AOS-CX 10.11.1010 Release Notes

10000 Switch Series

a Hewlett Packard Enterprise company

Published: May 2023

Open Source Code

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
6280 America Center Drive
San Jose, CA 95002
USA

Notices

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

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

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

Acknowledgments

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

Chapter 1
AOS-CX 10.11.1010 release notes

Products supported

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

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

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

Important information for 10000 Switches

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

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

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

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

To upgrade to:	Your switch must be running this version or later ***
AOS-CX 10.11.xxxx Note: 10.11 is an SSR, recommended release is 10.11.10xx	AOS-CX 10.08.0001
AOS-CX 10.10.xxxx Note: 10.10 is an LSR, recommended release is 10.10.10xx.	AOS-CX 10.06.0110

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

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

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

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

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

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

Version history

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

Version number	Release date	Remarks
10.11.1010	2023-03-28	Released, fully supported, and posted on the Web.
10.11.1005	2023-03-03	Released, fully supported, and posted on the Web.
10.11.0001	2022-11-30	Released, fully supported, and posted on the Web.

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	56
Safari (MacOS)	12
Safari (iOS)	10 (Version 12 is not supported)

Internet Explorer is not supported.

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

Management software	Recommended version(s)
AirWave	8.2.15.0
NetEdit	2.6.1
Aruba Central	Support in an upcoming Central upgrade (to be announced).
Pensando Policy and Services Manager (PSM)	v1.54.2-T
Aruba Fabric Composer	6.4.1
Aruba CX Mobile App	2.7.9 (or later)
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40

For more information, see the respective software manuals.

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

Enhancements

This section lists enhancements added to this branch of the software.

For a list of enhancements in previous releases, refer to the AOS-CX Release Notes Portal.

The number listed with the category is used for tracking purposes.

Enhancements for 10000 Switches in AOS-CX 10.11.1010

Category	Description
Flow Control	The **flow-control rxtx [pool <1-3>] override-negotiation** command is introduced to to pause flow control in the event that link partners (such as 25G DACs connected to NICs) do not correctly negotiate with the switch. ■ The **[pool <1-3>]** parameter is supported only if LLFC transmission is configured along with the **pool** setting ■ A reboot is not required for this config to take effect, however this command will cause the affected link will shut down and restart.

Resolved Issues

This section lists fixes found in this branch of the software. The **Symptom** statement describes what a user might experience if this issue is seen on the network. The **Scenario** statement provides additional environment details and trigger summaries. When available, the **Workaround** statement provides a workaround to the issue for customers who chooses not to update to this version of software.

For a list of issues resolved in previous releases, refer to the AOS-CX Release Notes Portal.

The Bug ID is used for tracking purposes.

Resolved issues for 10000 Switches in AOS-CX 10.11.1010

Category	Bug ID	Description
BGP	245472	**Symptom**: When BGP neighbors of an l2vpn EVPN family is changed from dynamic BGP peering to static bgp peering using checkpoint, the sessions get stuck in Idle state. **Scenario**: Static BGP l2vpn EVPN peers are configured and saved as checkpoint. That is removed and dynamic BGP l2vpn EVPN peering is configured. Now when static BGP l2vpn EVPN peering is brought back by using first checkpoint, the session is stuck in an idle state. **Workaround**: Remove and re-add the configuration manually.
BGP	257729	**Symptom:** Am SNMP walk for bgpPeerRemoteAddr returns a random IP address for peer groups. **Scenario:** This issue occurs when the BGP peer group is configured.
Flow Control	258205	**Symptom:** The link partner does not negotiate flow control even when the link supports auto-negotiation. Hence, no flow control is applied on the local interface. **Scenario:** This issue occurs when the link partner does not advertise a flow control mode that is different than what is configured on the local interface of a link that supports auto-negotiation. **Workaround:** The flow-control override-negotiation functionality can be used to pause flow control if the link partners do not correctly negotiate with the switch. The flow-control override-negotiation functionality works only when the link technology supports negotiation of flow control.

Feature caveats

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

Feature	Description
PIM-SM	Pim Active-Active not supported on overlay VXLAN SVIs.
BGP	If a route-map is applied and none of the routes satisfy the match condition(s) in any of the route-map entries, then all routes are dropped.
SNMP	If SNMP is enabled via the switch CLI, it can take between 1-2 minutes for the SNMP daemon to be ready to respond to requests. If a local or external SNMP MIB walk is performed in the interval between when SNMP is first enabled and the SNMP daemon is ready, the MIB walk action will return an error.
Certificates	When a switch uses a certificate with a legacy certificate name that is not supported in 10.11 because it contains disallowed characters, the information will migrate properly in the upgrade, but that certificate can no longer be edited. For new certificate names, only alphanumeric characters, dots, dashes, and underscores are allowed.
Config Mgmt	Configurations in JSON format may not be successfully imported from a previous release as a result of schema changes between software releases.
Port Access	Port-access (802.1x, MAC authentication, Device Profile), Port-security and/or DHCP v4/v6 snooping configurations are mutually exclusive with PSM stateful firewall policies.
Subinterfaces	BFD sessions are not supported on sub interfaces. Use a switch virtual interfaces (SVI) to configure a BFD session.
Stateful L4 Firewall	Port-access (802.1x, MAC authentication, Device Profile), Port-security and/or DHCP v4/v6 snooping configurations are mutually exclusive with PSM stateful firewall policies
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.
Stateful L4 firewall	For locally-switched and routed flows on the switch, the traffic from the host is subject to policy processing only once and only egress policy is enforced on the traffic egressing the workload and entering the switch.
Stateful L4 firewall	Stateful services for VRFs, where route leaking is enabled, are not supported.
Stateful L4 firewall	Port-access (802.1x, MAC authentication, Device Profile), Port-security and/or DHCP v4/v6 snooping configurations are mutually exclusive with PSM stateful firewall policies.

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`

Feature	Description
	neighbor 1.1.1.1 send-community extended exit-address-family !
Classifiers	Classifier policies, IPv6 and MAC ACLs are not supported on egress.
Classifiers	Egress ACL logging is not supported.
Classifiers	For Classifier policy modifications to be secure, Aruba strongly encourages modifications be done as a three-step process: Bring down the port, modify, and bring the port back up.
Classifiers	IPv4 egress ACLs can be applied only to route-only ports.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	Automatic downgrade of the startup–config is not supported during a software downgrade.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters	Layer 3 Route-only port counters are not enabled by default. Enabling them will reduce ipv4 route scale to 80K.
ICMP Redirect	The switch may incorrectly duplicate an IP frame that triggers ICMP redirect.
IGMP/PIM on Loopback and GRE interfaces	IGMP cannot be enabled on either Loopback or GRE interfaces. IGMP and PIM is not supported on 6-in-6 Tunnel . PIM can be enabled only on Loopback interfaces.
Multicast and VXLAN	▪ VXLAN must be configured prior to configuring VSX. ▪ IPv6 multicast is not supported for VXLAN overlay. ▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details.
MVRP and VSX	MVRP is mutually exclusive with VSX.
Network Analytics Engine (NAE)	Agents monitoring a resource that has column type enum with a list of strings (as opposed to a single string enum) is not supported.
Network Analytics Engine (NAE)	Network Analytics Engine (NAE) agents execute Command Line Interface (CLI) actions as 'admin' user, so they have permission to run any command by default. However, when the authentication, authorization and accounting (AAA) feature is enabled, the same restrictions applied to 'admin' will also apply to NAE agents. When using AAA, make sure to give the admin user the permissions to run all commands needed by enabled NAE agents. Otherwise, some CLI commands may be denied and their outputs won't be available. Actions other than CLI won't be affected and will execute normally. Also, NAE agents won't authenticate, thus the AAA service configuration must not block authorization for unauthenticated 'admin' user. ClearPass doesn't support such configuration, so it cannot be used as a TACACS+ server.
Network Analytics Engine (NAE)	The following tables are not supported for NAE scripts: OSPF_Route, OSPF_ LSA, OSPF_Neighbor, BGP_Route.

Feature	Description
OSPF	OSPFv2 and OSPFv3 do not support detailed LSA **show** commands.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RPVST+ and MSTP	Spanning Tree can only run in MSTP or RPVST+ mode.
RPVST+ and MVRP	RPVST+ is mutually exclusive with MVRP.
VRF	VRF names are limited to 31 characters.
VRRP	The same virtual link-local address cannot be used across different VRFs.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
VRRP	VRRP Preemption Delay Timer (preempt delay minimum) may be ignored after a switch reboot or power cycle.
DHCP Server, DHCP Relay, and DHCP Snooping DL	DHCP Relay and DHCP Snooping can co-exist on the same switch. DHCP Snooping and DHCP Server cannot co-exist on the same switch. DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.
VSX and Static VXLAN	Static VXLAN on VSX configuration is not supported. Use VSX and EVPN or VSX and HSC.

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
Local Proxy ARP	T-338	**Symptom**: ARP does not resolve when local proxy ARP is enabled. **Scenario**: This issue occurs in a VSX environment when local-proxy ARP is configured. **Workaround**: Enable ARP suppression.
L3 Routes	240831	**Symptom**: A route takes 180 seconds to get learned completely and stabilized when the cli setting **route recursive default route** is disabled during the route flap. **Scenario**: A route flap is observed upon any uplink failover scenarios when the nexthop of BGP routes tries to resolve via default route. In order to avoid the flap, r**oute recursive default route ipv4/ipv6** should be disabled during the issue state. The route learning takes 180 seconds to complete. **Workaround**: Issue the command **clear bgp ***.

Category	Bug ID	Description
VxLAN	T-1216	**Symptom**: A switch cannot be used as a border VTEP with PSM redirection enabled. L3VNI to L3VNI traffic cannot be supported with redirection and all multihop workflows will fail. The switch is not able to support firewalling on hosts directly attached to borders with this limitation. **Scenario**: This issue occurs when a switch is used as a TOR switch and border VTEP.
VxLAN	T-1223	**Symptom**: North-South or South-North traffic cannot be inspected. **Scenario**: This issue occurs on 10000 Series switches that support VRF to VRF traffic with firewall inspection. **Workaround**: Leak the inter-vrf traffic on borders (without firewall enabled) and inspect them on non-border VTEPs.
VxLAN	T-1224	**Symptom**: A policy cannot be configured on ROP interfaces. **Scenario**: This issue impacts traffic from ROP to the SVI or the SVI to ROP.
VxLAN	T-1225	**Symptom**: Traffic from VLAN with a policy to a VLAN without a policy is not supported. **Scenario**: Firewall inspection cannot be disabled for selected VLANs. It needs to be enabled on all VLANs of a VRF for normal traffic to flow. **Workaround**: For VLANs with no firewall inspection, enable a policy with a *permit all* rule.
VxLAN	T-1226	**Symptom**: TCP session information is synced locally within a VSX pair (TOR). When hosts/VM move to new racks, the TCP session is unknown to the new TOR and will be dropped. **Scenario**: This issue occurs during VMOTION of hosts between TORs. **Workaround**: Old sessions will have to be reconnected. New sessions are not impacted.
VxLAN	T-1244	**Symptom**: There is no support for application ALG for the firewall. **Scenario**: Applications that use multiple ports (UDP/TCP) and ports are dynamically negotiated will be affected.
VxLAN	T-1245	**Symptom:** Local proxy ARP cannot be disabled per VLAN. **Scenario**: Deployments that require local proxy ARP.
Port	PROJT-1013	**Symptom**: A port with AOC15 SFP might not link up after a link flap. **Scenario**: If AOC15 SFP is used, and there are multiple port flaps, then there is a chance that the port might not link up. **Workaround**: Recover from this issue by issuing the commands **shut** and **no shut** on the port.
Stateful L4 firewall	PROJT-985	**Symptom**: Glean traffic is not redirected to the Pensando Distributed Services Module (DSM) for policy evaluation. **Scenario**: In a VLAN where policy enforcement is enabled, if there is a host which does not have ARP resolved, then the first packet of this flow will not be redirected to DSM for policy enforcement. The flow will not be evaluated, and the flow table will not be programmed based on this first packet. Once ARP is resolved, subsequent packets will be redirected to Elba for evaluation.
Core	PROJT-454	**Symptom**: The **show core-dump all** command does not show cores from DSM. **Scenario**: Core dumps from DSM are not shown in the output of `show`

Category	Bug ID	Description
		`core-dump all` command in AOS-CX.
Stateful L4 firewall	PROJT-343	**Symptom**: In a VSX deployment , the first packet of a flow 9140 bytes or larger will fail flow sync. **Scenario**: This happens in a VSX scenario when there is a need to synchronize flows across the VSX peers to accommodate asymmetric traffic and firewall high availability. If the first packet of the flow is 9140 bytes or more, then this flow will not be synchronized. This can happen for UDP/ICMP packets, as TCP SYN packets are not larger than 9140 bytes. Virtual Machines (VMs) running on ESXi should not encounter this issue since DVS limits maximum MTU to 9000 bytes.
Stateful L4 firewall	PROJT-925	**Symptom**: The switch experiences inconsistent policy application in an L2 aggregation topology. **Scenario**: In a depoyment with L2 aggregation, when the switch is acting as an L2 access switch, a policy can not have different actions (PERMIT/DENY) for the same flow across ingress and egress policies on different VLANs.
L3 routes	240831	**Symptom**: Route takes 180 seconds to get learn completely or stabilized when the CLI command **route recursive default route** is disabled during the Route flap. **Scenario**: Route flap is observed upon any uplink failover scenarios when the nexthop of BGP routes tries to resolve via default route . In order to avoid the flap, route recursive default route ipv4 or ipv6 should be disabled. if the CLI is disabled during the issue state. Route learning takes 180 seconds for learning it completely. CLI command **Route recursive default route ipv4 or ipv6** needs to be disabled first. **Workaround**: Issue the command **clear bgp ***.

Upgrade information

AOS-CX 10.11.xxxx uses ServiceOS DL.01.11.0001.

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.

Manual configuration restore for software downgrade

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

1. Use the **show checkpoint** command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the **Image Version** column

in the output of the command, for example, DL.10.11.*yyyy*).

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

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

Performing the upgrade

For additional upgrade and downgrade scenarios, including limitations of automatic upgrade and downgrade scenarios provided by the Configuration Migration Framework (CMF), refer to the **AOS-CX 10.11 Fundamentals Guide**.

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

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

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

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

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

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

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

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

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

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

1 non-failsafe device(s) also need to be updated.
```

```
Please run the 'allow-unsafe-updates' command to enable these updates.

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

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

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

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

WARNING: Interrupting these updates may make the product unusable!

Continue (y/n)? y

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

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

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

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

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


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

Looking for SVOS.

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

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

```
    SHA:              6303a2a501bad91100d9e71780813c59f19c12fe

Boot Profiles:

0. Service OS Console
1. Primary Software Image [xx.10.10.1040]
2. Secondary Software Image [xx.10.11.1010]

Select profile(secondary):

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

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

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


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

Starting update...

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


Update successful (0.5 seconds).

reboot: Restarting system
```

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

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

                    RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software
```

```
 Documentation, and Technical Data for Commercial Items are licensed to the
 U.S. Government under vendor's standard commercial license.

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

switch login:
```

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

Chapter 2
Other resources

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

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

Chapter 3
Aruba security policy

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

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

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