# AOS-CX 10.14.0001 Release Notes

## 6300, 6400 Switch Series


May 2024
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 10.14.0001 Release Notes

This release applies to the 6300 and 6400 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 |
|---|---|---|
| S0E91A | HPE Aruba Networking 6300M 48p SR10 1G/2.5G/5G/10G PTP/AVB Class8 PoE and 4p 100G MACsec Switch | 10.13.1000 |
| S0X44A | HPE Aruba Networking 6300M 48p SR10 1G/2.5G/5G/10G PTP/AVB Class8 PoE 4p 100G MACsec TAA Switch | 10.13.1000 |
| R8S89A | Aruba 6300M 24p SR10 10Gbase-T, PTP/AVB, 60W Class6 PoE with 2 x 50G and 2 x 25G MACsec Switch | 10.10.0002 |
| R8S90A | Aruba 6300M 48p SR5 (up to 5G), PTP/AVB, 90W Class 8 PoE with 2 x 50G and 2 x 25G MACsec Switch | 10.10.0002 |
| R8S91A | Aruba 6300M 48p SR5 (up to 5G) 60W Class6 PoE with 12p 90W Class 8 PoE with 2x 50G and 2x10G LRM/MACsec Switch | 10.10.0002 |
| R8S92A | Aruba 6300M 24p SFP+ 10G LRM support and 2 x 50G and 2 x 25G MACsec Switch | 10.10.0002 |
| S0G03A | HPE Aruba Networking 6300M 24p SFP+ and 4p SFP56 TAA Switch | 10.14.0001 |
| S0G04A | HPE Aruba Networking 6300M 48p HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4p SFP56 TAA Switch | 10.14.0001 |
| S0G05A | HPE Aruba Networking 6300M 24p HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4p SFP56 TAA Switch | 10.14.0001 |
| S0G06A | HPE Aruba Networking 6300M 48p 1GbE Class 4 PoE and 4p SFP56 TAA Switch | 10.14.0001 |
| S0F99A | HPE Aruba Networking 6300M 24p 1GbE Class4 PoE 4p SFP56 TAA Switch | 10.14.0001 |
| S0G00A | HPE Aruba Networking 6300M 48p 1GbE 4p SFP56 TAA Switch | 10.14.0001 |
| S0G01A | HPE Aruba Networking 6300M 24p 1GbE 4p SFP56 TAA Switch | 10.14.0001 |
| S0G02A | HPE Aruba Networking 6300M 48p 1GbE 4p SFP56 Power-to-Port 2 Fan Trays 1 PSU TAA Switch Bundle | 10.14.0001 |
| S0G95A | HPE Aruba Networking 6300F 48G Class4 4p SFP56 50G TAA Switch | 10.14.0001 |

| Product number | Product name | Minimum software version |
|---|---|---|
| S0G96A | HPE Aruba Networking 6300F 24G Class4 4p SFP56 50G TAA Switch | 10.14.0001 |
| S0G97A | HPE Aruba Networking 6300F 48G 4p SFP56 50G TAA Switch | 10.14.0001 |
| S0G98A | HPE Aruba Networking 6300F 24G 4p SFP56 50G TAA Switch | 10.14.0001 |
| JL665A | Aruba 6300F 48-port 1GbE Class 4 PoE and 4-port SFP56 Switch | 10.04.0001 |
| JL666A | Aruba 6300F 24-port 1GbE Class 4 PoE and 4-port SFP56 Switch | 10.04.0001 |
| JL667A | Aruba 6300F 48-port 1GbE and 4-port SFP56 Switch 10.04.0001 | 10.04.0001 |
| JL668A | Aruba 6300F 24-port 1GbE and 4-port SFP56 Switch 10.04.0001 | 10.04.0001 |
| R0X31A | Aruba 6400 Management Module | 10.04.1000 |
| R0X38B | Aruba 6400 48-port 1GbE Class 4 PoE Module | 10.04.1000 |
| R0X38C | Aruba 6400 48-port 1GbE Class 4 PoE v2 Module | 10.09.1000 |
| R0X39B | Aruba 6400 48-port 1GbE Class 4 PoE and 4-port SFP56 Module | 10.04.1000 |
| R0X39C | Aruba 6400 48-port 1GbE Class 4 PoE and 4-port SFP56 v2 Module | 10.09.1000 |
| R0X40B | Aruba 6400 48-port 1GbE Class 6 PoE and 4-port SFP56 Module | 10.04.1000 |
| R0X40C | ruba 6400 48-port 1GbE Class 6 PoE and 4-port SFP56 v2 Module | 10.09.1000 |
| R0X41A | Aruba 6400 48-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 Module | 10.04.1000 |
| R0X41C | Aruba 6400 48-port HPE Smart Rate 1/2.5/5GbE Class 6 PoE and 4-port SFP56 v2 Module | 10.09.1000 |
| R0X42A | Aruba 6400 24-port 10Gbase-T and 4-port SFP56 Module | 10.04.1000 |
| R0X42C | R0X42C Aruba 6400 24-port 10Gbase-T and 4-port SFP56 v2 Module | 10.09.1000 |
| R0X43A | Aruba 6400 24-port SFP+ and 4-port SFP56 Module | 10.04.1000 |
| R0X43C | Aruba 6400 24-port SFP+ and 4-port SFP56 v2 Module | 10.09.1000 |
| R0X44A | Aruba 6400 48-port 10/25GbE SFP28 Module | 10.04.2000 |
| R0X44C | Aruba 6400 48-port 1G/10G/25GbE SFP28 v2 Extended Tables Module | 10.09.1000 |
| R0X45A | Aruba 6400 12-port 40/100GbE QSFP28 Module | 10.04.2000 |
| R0X45C | Aruba 6400 12-port 40/100GbE QSFP28 v2 Extended Tables Module | 10.09.1000 |
| R0X26A | Aruba 6405 Switch | 10.05.0021 |
| R0X27A | Aruba 6410 Switch | 10.05.0001 |

| Product number | Product name | Minimum software version |
|---|---|---|
| JL741A | Aruba 6410 96-port 1GbE Class PoE 4 and 4-port SFP56 Switch | 10.05.0001 |
| S0E48A | HPE Aruba Networking CX 6400 v2 32p SFP28 25G 4p QSFP28 100G MACsec Extended Tables Module | 10.13.1000 |
| S0E48A #0D1 | HPE Aruba Networking CX 6400 v2 32p SFP28 25G 4p QSFP28 100G MACsec Extended Tables FIO Module | 10.13.1000 |
| S1T83A | HPE Aruba Networking CX 6400 v2 24p Smart Rate 1G/2.5G/5G/10G Class8 PoE 4p SFP56 50G Module | 10.13.1000 |
| S1T83A #0D1 | HPE Aruba Networking CX 6400 v2 24p Smart Rate 1G/2.5G/5G/10G Class8 PoE 4p SFP56 50G FIO Module | 10.13.1000 |

# Important information for 6300 and 6400 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.

Switch fans will run at full speed when a fault is detected with the temperature sensors in the switch. This is normal behavior to ensure overheating does not occur. Should the fans run at full speed at unexpected times, check the output of `show environment temperature` and `show environment fans`, then contact support for further assistance.

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.

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 | 27 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) 6410 Switch Series not supported |

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 6300 and 6400 Switches in AOS-CX 10.14.0001

This section describes the enhancements introduced in this release.

| Category | Description |
|---|---|
| ARP Security | AOS-CX 10.14 supports additional event log messages that allow network admins to see on which port ARP packets are getting dropped when the ARP packets are getting dropped with valid reason. |
| Power Management | The output of the **show running-config** command now displays the details of the power-redundancy configuration. |
| SNMP | The switch can display supported MIBS in RMON commands using the **snmpget** command in the bash shell. |
| SNMP | Rmon entry are increased from 20 to 48 when using the **snmpget** command in the bash shell. |
| EVPN | EVPN routes can be matched against additional **evpn-type** values:<br>▪ evpn-type-2 MAC/IP Advertisement Route<br>▪ evpn-type-3 Inclusive Multicast Ethernet Tag Route<br>▪ 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. |

| Category | Description |
|---|---|
| Overlay Fabric | BGP update-group for VPNv4 routes for optimized BGP processing. |
| Overlay Fabric | Multicast inter-VXLAN L2 bridging support over static VXLAN tunnels. |
| Overlay Fabric | Multicast BUM replication in underlay in a VXLAN overlay fabric design. |
| Overlay Fabric | Multicast anycast RP/MSDP for IPv4 multicast routing in the VXLAN overlay fabric design. |
| Overlay Fabric | EVPN route types [1 to 5] match support in a route-map. |
| 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 | Blocking of unknown multicast packets in a VLAN configured with: IGMP Snooping, MLD Snooping, VXLAN, VSF (6300 Switch series only), VSX (6400 Switch series only) and ISSU (6400 Switch series only). Default behavior is to allow initial flooding; to enable this feature, an explicit configuration command is required. |
| Underlay Fabric | Fix for setting multiple communities and extended communities in a route-map.<br>Ability to set multiple and extended communities per prefix in a route-map used by BGP for both IPv4 and IPv6 address families. |
| Underlay Fabric | Number of PVLAN secondary ports is increased to 48 |
| MACsec | WAN MACsec enhancement to support a custom Ether-Type for EAPoL frames |
| ARC | Fast mode for ARC (Application Recognition and Control)<br><br>Fast Mode: Identifies only application name and category<br>Normal Mode: Identifies application name and category as well as URL and TLS attributes |
| ACLs | Enhancement to reflexive ACL to also support ICMP flows |
| GBP | GBP infrastructure enhancement to support application-based role-to-role policies |
| Containers | Multiple container infrastructure hardening features to increase overall system stability |

| Category | Description |
|---|---|
| Security | ACL support for L3 VXLAN VNI |
| Security | Port-access over LAG for Device Profile now is supported over MCLAG |
| Observability | Traffic insight enhancements to display live and aggregated flows |
| Observability | Support for flow counters (bytes and packets) in the IP Flow table |
| Observability | Support for IP Flow table based IPFIX telemetry for the following features:<br>▪ UBT<br>▪ MAC Lockout<br>▪ Extended Router MAC<br>▪ Source Port Filter<br>▪ IP Lockdown (Rogue Only)<br>▪ VXLAN L3 VNI |
| Observability | Visibility into blocked flows by PAP, GBP, ABP, RACL policies applied on the user role |
| Observability | Visibility into blocked flows dropped by ACLs applied on L2 interface, L2 LAGs, VLANs, and Interface VLANs |
| Observability | IPFIX per VRF export source interface or source IPv4 / IPv6 addresses |
| 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 |
| 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 | Switch hardware and config reset capability using the hard reset button |
| Infrastructure Management and Usability | SNMP read extended interface MIB for reporting |

# Resolved Issues for 6300 and 6400 Switches in AOS-CX 10.14.0001

This section describes the issues resolved in this release.

| Component | Summary | Description |
|---|---|---|
| L3 routes | 207077 | **Symptom:** Traffic convergence takes approximately two minutes when a VSF switchover is performed.<br>**Scenario:** If traffic is flowing through the switch using the uplink on the commander, a VSF switchover causes the standby to become the new commander. It takes approximately two minutes for traffic to resume using the uplink of the new commander.<br>**Workaround:** If the uplink from the VSF is a LAG with members in the Commander/Standby/Member, the convergence time would be lesser and around 70 seconds. |
| Central | 294122 | **Symptom**: Some hpe-restd core dumps may be generated after the switch reboots.This will not interrupt the normal switch operation.<br>**Scenario**: This can occur every time the switch reboots.<br>**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.<br>**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.<br>**Workaround**: Restart the MGMD daemon using the command **systemctl restart hpe-mgmdd**. |
| Physical Interfaces | 224311 | **Symptom**: When parallel detection is enabled, autonegotiating interfaces that are linked with non-autonegotiating interfaces are expected link up at the detected speed, but in half duplex mode. BASE-T ports on AOS-CX switches<br>have parallel detection enabled and are compliant the IEEE 802.3 standard.<br>However, there are some interfaces that are not conforming to this behavior due to hardware limitations.<br>**Scenario**: The following ports have non-conforming parallel detection, or does not have parallel detection enabled.<br>■ JL659A: Ports 1-48, Enabled for 100M but links at full duplex<br>■ JL660A: Ports 1-24, Enabled for 100M but links at full duplex<br>■ JL720A, JL720C: Ports 11-48, Enabled for 100M but links at full duplex<br>■ R0X41A, R0X41C: Ports 1-48, Enabled for 100M but links at full duplex<br>■ R0X42A, R0X42C, S1T83A: Ports 1-24, Enabled for 100M |

| Component | Summary | Description |
|---|---|---|
| | | but links at full duplex<br>▪ R9W95A: Ports 1-24, Enabled for 100M but links at full duplex<br>▪ R9W97A: Ports 11-40, Enabled for 100M but links at full duplex<br>▪ R8Q71A, R8V12A: Ports 37-48, Not enabled (will not link with non-autonegotiating partner)<br>▪ R8S89A: Ports 1-24, Not enabled (will not link with non-autonegotiating partner)<br>▪ R8S90A, R8S91A: Ports 11-48, Not enabled (will not link with non-autonegotiating partner)<br>▪ S0E91A, S0X44A: Ports 1-48, Not enabled (will not link with non-autonegotiating partner)<br>**Workaround**: Enable autonegotiation on the link partner whenever possible to ensure linking up at highest speed. If not possible, you can also explicitly force speed through the **speed 100-full** command in the **interface-config** context to link up with a non-negotiating link partner (assuming the link partner is 100M full duplex). |
| Physical Interfaces | 251722 | **Symptom**: Low throughput is observed on a smart rate interface operating at 100Mbps when connected to third-party device.<br>**Scenario**: Some third-party devices silently drop packets that are sent from the Smart Rate interface that has been negotiated at 100Mbps. This can cause packet retransmission. |
| DNS | 230380 | **Symptom:** The switch experiences high CPU utilization .<br>**Scenario:** High CPU utilization occurs when SNMP invokes DNS resolution, due to access of source IP which causes CPU overhead. |
| Internal srvcs: linux | 273640 | **Symptom:** The ARM kernel Unimplemented Instruction (UI) trap had an error that caused incorrect information to be logged in the rare circumstance of an unhandled UI.<br>**Scenario:** This issue is seen only in the uncommon circumstance of a kernel corruption of the UI. |
| Physical Interfaces | 279303 | **Symptom:** A cable diagnostic test incorrectly reports cables as faulty.<br>**Scenario:** Starting with AOS-CX 10.14.0001, a cable diagnostic test will show output pairs as **open**. |
| BGP | 285540 | **Symptom:** When both IPv4 and IPv6 neighbors are configured in BGP, an SNMP walk displays incorrect information on IPv4 peer sessions.<br>**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 as expected. |
| LLDP | 287305 | **Symptom:** A Client is assigned a role VLAN instead of a Port VLAN ID (PVID).<br>**Scenario:** This issue occurs on a Device-profile client |

| Component | Summary | Description |
|---|---|---|
| | | onboarded with LLDP neighbor info, whenever the user disconnects AP, which is already assigned DP profile, then unplugs the AP and connects the Notebook/Workstation. It received the IP address from the device profile native role assigned VLAN. HOwever, It is supposed to receive the VLAN IP address from the PVID VLAN .<br>**Workaround:** Wait for the LLDP neighbor entry to age out for the device that was unplugged before plugging in a different device to the same port. |
| Slot Management | 289635 | **Symptom:** When a v2 card is replaced with a v1 card in a v2 chassis, the v1 card will not boot up, even if switch is in default profile<br>**Scenario:** A v2 card can have features that are not supported by v1 cards, so slots configured with v2 cards cannot have v1 cards.<br>**Workaround:** Run the command **no module** on the slot, to remove the configuration for that slot and allow the v1 card to be inserted as a new module. |
| Internal srvcs: Security PA infra | 290068 | **Symptom:** The **port-accessd** process crashes and restarts, and a core-dump file is generated.<br>**Scenario:** This issue occurs if a client continuously moves from one port to another port.<br>**Workaround:** Avoid frequently the client between the ports. |
| DHCP Relay | 291742 | **Symptom:** DHCP relay does not change the source IP address of the DHCP discover frame<br>**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.<br>**Workaround:** Use the source interface configuration. |
| MLDv2 | 292078 | **Symptom**: Multiple event logs are triggered with the message **IGMP/MLD internal queue limit exceeded. Needs admin intervention.** IGMP/MLD protocol join messages are missing, leave messages are not getting processed, and querier information is not learned.<br>**Scenario:** This issue can occur when VxLAN is set up without IGMP/MLD running on a few VLANs associated with VNI, when multicast control packets are coming in continuously through the VLAN without IGMP/MLD.<br>**Workaround**: Enable IGMP/MLD snooping on all the VLANs where multicast clients are sending IGMP/MLD control packets. |
| Physical Interfaces | 292703 | **Symptom:** Some client network cards can only negotiate 100M<br>**Scenario:** When a client device connects to a smart-rate port, some devices with 1Gbps NICs can only negotiate a link speed of 100Mbps. |
| Port-Access Policy | 295644 | **Symptom**: Traffic loss occurs on the switch, where RADIUS responses or other traffic on the switch gets dropped, and new clients do not get onboarded.<br>**Scenario**: When all ABP/Refliexive ACL clients log off or age out, the switch can start dropping the traffic.<br>**Workaround**: Enable a group-based policy (GBP) on the |

| Component | Summary | Description |
|---|---|---|
| | | switch. |
| BGP | 295703 | **Symptom**: When the **show bgp vrf info** command is run, the , vtysh session is logged out.<br>**Scenario:** This issue occurs when VRF is configured with export RT (Route Target).<br>**Workaround:** Use the command **show running-config vrf** to prevent the vtysh session from logging out. |
| CaptivePortal | 296004 | **Symptom:** When a captive-portal profile is configured and multiple clients use the Chrome browser to open the login page at the same time, the Chrome browser displays the error **404: page not found**.<br>**Scenario:** The issue can occur only when approximately 20 Windows clients try to open re-direct URL login page at the same time from the Chrome browser. T<br>**Workaround:** Refresh the Chrome Web page. |
| RADIUS Port-Access | 296010 | **Symptom**: The port-access daemon crashes continually.<br>**Scenario**: This issue occurs if the RADIUS server is added user server group without configuring a group priority via REST or the Aruba Fabric Composer<br>**Workaround**: Use the switch CLI to add a server to the user group or pass the user priority along with group using the REST interface. |
| Internal srvcs: Security PA infra | 297755 | **Symptom:** Traffic to existing clients on VLAN would stop if a new client is seen on an auth-enabled port with the switch's system MAC.<br>**Scenario:** If a packet with switch's system MAC address as a source MAC is received on a auth-enabled port, the traffic to existing clients on same VLAN would stop.<br>**Workaround:** Interface VLAN has to be disabled and then reenabled for the traffic to existing clients to resume. |
| LEDs - Buttons | 297812 | **Symptom:** Port LEDs remain off even when link is established and traffic is flowing.<br>**Scenario:** This issue can occur if the **no module** command is issued on a line card.<br>**Workaround:** Check the CLI for link status and health, as the CLI can deliver the same information provided by the port LEDs. |
| Power Management | 298124 | **Symptom**: The power-redundancy configuration was not displayed in the output of the **show running-config** command.<br>**Scenario**: This issue occurs when running the **show running-config** command.<br>**Workaround**: The power-redundancy configuration can be checked with the command **show environment power-redundancy**. |
| WebUI | 299012 | **Symptom** : *script-src: 'unsafe-inline'* does not allow the Content-Security-Policy feature to work as intended.<br>**Scenario** : Using this script allows inline scripts to be executed by client browsers.<br>**Workaround** : The script should be moved into files called by functions. |

| Component | Summary | Description |
|---|---|---|
| IGMP | 299447 | **Symptom:** When IGMPv3 Snooping is enabled, IGMP groups are not pruned when a multicast client sends an IGMP Leave message.<br>**Scenario**: When a client sends an IGMP Leave message, the switch should forward it to the IGMP Querier, which should then respond with an IGMP Group-Specific Query (GSQ) for the group. The switch should then send the GSQ out of all ports associated with the group and reset the group's expiry timer to the Last Member Query Internal. However, in some cases, the expiry timer is not reset after sending the GSQ, causing the group to continue functioning on the port until the Group Membership Interval timer expires.<br>**Workaround:** Switch to IGMPv2 Snooping, and consider enabling IGMP Fast Leave on the port if it's only connected to one multicast client. |
| VSX-Sync | 299838 | **Symptom**: An Interface VLAN configuration is not getting synced to secondary switch.<br>**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.<br>**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.<br>**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.<br>**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. |
| Internal srvcs: Security PA infra | 301734 | **Symptom:** A role assigned by CoA gets overridden by low-priority methods, such as a RADIUS assigned role.<br>**Scenario:** This issue occurs on a switch with the default auth-priority on port ifyou configure both mac-auth and dot1x and assign a role from RADIUS on successful mac-auth authentication and concurrent on boarding. While dot1x is in authenticating state, if you assign a different role RADIUS using CoA, you can observe that role assigned by CoA gets overridden by the RADIUS-assigned role (during mac-auth success)<br>**Workaround:** Remove concurrent onboarding. |
| RADsec | 308854 | **Symptom**: Client authentication failures can occur, and packets sent to a RADIUS server are timed out by the switch.<br>**Scenario**: In some scenarios when the RADSec server connection is lost and restored while multiple port-access users are authenticated to the RADIUS server the switch |

| Component | Summary | Description |
|---|---|---|
| | | might incorrectly time out the RADIUS packets.<br>**Workaround**: Unconfigure and reconfigure the RADSec server. |
| SNMP | 303650 | **Symptom**: The snmpd process crashes and SNMP polling stops for a few seconds.<br>**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. |
| SW-Diagnostics | 311012 | **Symptom**: High storage utilization in observed in the file system, preventing the copying of support files.<br>**Scenario**: Logs from various daemons are continuously generated and stored in multiple chunk files (for example, critical.gz, messages.gz) in the /fs/logs/boot/ directory. This leads to high storage utilization and prevents the copying of support files due to high memory usage.<br>**Workaround**: Instead of using file mode support file collection, utilize directory mode support file collection. |
| ASIC SDK - HPE | 303760 | **Symptom:** A line module failed and the switch displayed the error code **Line module 1/5 has failed: Fatal agent crash**.<br>**Scenario:** When Energy Efficient Ethernet is enabled on the peer device, an interrupt is triggered that causes the switchd agent to crash.<br>**Workaround:** Disable EEE mode on all peer devices. |
| User Based Tunnel | 304277 | **Symptom:** A User-Based Tunnel (UBT) will be upon the switch, clients will be authenticated and user tunnels will be present, but users will be not be able to communicate.<br>**Scenario:** This issue occurs during VSF switchover, when the standby is replaced with new standby.<br>**Workaround:** Disable and reenable the UBT zone. |
| ACL | 305843 | **Symptom:** The switch reloads unexpectedly during a firmware update<br>**Scenario**: When upgrading the switch firmware to a later build, the switch might reload while parsing an Access List (ACL) configuration.<br>**Workaround**: Before updating the switch, run through the following alternative process:<br>▪ Save the full configuration as a checkpoint using the command **copy running-config checkpoint <name>**.<br>▪ Remove all access-list configurations, then save the configuration as the startup configuration using the command **copy running-config startup-config**.<br>▪ Upgrade the switch as usual.<br>▪ Once the switch is upgraded, move the ACLs back to the running configuration by copying the saved checkpoint to the running configuration using the command copy checkpoint <name> running-config |
| CX-Licensing | TMA-4234 | **Symptom:** The switch advanced feature pack shows as expired. |

| Component | Summary | Description |
|---|---|---|
| | | **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<br>**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 |
|---|---|
| User Based Tunnel | The switch does not support double encapsulation. A packet can be encapsulated with either L2GRE (UBT) or VXLAN, but not both. The network admin should decide the tunneling type to be used, and then plan the configuration accordingly. |
| User Based Tunnel | In the event of license issues when onboarding an DUT to primary or backup mobility conductor, the DUT will not try to bootstrap to other mobility conductor where a license is available. For example, if a mobility conductor<br>▪ does not have a have license to on-board the DUT but mobility conductor.<br>▪ does have adequate licenses, if both mobility conductors are reachable then UBT will be down, and the DUT will not attempt to bootstrap to the backup controller. However, if the primary mobility conductor is not reachable, the DUT gets tunneled to the standby/backup mobility conductor. Once the primary mobility conductor reachable by the DUT once again, the DUT will not automatically bootstrap back to the primary. Network administrators should manually disable and enable UBT on the DUT to re-establish the tunnel to the primary mobility conductor. |
| 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. |

| Feature | Description |
|---|---|
| VXLAN | VXLAN encapsulation does not copy the ECN bits from inner header to outer header. If you create a traffic stream between connected hosts and enable the ECN bit for the hosts and start the traffic, a traffic capture may show that ECN bits arent copied from the inner header to the outer header. |
| 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. |
| ACLs | **NOTE:** Applies only to the Aruba 6300 Switch Series.<br><br>In a VSF stack, the switch may fail to log events for the matching access-list entries. ACL functionality is not impacted; access-list entries are applied properly and only the logging is incorrectly generated. |
| Aruba CX Mobile App | VSF stack formation is blocked when there are reserved autojoin interfaces (25, 26, 49, 50) in the stack topology. |
| 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:<br><br>`!`<br>`route-map rmap permit seq 10`<br>`  set local-preference 50`<br>`!`<br>`router bgp 100`<br>`  vrf red`<br>`  neighbor 1.1.1.2 remote-as 100`<br>`  address-family ipv4 unicast`<br>`  neighbor 1.1.1.2 activate`<br>`  neighbor 1.1.1.2 route-map rmap in`<br>`  exit-address-family`<br><br>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:<br><br>`router bgp 1`<br>`neighbor 1.1.1.1 remote-as 2`<br>`address-family l2vpn evpn`<br>`neighbor 1.1.1.1 activate`<br>`neighbor 1.1.1.1 next-hop-unchanged` |

| Feature | Description |
|---|---|
| | `neighbor 1.1.1.1 send-community extende`<br>`exit-address-family` |
| 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. |
| Counters (6400 only) | Bytes/errors/drops count in **show interface *<IF-NAME>*** and **show interface *<IF-NAME>*** queues can have up to 10% deviation. This will manifest mainly when running at line rate with small packet sizes and after a port goes up/down. |
| Counters (6400 only) | The "Bytes" counter is not supported in **show interface *<IF-NAME>*** queues output. |
| DHCP Server, DHCP Relay, and DHCP Snooping | DHCP Relay and DHCP Snooping can co-exist on the same switch.<br>DHCP Snooping and DHCP Server cannot co-exist on the same switch.<br>DHCP Snooping, DHCP Relay, and DHCP Server together 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. |
| Flow control (6400 only) | Flow control is not supported. |
| 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 only software forward at a rate of 100pps if the packets that trigger 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. |
| Line module Hot Swap and Reboot (6400 only) | Concurrent physical hot insert/removal or reboot of a line-module is not supported. Subsequent insert/removal or reboot of a line-module must be initiated only after preceding attempts have been completely processed by the system.<br>For hot insert you must wait until the preceding line-module has reached the "ready" state before inserting subsequent line-modules. For hot removal you must wait until the line-module is no longer present in the system. See the CLI command **show module** for line-module status information.<br>Aruba recommends line-modules be gracefully shut down before removal. Use the CLI config command **module *<SLOT-ID>* admin-state [diagnostic \| down \| up]** to change the administrative state of the line-module.<br>Line module reboot and hot removal is not a hitless operation. Up to 2 seconds of traffic loss may be expected when any module is rebooted or |

| Feature | Description |
|---|---|
| | removed from the system. Hot insert does not result in any traffic loss. |
| MACsec | In an environment with a Cisco device, the Cisco device must be designated as the key server. Designating the AOS-CX as the key server results in complete traffic loss. |
| MACsec | In an environment with Cisco and FlexFabric or H3C devices, do not update confidentiality-offset on the live channel. There can be complete traffic loss for an extended period on the MACsec channel when confidentiality-offset is updated on both ends. |
| MACsec | MACsec uses a software-based implementation to track start and stop times for secure channels and secure associations. As the implementation is software-based, the stop times for MACsec secure channel and secure associations are only updated when they are deleted and therefore never updated in the output of the **show macsec status detailed** command. |
| MACsec and UDLD | In an environment with devices running AOS-Switch, do not enable UDLD on the same link. The UDLD session can toggle between up and down continuously when both MACsec and UDLD is enabled on the same link. |
| MACsec | In an environment with Cisco devices, when the GCM-AES-XPN-128 or GCM-AES-XPN-256 cipher suite is used for establishing the MACsec channel, the MKA policy on the Cisco device must be configured with **ssci-based-on-sci**. |
| MACsec | MACsec works between a CX device and a Windows VM running AnyConnect with AES-128 cipher. AnyConnect does not support AES-256 in the NAM module (works only for the VPN module). |
| MACsec | When Cisco AnyConnect is used as dot1x supplicant, it is recommended to configure cak-length to be 16 under dot1x-authenticator mode. |
| MACsec | Ensure the cipher suite **GCM-AES-128** is configured when AOS-CX is acting as a key server. This is because, by default AOS-CX will use the most secure cipher suite **gcm-aes-xpn-256** for establishing MACsec secure link and Comware/PVOS doesn't support an XPN cipher suite. |
| Multicast and VXLAN | ▪ VXLAN must be configured prior to configuring VSX.<br>▪ IPv6 multicast is not supported for VXLAN overlay.<br>▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details. |
| Priority queues (6400 only) | A maximum of four (4) priority queues is supported. |
| RADIUS | Authorization by means of HPE VSAs is not supported. |
| Reduction in TCAM entries (6400 only) | On some line cards, a small number (~200) of TCAM entries are used for internal purposes. |
| 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+. |
| RIP/RIPng | RIP/RIPng metric configuration support is not available. |

| Feature | Description |
|---|---|
| SFTP | When the path to the SFTP server crosses segments with different MTU frame sizes, file transfers will fail. Configure the same MTU on all nework segments on the path to the SFTP server to use SFTP to transfer files. |
| Sub-interface | BFD is not supported on a sub-interface. A sub-interface as underlay for EVPN-VXLAN is not supported |
| Tunnels | When configuring tunnels (VXLAN/IP tunnels) with the underlay as a static route, the next-hop IP should be an SVI or ROP IP and not configured as the Active-Gateway. |
| 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. |
| PTP | *(6300 Switch Series only*)<br>End clients offset might be slightly high when using PTP Default profile 1588v2 with default PTP parameters (1 PPS) |

# 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 |
|---|---|---|
| TFTP | 269619 | **Symptom**: TFTP Software image upload/download transfer operation fails.<br>**Scenario**: Downloading/uploading the software Image via sm ubuntu IPv6 TFTP server fails.<br>**Workaround**: Use the **blocksize** option in the copy command with a blocksize of 1375 or less. For example :<br>`copy tftp://[20:1::100];blocksize=1375/image.swi secondary vrf vrf1` |
| MACsec | 240672 | **Symptom**: Traffic is dropped for a few seconds on a MACsec channel during a VSF switchover.<br>**Scenario**: When the MACsec channel has data-delay protection enabled, there can be |

| Category | Bug ID | Description |
|---|---|---|
| | | traffic drops for a few seconds on the channel post a VSF switchover due the reset of the MKA session on the interface.<br>**Workaround**: Do not use data-delay protection in a MACsec policy if the system is deployed as a VSF stack. |

# 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*.

Due to an image size issue, a one-step upgrade from some versions of AOS-CX using the WebUI is not supported. This limitation only affects upgrades performed using the switch WebUI, and does not impact upgrades performed using the command-line interface or Aruba Central.

**Upgrades requiring two steps:**

| Original Release | Intermediate Upgrade Release | Final Upgrade Releases |
|---|---|---|
| 10.09.0001 - 10.10.1010 | 10.11.xxxx release | 10.14.xxxx |

**Upgrades requiring one step:**

| Original Release | Final Upgrade Release |
|---|---|
| 10.11, 10.12 or 10.13 | 10.14.xxxx |

For 6400 only: For information about supported In Service Software Upgrade (ISSU) paths and detailed ISSU upgrade information, refer to https://networkingsupport.hpe.com/issu.

## 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, FL.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.

## Hardware updates

The 6400 switch series chassis hardware images may have a different upgrade sequence if programmable device updates are pending that require a power cycle. To determine if there are pending upgrades:

1. Issue the command **show needed-updates [next-boot [primary|secondary]]** and check the output of the command see if it indicates that one or more devices need to be updated.
2. Issue the command **show needed-updates [primary|secondary]** and check the output to see which updates are required for the current switch image.
3. Issue the command **allow-unsafe-updates <NUM_MINUTES>** if any non-failsafe device such as an icbbp_secondary needs to be updated.
4. Issue the command **show fabric** and **show module** repeatedly until the output of this command shows that all modules are in the **Ready** state.
5. Perform a manual chassis power-cycle. If no remote power control is available, physically unplug all the power cables wait at least ten seconds, and plug the power cables back in. This is the only way to clear the write-protection security set on the switch hardware.
6. Wait for the chassis to reboot, and log in to the command-line interface as an admin user (or with an account with similar privileges).
7. Issue the command **show fabric** and **show module** repeatedly until the output of this command shows that all modules are in the **Ready** state.
8. Issue the command **show needed-updates**.
9. If the output of the command **show needed-updates** doesn't report any further needed updates or other issues such as a needed power-cycle, then the switch update is complete.
10. However, if icbbp_primary was updated since the last chassis power-cycle, you wimay ll need to repeat this process and perform a second power cycle, to get the newly-updated switch image.

## 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.