AOS-CX 10.13.0005 Release Notes

9300 Switch Series

November 2023
Edition: 1

Notices

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

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

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

Acknowledgments

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

Chapter 1
AOS-CX 10.13.0005 release notes

Products Supported

This release applies to the 9300Switch Series. The following table lists any applicable minimum software versions required for that model of switch.

NOTE

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

Product number	Product name	Minimum software version
R9A29A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Front-to-Back 6 Fans 2 AC PSU Bundle	10.10.1000
R9A30A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Back-to-Front 6 Fans 2 AC PSU Bundle	10.10.1000
R8Z96A	Aruba 9300-32D 32-port 100/200/400G QSFP-DD 2-port 10G Switch	10.10.1000

Important information for 9300 Switches

NOTE

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

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

NOTE

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

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

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

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

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

AOS-CX 10.13 is a Long Supported Release (LSR).

- LSRs are long lived releases where Aruba will introduce new features and new hardware, and park hardware (that is, this may be the last major release supported) as needed.
- LSRs are be maintained and supported for 5 years (i.e., Initial Release + 5 years)
- Initial Release to End of Maintenance (EOM*): Bug and vulnerability patching with releases reducing in frequency over time.
- EOM to End of Support (EOST): Vulnerability patching on an as needed basis for High or Critical CVSS issues.

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 10.13.xxxx	AOS-CX 10.10.0002
AOS-CX 10.12.xxxx	AOS-CX 10.09.0002
AOS-CX 10.11.xxxx Note: 10.11 is an SSR, recommended release is 10.11.0001	AOS-CX 10.08.0001

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

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

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open-source licenses. A complete machine-readable copy of the

source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

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

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

Version history

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

Version number	Release date	Remarks
10.13.0005	14/11/2023	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)

Internet Explorer is not supported.

Recommended versions of network management software for switches found in this release note:

Management software	Recommended version(s)
NetEdit	2.9.0
Aruba Central	2.5.7
Central On-Premises	2.5.6.4

Management software	Recommended version(s)
Aruba Fabric Composer	Support coming in future release.
Aruba CX Mobile App	Support coming in future release.

NOTE

For more information, see the respective software manuals.

NOTE

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

Enhancements

This section describes the enhancements introduced in this release.

Enhancement	Description

PKI	In previous releases, under a certificate configuration context, the key-size or curve-size is a mandatory keyword following a key-type, even when the key-size to configure is the default value. For example:
	`(config-cert01)# key-type rsa key-size 2048`
	`(config-cert01)# key-type ecdsa curve-size 256`
	Starting with AOS-CX 10.13, when the key-curve-size to configure is the default value, the key-size/curve-size keyword is optional and may be omitted. For example, this command
	`(config-cert01)# key-type ecdsa`
	Is equivalent to:
	`(config-cert01)# key-type ecdsa curve-size 256`
	And this command:
	`(config-cert01)# key-type rsa`
	Is equivalent to:
	`(config-cert01)# key-type rsa key-size 2048`

Rate Limiting by Percentage	Enables the use of percentages based on link speeds with rate-limiting.

Enhancement	Description
CISCO VSA Support	Enables the processing of the COA requests with Cisco VSA from Cisco ISE-ANC.
CX feature pack subscriptions	AOS-CX 6300, 6400, 8xxx, 9300, and 10000 Switch series running AOS-CX 10.13 or later support optional add-on feature packs that enhance the base AOS-CX operating system. Depending upon the requirements for their networks, network administrators may choose to purchase a subscription for these features that provide enhanced traffic visibility and troubleshooting, and support advanced security.
NTP v6 on an overlay	Provides support for NTPv6 in VXLAN overlay networks with both IPv4 and IPv6 underlay
OSPF distribution list	Supports the ability to filter OSPF routers from being installed into the forwarding information base (FIB) and to filter redistributed routes from other protocols.
Server certificate validation	In previous releases, when a certificate is validated, the event log does not indicate what CA certificate was used to validate the certificate. A new event is added to this release to provide the CA certificate information.
Bidirectional PIM	Bidirectional PIM (BIDIR-PIM) is a variant of PIM that builds bidirectional shared trees connecting multicast sources and receivers. BIDIR-PIM Mode can be configured on physical ports, VLAN interfaces, LAG interfaces, and loopback interfaces.
Queue shaper for All queue types	Enables shaping feature on all queue types (GMB, WFQ and DWRR) in addition to the legacy support for strict priority queues
Routemap support to redistribute host-routes to BGP/OSPF	Enables the addition of route-maps to filter host-routes being redistributed into OSPF/BGP.
IPv6 Response Source for SNMP	An IPv6 source interface can be used for all SNMP communications.
SNMPv3 SHA256, AES256 Support	Support for AES128, AES192 and AES256 and SHA224, SHA256,SHA384 and SHA512
SNMP OIDS for L3 Route details	The feature enables the OIDS ipNetToMediaTable and ipAdEntAddr for manageability through Solarwinds
VRRP: Support for IPv6 Link Local	Allows the same IPv6 Link local address to be configured as VIP on multiple Interfaces
VXLAN PBR on L3VNI	Policy-based routing (PBR) can be applied over a VXLAN on a L3VNI for symmetric IRB deployments
WebUI	Hot patch software can be uploaded using the switch WebUI.

Resolved Issues

This section describes the issues resolved in this release.

Category	Bug ID	Description
Internal srvcs: pspo	267398	**Symptom**: VXLAN tunnels go down after removing interfaces with IPv6 address that are the same as the VXLAN VTEP IP addresses. **Scenario**: In an EVPN-VXLAN deployment with an IPv6 tunnel, if any interface (irrespective of the VRF) that has same IP address as the tunnel source IP, it goes down, and then the tunnel interface is brought down **Workaround**: Unconfigure loopback and VXLAN and re-configure them.

BGP	285425	**Symptom**: Aruba Central and NetEdit are unable to synchronize new configuration changes to a switch. Aruba Central MultiEdit will display a warning message like the following:
		`neighbor 1.1.1.1 remove-private-AS]`
		`Incomplete command or invalid parameters`
		A device validation failure will display a message like the following:
		`Neighbor 1.1.1.1 does not exist`
		Scenario: A configuration synchronization failure will occur when using NetEdit or Aruba Central MultiEdit to modify a switch configuration that has the BGP configuration **neighbor remove-private-AS** in the current running-config.
		Workaround: Manually configure the switch from the switch command-line interface.

SNMP	285540	**Symptom**: If both IPv4 and IPv6 neighbors are used while configuring BGP. SNMP walk displays IPv4 in addition to other entries. **Scenario**: This issue can occur if a user configures both IPv4 and IPv6 neighbors. IPv4 data displays properly and some extra entries are getting added due to IPv6.
PKI	283686	**Symptom**: When an X509 certificate profile configuration with an EST profile association is pushed to a switch, it can trigger EST enrollment two times, causing the EST server to issue two certificates to the switch. **Scenario**: This issue has no functional impact, because only the latest enrolled certificate will take effect.
SNMP	281792	**Symptom**: A desired source IP address is not seen when inform packets are received by the inform receiver. **Scenario**: This issue occurs when a user sets a source IP address for traps.
PKI	281380	**Symptom**: When a certificate is validated, the event log did not indicate what CA certificate was used to validate the certificate. A new event is added to this release to provide the CA certificate information. **Scenario**: This issue occurs when validating an Aruba Central server certificate.
Boot Process	279046	**Symptom**: A firmware upgrade from Central will fail. **Scenario**: This issue occurs when switch's connection to the internet is configured using the command **ip source-interface http** or **ip source-interface all**. **Workaround**: Configure the switch to connect to the internet without using an ip source interface.
WebUI	279019	**Symptom**: After uploading an invalid PER certificate, the hpe-restd process becomes unstable, the WebUI temporarily stops responding, and all REST API calls from the WebUI fail. **Scenario**: If a user uploads a corrupt PEM certificate file using WebUI certificate management window, selecting the **Upload** button in the WebUI causes the WebUI

Category	Bug ID	Description
		to stop working completely. To recover from this state, restart hpe-restd from the bash prompt in the comand-line interface or restart the switch. **Workaround**: Use the CLI to upload certificates.
Internal srvcs: Security PA infra	278954	**Symptom**: Clients are onboarding with an incorrect auth-priority order. Users onboarded with a lower-prority authentication method, so higher-priority authentication requests werenot seen. **Scenario**: When concurrent onboarding is enabled with a default authentication priority and non-default auth-precedence on a port, clients onboarding are taking the wrong auth-priority. **Workaround**: At the issue state, reconfigure the auth-priority on the port to onboard the clients.

*QoS	275060	**Symptom**: If a REST customer configures ingress rate-limiting on a port such that there is a combination of pps-mode and percentage-mode limits, an error message will show up in the log output. For **show events**,
		`2023-09-16T23:45:37.600529+00:00 8325 ops-switchd [3846]:Event|5702|LOG_ERR|AMM|1/1|QoS error: Interface 1/1/8 rate-limit not applied,due to unit-type conflict. All rate limits for an interface must use the same units, either pps or percent.`
		Via /var/log/messages:
		`2023-09-16T23:45:37.600361+00:00 8325 ops-switchd [3846]: debug|LOG_ERR|AMM|-|QOS|QOS_CONFIG_PORT| Interface 1/1/8 rate-limit not applied, due to unit-type conflict.All rate limits for an interface must use the same units, either pps or percent.`
		`2023-09-16T23:45:37.600463+00:00 8325 ops-switchd [3846]: debug|LOG_ERR|AMM|-|QOS|QOS_ASIC_PORT|Port 29 rate limiting has both pps and percentage units, which cannot be combined`
		NOTE: This is only an issue when rate-limiting configurations on a single port have different rate units. Mixing pps and percent configurations across different ports is fine.
		Scenario: If there was a previous, valid rate-limit configuration on the port, it will remain in hardware and will be displayed in the **show int** output. This is because port rate-limiting is also used as a security feature, so we do not remove a valid configuration in favor of a bad configuration in which no new rate-limit settings can be put in HW.
		Workaround: Either remove or adjust rate-limiting on the affected port so that there is either no configuration, or ensure the rate-limit entries in the configuration all use the same unit type (pps or percent). If you reboot the switch without fixing the conflicting configuration, then no rate-limit entries for that port are programmed in hardware after bootup.

BGP	274060	**Symptom**: Traffic loss occurs for some BGP learned networks. **Scenario**: When BGP route is relearned due to connected BGP peer having a network event like a port link flap. some BGP routes failed to get programmed in the hardware. **Workaround**: Add a static route for failed BGP route.

Category	Bug ID	Description
PKI	272227	**Symptom**: The **hpe-restd** process crashes unexpectedly. **Scenario**: Rare timing issues occur during the initialization and teardown phases of certificate validation requests from multiple modules, potentially leading to crashes in the REST daemon.2
VLANS	271762	**Symptom**: A user is ogged out of the CLI session after executing "show vlan" command. **Scenario**: This issue can occur of a user issues the **show vlan** command on the switch that has **interface persona** configured. **Workaround**: Remove the interface persona configuration if it is not required.
CLI infra	269871	**Symptom**: The system-socket proxyd process utilizes a high level of CPU resources. **Scenario**: 100% CPU utilization is observed when user leaves a vtysh console waiting at a user-input or page-prompt. **Workaround**: Provide input at page-break or stop the vtysh process.
WebUI	269716	**Symptom**: Graphs for Analytics may display unexpected variations after refreshing. **Scenario**: This may occur when refreshing a Network Analytics Engine (NAE) Graph using a larger temporal window.
Sflow	269486	**Symptom**: The counter stats may display 0 packets for some interfaces. A short while later, when interface stats are retrieved again in the subsequent cycle, the value is displayed as expected. **Scenario**: The problem is sporadic. However, this problem can arise when the statistics from the interface table are retrieved slowly.
VXLAN	267398	**Symptom:** VxLAN tunnels go down after removing interfaces with an IPv6 address which is same as the VXLAN VTEP IP. **Scenario:** In a EVPN-VxLAN setup with an IPv6 tunnel, if any interface that has same IP address as the tunnel source(regardless of the VRFp goes down thenthe tunnel interface is also brought down **Workaround**: Unconfigure and then reconfigure loopback and the VXLAN.
webUI	265798	**Symptom**: When NAE graphs refresh automatically, a user may see a lot of variations in graph rendering. **Scenario**: NAE graphs have a window of ten days; when the display refreshes to the next window, the user could experience variations in graph rendering, including graphs incorrectly depicting CPU utilization spikes up to 100%.
TPM	265125	**Symptom**: Failure to establish or maintain a connection to Aruba Central **Scenario**: A switch may fail to establish or maintain its relationship with Aruba Central. In these cases, the switch may display the error **{_}Central source connection status" field in the "show aruba-central" command will read "connection_failure"{_}** . **Workaround**: Issue the following commands in order: ▪ start-shell ▪ sudo bash ▪ systemctl restart_jitterentropy-rngd ▪ exit ▪ exit ▪ show aruba-central

Feature Caveats

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

Feature	Description
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.
Classifiers	For Classifier policy modifications to be secure, Aruba strongly encourages modifications be done as a three-step process: Bring down the port, modify, and bring the port back up.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
IGMP/PIM on 6-in-6, Loopback and GRE interfaces	IGMP cannot be enabled on either Loopback or GRE interfaces. IGMP and PIM is not supported on a 6-in-6 Tunnel.
Multicast and VXLAN	▪ VXLAN must be configured prior to configuring VSX. ▪ IPv6 multicast is not supported for VXLAN overlay. ▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details.
PFC	Priority-based flow control (PFC) is not supported on a split port.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
Traceroute	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).

Known Issues

There are no known issues in this release.

Upgrade information

AOS-CX 10.13.0005 uses ServiceOS CL.01.12.0002.

CAUTION

Each VSX switch in a pair must run the same version of AOS-CX. If a primary VSX switch is upgraded to 10.10.xxxx, the secondary VSX switch must be immediately upgraded to that same version. If the ISL link is disabled and enabled on VSX switches that are running different versions of AOS-CX, a VSX secondary switch running an older version of AOS-CX may be unable to synch information from the VSX primary, which can cause the port state to become blocked and lead to traffic loss.

NOTE

Do not interrupt power to the switch during this important update.

Manual configuration restore for software downgrade

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

1. Use the **show checkpoint** command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the **Image Version** column in the output of the command, for example, CL.10.xx.*yyyy*).

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

Performing the 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 10.13 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.10.12.1000]
2. Secondary Software Image [xx.10.13.0001]

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 2017-2023 Hewlett Packard Enterprise Development LP

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

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

switch login:
```

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

Chapter 2
Other resources

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

- AOS-CX switch software documentation portal: https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
- AOS-CX 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.