AOS-CX 10.10.1030 Release Notes

6000, 6100 Switch Series

a Hewlett Packard Enterprise company

Published: December 2022

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.

Products supported

This release applies to the 6000 and 6100 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
R8N85A	Aruba 6000 48G Class4 PoE 4SFP 370W Switch	10.08.1010
R8N86A	Aruba 6000 48G 4SFP Switch	10.08.1010
R8N87A	Aruba 6000 24G Class4 PoE 4SFP 370W Switch	10.08.1010
R8N88A	Aruba 6000 24G 4SFP Switch	10.08.1010
R8N89A	Aruba 6000 12G Class4 PoE 2G/2SFP 139W Switch	10.08.1010
JL675A	Aruba 6100 48G Class4 PoE 4SFP+ 370W Switch	10.06.0100
JL676A	Aruba 6100 48G 4SFP+ Switch	10.06.0100
JL677A	Aruba 6100 24G Class4 PoE 4SFP+ 370 Switch	10.06.0100
JL678A	Aruba 6100 24G 4SFP+ Switch	10.06.0100
JL679A	Aruba 6100 12G Class4 PoE 2G&2SFP+ 139W Switch	10.06.0100

Important information for 6000 and 6100 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>`."

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.

If using the Web UI, you should 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 PL.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.

To upgrade to:	Your switch must be running this version or later:
AOS-CX 10.10.xxxx Note: 10.10 is an LSR, recommended release is 10.10.10xx.	AOS-CX 10.06.0110
AOS-CX 10.09.xxxx Note: 10.09 is an SSR, recommended release is 10.09.10xx.	AOS-CX 10.06.0110
AOS-CX 10.08.xxxx Note: 10.08 is an SSR, recommended release is 10.09.10xx.	AOS-CX 10.05.0001
AOS-CX 10.07.xxxx Note: 10.07 is an SSR, recommended release is 10.09.10xx.	AOS-CX 10.04.0001
AOS-CX 10.06.xxxx Note: 10.06 is an LSR, recommended release is 10.06.10xx.	AOS-CX 10.03.0001

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
10.10.1030	2022-12-08	Released, fully supported, and posted on the Web.
10.10.1020	2022-11-07	Released, fully supported, and posted on the Web.
10.10.1010	2022-09-22	Released, fully supported, and posted on the Web.
10.10.1000	2022-08-14	Released, fully supported, and posted on the Web.
10.10.0002	2022-06-21	Initial release of AOS-CX 10.10. 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	8.2.14.1(6000 not supported)
NetEdit	2.5.0
Aruba Central	2.5.5
IMC	7.3 (E0706P11) (6000 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

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 6000 and 6100 Switches in AOS-CX 10.10.1030

There are no enhancements introduced in this release.

Fixes

This section lists released builds that include fixes found in this branch of the software. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

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 for customers who decide not to update to this version of software.

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

The Bug ID is used for tracking purposes.

Resolved issues for 6000 and 6100 Switches in AOS-CX 10.10.1030

Category	Bug ID	Description
Logging	246447 232176	**Symptom**: High CPU utilization seen in switches seems unexpectedly high. **Scenario**: Housekeeping scripts run every hour, taking care of essential tasks like rotating log files to ensure they do not grow too big. These processes running these scripts can sometimes take roughly 50% of the

Category	Bug ID	Description
		total CPU for approximately one minute, displaying spikes in monitoring solutions, such as graphs. It might also cause monitoring systems to send alerts. **Workaround**: The spike is generally short-lived and can be ignored
MSTP	249623	**Symptom**: BPDU guard is disabling an access port after a Windows 11 workstation sends LLDP frames with a STP DA. **Scenario**: Windows 11 has LLDP enabled by default. It uses the DA address "01:80:c2:00:00:00". AOS-CX is not checking for ether-type 0x88CC explicitly **Workaround**: Disable the Microsoft LLDP protocol driver in Windows 11 or configure'**spanning-tree bpdu-filter** instead of bpdu-guard, so that the port will not go down. Note with a bpdu-filter configuration, that specific port is expected to be connected exclusively to an end device, since loops will no longer be identified.
IGMP	248258	**Symptom**: Multicast streams fail to arrive at clients, typically seen when clients on multiple VLANs request the same S,G multicast streams. Running the **show ip igmp snooping details** command will show the group associated with the client port, but no traffic will get sent down the port. **Scenario**: When two multicast clients in different VLANs join the same multicast stream, the system will incorrectly leave a stale ASIC entry for one of the VLANs once one of the two clients leaves the stream. Once the system is in this state, the stream will no longer work for one of the VLANs. **Workaround**: Reload the switch and migrate all multicast clients interested in the same S,G groups into one VLAN.
IGMP	237274	**Symptom**: Clients may experience IGMP join delays in cascaded topologies and IPTVs may experience blank screens during channel changes. **Scenario**: The issue is observed in cascaded topologies with four or more devices between the client and the querier. **Workaround**: Move the querier towards clients. Configure port forwarding to pre-program multicast flows.

Feature caveats

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

Feature	Description
TFTP	Blocksize greater than 1480 is not supported in 4100i, 6100 and 6000 Switch series.
VRRP	The same virtual link-local address cannot be used across different VRFs.
VRRP	MD5 authentication interoperation is not supported with Comware-based switches
DHCP Server DHCP Relay DHCP Snooping	Note the following caveats for these features: ■ 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
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	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.
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

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 environment details and trigger summaries. When available, the **Workaround** statement provides a workaround to the issue.

Category	Bug ID	Description
Classifier	232166	**Symptom**: Policy application fails. **Scenario**: Install a CoPP entry, then a V4 entry, followed by a V6 entry which has count and dscp actions enabled. The v6 policy should be applied to VLAN or global context. Policy application will fail. Workaround: Avoid using counters with dscp action of an ipv6 policy.
CLI Infra	211466	**Symptom**: The user session does not timeout. **Scenario**: When the switch console is left idle, with a CLI command output in progress, waiting for user input to display the next page, the user session does not timeout when the configured timer expires. **Workaround**: The session idle timeout counts when CLI command is completed and the switch is idle at the switch prompt.
Port Access	156628	**Symptom:** The **port-access** daemon crashes. **Scenario:** When port security is enabled on a port where the **port-security client-limit** is configured with a value lower than the number of the port-security static clients configured on the port, after a downgrade from 10.07 to 10.05 or 10.06 the **port-access** daemon crashes. **Workaround:** Prior to the downgrade, set the port-security limit configuration to a value equal to or higher than the number of static port-security clients configured on the port.

Upgrade information

AOS-CX 10.10.0002 uses ServiceOS PL.01.09.0003.

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, PL.10.10.*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 10.10 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.10.10.1020]
2. Secondary Software Image [xx.10.10.1030]

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 2017-2022 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 10.10 playlist of technical training videos on YouTube: https://www.youtube.com/playlist?list=PLsYGHuNuBZcZmHTZQC9LuivtrVecOx5vk

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.