AOS-CX 10.14.0001 Release Notes

4100i 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.

This release applies to the 4100i 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
JL817A	Aruba 4100i 12-port 1GbE (8-port Class 4 POE and 4-port Class 6 POE) 2-port SFP+ DIN Mount Switch	10.08.0001
JL818A	Aruba 4100i 24-port 1GbE (20-port Class 4 POE and 4-port Class 6 POE) 4-port SFP+ Switch	10.08.0001

Important information for 4100i 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.

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`, then contact support for further assistance.

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

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

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

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

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

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

Version history

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

Version number	Release date	Remarks
10.14.0001	21 May 2024	Initial release.

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	113
Safari (MacOS)	12
Safari (iOS)	10 (Version 12 is not supported)

Internet Explorer is not supported.

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

Management software	Recommended version(s)
NetEdit	2.11.0
Aruba Central	2.5.8
IMC	(708P03)

For more information, see the respective software manuals.

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

Enhancements for 4100i Switches in AOS-CX 10.14.0001

This section describes the enhancements introduced in this release.

Category	Description
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.
Underlay Fabric	Blocking of unknown multicast packets in a VLAN configured with: IGMP Snooping, and MLD Snooping. Default behavior is to allow initial flooding; to enable this feature, an explicit configuration command is required
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	SNMP trap filter per host
Infrastructure Management and Usability	SNMP read extended interface MIB for reporting

Resolved Issues for 4100i Switches in AOS-CX 10.14.0001

This section describes the issues resolved in this release.

Component	Summary	Description
IGMP	215677	**Symptom**: IGMP/MLD configuration changes do not take effect when the **hpe-mgmdd** process is flooded with IGMP/MLD control packets. **Scenario**: In a situation where IGMP or MLD control packets (Joins or Leaves) are part of a loop, or if misbehaving clients send continuous streams of IGMP/MLD control packets, the **hpe-mgmdd** daemon's packet queue can become continuously full. **Workaround**: Restart the MGMD daemon using the command **systemctl restart hpe-mgmdd**.
DNS	230380	**Symptom:** The switch experiences high CPU utilization . **Scenario:** High CPU utilization occurs when SNMP invokes DNS resolution, due to access of source IP which causes CPU overhead.
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. **Scenario:** This issue is seen only in the uncommon circumstance of a kernel corruption of the UI.
SW-Diagnostics	285649	**Symptom:** The output of the command **top cpu display limit** is not restricted to displaying the specified number of processes, and instead displays the full process list. **Scenario:** This issue occurs when using the **top cpu display** CLI command to display the list of the processes by CPU usage**.** **Workaround:** Enter the shell using the command **start-shell** and run the **top** command from within the shell.
LLDP	287305	**Symptom:** A Client is assigned a role VLAN instead of a Port VLAN ID (PVID). **Scenario:** This issue occurs on a Device-profile client 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 . **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.
Internal srvcs: Security PA infra	290068	**Symptom:** The **port-accessd** process crashes and restarts, and a core-dump file is generated. **Scenario:** This issue occurs if a client continuously moves from one port to another port. **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 **Scenario:** This issue occurs if the DHPCP client does not use **0.0.0.0** as the source IP, for example. when the DHCP packet is generated by the client with a valid private IP as source IP. **Workaround:** Use the source interface configuration.
MAC Tables	295625	**Symptom:** The switch reboots unexpectedly

Component	Summary	Description
		Scenario: Multiple threads in switch-agent might access the same cache. In this scenario, the hit-bit set thread locks the pd-l2-cache for its operation, meanwhile the mac-learning thread waits for its turn to lock it to add a new MAC entry. This request comes from the TL-Notify and gets an agent timeout, so it is rebooted and starts fresh.
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**. **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 **Workaround:** Refresh the Chrome Web page.
RADIUS Port-Access	296010	**Symptom**: The port-access daemon crashes continually. **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 **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	301734	**Symptom:** A role assigned by CoA gets overridden by low-priority methods, such as a RADIUS assigned role. **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) **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. **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 might incorrectly time out the RADIUS packets. **Workaround**: Unconfigure and reconfigure the RADSec server.
Multicast	309476	**Symptom**: Multicast traffic loss occurs when the joined port or the IGMP Querier Port is a LAG. **Scenario**: This issue occurs if IGMP and MLD Snooping is enabled on VLANs with a LAG port **Workaround**: Disable IGMP/MLD Snooping, convert the LAG to a physical port, and downgrade to 10.12 release.
SNMP	303650	**Symptom**: The snmpd process crashes and SNMP polling stops for a few seconds. **Scenario**: This issue can occur when polling by SNMP (snmpwalk), and simultaneously performing a snmpget/snmpbulkget on a non-existent OID. The SNMP process will recover itself after the crash.

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	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 ▪ does not have a have license to on-board the DUT but mobility conductor. ▪ 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.
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.
DHCP Server, DHCP Relay, and DHCP Snooping	DHCP Relay and DHCP Snooping can co-exist on the same switch. DHCP Snooping and DHCP Server cannot co-exist on the same switch. DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.

Feature	Description
DHCP Server, DHCP Relay, and DHCP Snooping	DHCP Relay and DHCP Snooping can co-exist on the same switch. DHCP Snooping and DHCP Server cannot co-exist on the same switch. DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.
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.
RADIUS	Authorization by means of HPE VSAs is not supported.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.

Known Issues

There are no known issue in this release.

Category	Bug ID	Description

Upgrade information

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, RL.10.xx.*yyyy*).

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

Performing the software upgrade

For additional upgrade and downgrade scenarios, including limitations of automatic upgrade and downgrade scenarios provided by the Configuration Migration Framework (CMF), refer to the **AOS-CX 10.14 Fundamentals Guide**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WARNING: Interrupting these updates may make the product unusable!

Continue (y/n)? y

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

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

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

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

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


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

Looking for SVOS.

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

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

Boot Profiles:

0. Service OS Console
1. Primary Software Image [xx.10.13.1000]
2. Secondary Software Image [xx.10.14.0001]

Select profile(secondary):

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

Advanced:
```

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

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


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

Starting update...

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


Update successful (0.5 seconds).

reboot: Restarting system
```

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

```
 (C) Copyright 2017-2024 Hewlett Packard Enterprise Development LP

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

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

switch login:
```

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

Chapter 2
Other resources

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

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

Chapter 3
Aruba security policy

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

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

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