AOS-W 8.10.0.8 Release Notes

Alcatel·Lucent Enterprise

Copyright Information

Open Source Code

Contents

Chapter 1
Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release:

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 2
Release Overview

This AOS-W release notes includes the following topics:

- New Features and Enhancements
- Supported Platforms
- Regulatory Updates
- Resolved Issues
- Known Issues and Limitations
- Upgrade Procedure

Important

- As mandated by the Wi-Fi Alliance, AOS-W 8.10.0.x requires Hash-to-Element (H2E) for 6 Ghz WPA3-SAE connections. H2E is supported only on Windows 11, Linux wpa_supplicant version 2.10 and later versions. Hence, users must upgrade their Windows and Linux software for successful 6 Ghz WPA3-SAE connections.
- The factory-default image of APs introduced in AOS-W 8.9.0.0 or later versions use **aruba-conductor** as the host name instead of **aruba-master** to identify a target managed device or stand-alone switch during DNS discovery. However, the factory-default image of APs that were introduced prior to AOS-W 8.9.0.0 still use **aruba-master** during DNS discovery. The usage of **aruba-conductor** is to align with the Inclusive Language Initiative.
- Upgrading to AOS-W 8.10.0.7 or later versions on OAW-41xx Series and 9200 Series switches will take longer than usual as we will be automatically upgrading the BIOS version to support additional functionality in the future. This upgrade is estimated to take up to 15 minutes and should not be interrupted for any reason. Power failures and interruptions during the upgrade may make the switch unusable. Please use caution and plan accordingly.

NOTE

Cluster Rolling Upgrade is not supported when a BIOS upgrade is required. AOS-W 8.10.0.8 must be manually upgraded for these controllers.

Related Documents

The following guides are part of the complete documentation for the Alcatel-Lucent user-centric network:

- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W API Guide*
- *Alcatel-Lucent Mobility Conductor Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*

- *Alcatel-Lucent AP Software Quick Start Guide*

Supported Browsers

The following browsers are officially supported for use with the AOS-W WebUI:

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	■ Windows 10 or later ■ macOS
Firefox 107.0.1 or later	■ Windows 10 or later ■ macOS
Apple Safari 15.4 (17613.17.1.13) or later	■ macOS
Google Chrome 108.0.5359.71 or later	■ Windows 10 or later ■ macOS

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our ALE culture and moving forward, ALE will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://myportal.al-enterprise.com

Contact Center Online	
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

Chapter 3
What's New in AOS-W 8.10.0.8

This chapter describes the features, enhancements, and behavioral changes introduced in this release.

Enhancements to the OFA Core Size

By excluding a section of process memory, OFA core size is reduced. This reduction helps in capturing and debugging OFA cores in scale scenarios.

PoE Support for OAW-AP535 Access Point

OAW-AP535 access points can now boot up while using a USB converter and a console cable that's powered by PoE switch.

Unnecessary Logs are Reduced

In unsupported platforms of the **show uplink cellular** details command, the logs generated by this command are largely reduced: **webui[3433]: <399838> <3433> <WARN> || Error in processing cmd: show uplink cellular details (len: 28), err: Command not applicable for this platform (pos: 0)**. This avoids unnecessary information.

Enhanced Time Efficiency

In AOS-W 8.10.0.8, the time efficiency when using the **write memory** command has been improved by adding **bocmgr** in the nanny list.

Enhanced RADIUS Attribute Modifier

Administrators can now construct STRING-type RADIUS attributes with prefixes and suffixes together with either static values or dynamic values. The **aaa radius modifier <RAD-MOD-NAME>** command has been expanded to include the **[prefix <prefix_val>]** and **[suffix <suffix_val>]** sub-commands.

This enhancement enables administrators to optionally add static or dynamic values with a prefix. Similarly, a suffix can be optionally appended to the value. The resulting string becomes the value of the target RADIUS attribute.

Behavioral Changes

This release does not introduce any changes in AOS-W behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.10.0.8.

Chapter 4
Supported Platforms

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

The following table displays the Mobility Conductor platforms that are supported in this release:

Table 3: *Supported Mobility Conductor Platforms*

Mobility Conductor Family	Mobility Conductor Model
Hardware Mobility Conductor	MCR-HW-1K, MCR-HW-5K, MCR-HW-10K
Virtual Mobility Conductor	MCR-VA-50, MCR-VA-500, MCR-VA-1K, MCR-VA-5K, MCR-VA-10K

OmniAccess Mobility Controller Platforms

The following table displays the OmniAccess Mobility Controller platforms that are supported in this release:

Table 4: *Supported OmniAccess Mobility Controller Platforms*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series OmniAccess Mobility Controllers	OAW-4104, 9012
9200 Series OmniAccess Mobility Controllers	9240
MC-VA-xxx Virtual OmniAccess Mobility Controllers	MC-VA-10, MC-VA-50, MC-VA-250, MC-VA-1K

AP Platforms

The following table displays the AP platforms that are supported in this release:

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H, OAW-AP303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP318
OAW-AP320 Series	OAW-AP324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP370EX Series	OAW-AP375EX, OAW-AP377EX, OAW-AP375ATEX
OAW-AP387	OAW-AP387
OAW-AP500 Series	OAW-AP504, OAW-AP505
OAW-AP500H Series	OAW-AP503H, OAW-AP503HR, OAW-AP505H, OAW-AP505HR
OAW-AP510 Series	OAW-AP514, OAW-AP515, OAW-AP518
OAW-AP518 Series	OAW-AP518
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP580 Series	OAW-AP584, OAW-AP585, OAW-AP585EX, OAW-AP587, OAW-AP587EX
OAW-AP630 Series	OAW-AP635
OAW-AP650 Series	OAW-AP655

Chapter 5
End-of-Support

This chapter provides information on the Alcatel-Lucent products that are not supported for a particular release.

The following AP models will no longer be supported beginning with the next major release, AOS-W 8.11.0.0 and higher:

- 200 Series
- OAW-AP203H Series
- OAW-AP203R Series
- OAW-AP205H Series
- OAW-AP207 Series
- 210 Series
- 220 Series
- OAW-AP228 Series
- 270 Series
- 320 Series
- 330 Series
- OAW-AP340 Series
- OAW-AP387

Chapter 6
Regulatory Updates

This chapter contains the Downloadable Regulatory Table (DRT) file version introduced in this release.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the switch Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at https://myportal.al-enterprise.com.

The following DRT file version is part of this release:

- DRT-1.0_87407

Chapter 7
Resolved Issues in AOS-W 8.10.0.8

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-208640	In some OAW-AP505 access points running AOS-W 8.7.1.0 or later versions, client devices experienced slow performance. This issue occurred when **HE MU-OFDMA** parameters were enabled. The fix ensures client devices perform as expected.	AOS-W 8.7.1.0
AOS-224143 AOS-221378	The output of the **show ap debug radio-stats** command displayed incorrect Rx data frame statistics. The fix ensures the command displays the correct information. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-225263	L2 database synchronization failed on standby switches. The fix ensures that L2 database synchronization does not fail. This issue was observed in standalone switches running AOS-W 8.8.0.1 or later versions.	AOS-W 8.8.0.1
AOS-227390	After the initiation of a ping from the Branch Gateway to the neighbor's IP address, there was a transition of the BGP state from **Idle** to **Established** state. The fix ensures the process works as expected. This issue is observed in controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-231473	The **Dashboard** > **Overview** > **Wired Clients** page of the WebUI did not display the details of the APs to which clients were connected. The fix ensures the information is correctly displayed. This issue is observed in Mobility Conductors running AOS-W 8.8.0.2 or later versions in a IPv6 deployment.	AOS-W 8.8.0.2
AOS-232541	The WebUI **Configuration** > **AP Groups** > **APs** section did not show or apply any configurations beyond the first page. The fix ensures the WebUI works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232620	A discrepancy was observed between the total number of APs and the total number of AP BLE devices reported. The fix ensures no discrepancies are found. This issue was observed in standalone controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.8.0.2
AOS-232717 AOS-245030 AOS-243103	The VPNC crashed and rebooted unexpectedly with reboot cause: **Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:60)**. The fix ensures the VPNC works as expected. This issue was observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-233051	In some OAW-4104 switches running AOS-W 8.7.0.0 or later versions, the DHCP relay stopped working for certain VLANs preventing clients in those VLANs from getting an IP address. The fix ensures that DHCP relay works as expected.	AOS-W 8.7.0.0
AOS-234761 AOS-240612 AOS-240809	The **Dashboard > Overview > Wireless Clients** page of the WebUI did not display the IP address of the Active Controller and Standby Controller. However, the CLI displayed the IP address of the active and standby controllers. The fix ensures the correct information is displayed. This issue was observed in Mobility Conductors running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
AOS-235239 AOS-240499	In some OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions, the **Profiles > RF Management > 6GHz radio** section in the WebUI did not allow the **Allowed bands for 40MHz channels** option to be set to **None**. The fix ensures that this option can be set.	AOS-W 8.10.0.5
AOS-235479	The commands **copy ftp** and **copy tftp** did not work as expected for the management interface. The fix ensures the commands work as expected. This issue was observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-237643 AOS-238995	In some cases, the gateway failed to send the outgoing traffic with IKEv2 for VIA tunnels. The fix ensures that VIA can successfully send data packets to external traffic with IKEv2 profile. This issue was observed in gateways running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-237710	During ARP discovery, devices with the same IP as the AP's default gateway caused the MAC address of the IP to be overwritten in the ARP cache, leading to unexpected rebootstrap processes. The fix ensures the ARP process is executed successfully and APs work as expected. This issue was observed in APs running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-237931 AOS-242118 AOS-245405	A datapath crash was observed on Ubuntu 20_04 servers if the OS type was set to RHEL 7.2 or above. The fix ensures the servers work as expected. This issue was observed in virtual machines running on AOS-W 8.7.1.11 or later versions.	AOS-W 8.7.1.11
AOS-238103	Some OAW-AP635 access points were reporting high path loss values when compared to earlier models. The fix ensures the access points work as expected. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
AOS-238600 AOS-239753	In some switches running AOS-W 8.11.0.0 or later versions, the logs were not displayed on the LCD during reload or halt. Information came up on the LCD after BIOS loaded. The fix ensures the logs are visible on the LCD as expected.	AOS-W 8.11.0.0
AOS-238604	The AP regulatory domain profile displayed different information in the WebUI and CLI. The fix ensures the information displayed in the WebUI matches with the CLI. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-238817	The **Dashboard** > **Security** > **Suspected Rogue and Authorized** section of the WebUI displayed an error message: **Error retrieving information. Please try again later.** This caused the list of APs to not populate correctly. This issue occurred because non-UTF-8 characters were added to the backend. The fix ensures the WebUI displays the information correctly. This issue was observed in some controllers running AOS-W 8.6.0.19 or later versions.	AOS-W 8.6.0.19
AOS-239130	The **TOTAL HIT** and **NEW HIT** information in the **Configuration > Authentication > User Rules > Rules-set** page of the WebUI displayed as **--**. However, the **show aaa derivation-rules user** command in the CLI displayed the information accurately. The fix ensures that the WebUI information matches with the CLI. This issue was observed in Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17
AOS-239378	Some cluster nodes missed the cluster heartbeat from a different node. This caused both nodes to disconnect and isolate in a subcluster, creating an expected cluster split. The fix ensures that heartbeat misses do not derive in a cluster split. This issue was observed in managed devices running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239472 AOS-242785	The **show loginsessions** command displayed multiple entries with empty **User Name** and **User Role**. This issue also caused the SSH process to fail. This issue occurred because the CLI processes from previous sessions were still active in the background. The fix ensures such sessions are timed out accordingly, discarding empty entries in the **show loginsessions** command and resolving issues with the SSH process. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-239821 AOS-243932	The output of the **show running-config** command displayed with no left indentations. The fix ensures that the command output is displayed as expected. This issue was observed in switches running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-240076	OAW-4650 Gateways running AOS-W 8.7.0.0-2.3.0.9 rebooted unexpectedly. The log files listed the reason for this event as **Reboot Cause: Nanny rebooted machine - isakmpd process died (Intent:cause:register34:86:50:2)**. The fix ensures that the gateway works as expected.	AOS-W 8.7.0.0-2.3.0.9
AOS-240312	The **arci-cli-helper** process crashed on OAW-4750XM switches running AOS-W 8.7.1.10 or later versions. This generated crash files, but the switch did not reboot. The fix ensures that this process works as expected.	AOS-W8.7.1.10
AOS-240419	Some packets were lost when sending traffic over a network secured using WPA3 and CNSA. This issue occurred when downloading files from a SMB server in a PC running Windows 10. This issue was observed in access points running AOS-W 8.10.0.5 or later versions. The fix ensures the APs work as expected.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-240435	Some APs sent random false alerts to the OmniVista 3600 Air Manager monitor to display their status as **Down** while remaining **Active** on the controller. The fix ensures the APs send only correct alerts to OmniVista 3600 Air Manager. This issue was observed in OAW-AP303H access points running AOS-W 8.7.1.10 or later versions.	AOS-W 8.10.0.6
AOS-240568 AOS-244716	The **write mem** command took a long time to save tunnel configurations on standby switches. The same issue was observed when saving the configuration through the switch's WebUI. The fix ensures the saving process for tunnel configuration completes in an appropriate time frame, as expected. This issue was observed in standby switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-240653	The size of **/mswitch/logs/fpapps.log** file increased indefinitely by 40 MB per month, consuming unnecessary memory resources. The fix ensures the log files are handled as expected. This issue was observed in standalone controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-240740	Some OAW-AP635 access points running AOS-W 8.10.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures the APs work as expected.	AOS-W 8.10.0.4
AOS-241160 AOS-242900 AOS-243302	Some OAW-AP535 access points running AOS-W 8.10.0.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as: **kernel panic: Fatal exception in interrupt** and **kernel panic: Take care of the TARGET ASSERT first**. The fix ensures the APs work as expected.	AOS-W 8.10.0.5
AOS-241256	The **Global User-Table** record displayed the MAC addresses of some clients to be associated with multiple APs. The fix ensures the correct information is displayed. The issue was observed in Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.5
AOS-241325	In some switches running AOS-W 8.10.0.2 or later versions, the **Beacon Period** in the **Configuration > System > Profiles > RF Management** section in the WebUI, and the **show rf dot11a-radio-profile** command in the CLI was displayed as 100 msec. Instead, the **Beacon Period** should be expressed as 100 time units or 102.4 msec. The fix ensures that the **Beacon Period** value and units are displayed correctly.	AOS-W 8.10.0.2
AOS-241438	A case sensitive check was performed when the following commands were executed in the CLI: ■ **show global-user-table list name <username>** ■ **show global-user-table list role <role name>** ■ **show global-user-table count ap-name <name>** This prevented users from getting accurate search results for usernames or APs. The fix ensures the command works for case sensitive inputs as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-241498 AOS-245217	A corrupt bridge ACL issue was observed in APs running AOS-W 8.10.0.5 or later versions, where some user roles were either missing or contained a duplicate of the **logon** role. This issue occurred when the AP failed over to a controller with a different ACL configuration, preventing the AP from passing traffic. The fix ensures APs work as expected.	AOS-W 8.10.0.5
AOS-241737	The **RADIUS User-Name** attribute contained an empty value in the RADIUS Accounting-Stop packet when an authenticated Captive-Portal client clicked the **Logout** button. The fix ensures the User-Name attribute contains user-name value in the RADIUS Accounting-Stop packet. This issue was observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-241801	Some 802.11r client devices running AOS-W 8.10.0.4 or later versions were unable to FT-roam. This issue was related to the PTKSA/GTKSA ReplayCounters in RSNE mismatching with the same in Probe-Response/Beacon packets. The fix ensures that 802.11r client devices are able to roam as expected.	AOS-W 8.10.0.4
AOS-241870	The **Dashboard > Infrastructure** page displayed APs as **Down**, even after being cleared by executing the **clear gap-db ap-name** command. The fix ensures the WebUI displays the expected information. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241898	The **Configuration > WLANs > VLANs** section of the WebUI did not reflect changes made to the VLAN. This issue was observed in controllers running AOS-W 8.10.0.5 or later versions. The fix ensures that the WebUI reflects the VLAN changes correctly.	AOS-W 8.10.0.5
AOS-242048	Clients connected to a controller with mesh point enabled experienced latency issues while roaming in a mesh topology. The fix reduced latency during mesh point while roaming. This issue was observed in OAW-AP515 access points running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-242301	In some OAW-4550 Branch Gateways running AOS-W 8.7.0.0, the **Dot1x** process crashed intermittently and caused the Branch Gateway to reboot. This issue occurred because of a double freeing error in the **802.1x module** due to a timer issue. The fix ensures the gateways perform as expected.	AOS-W 8.7.0.0
AOS-242343	Some wired AirGroup servers were randomly removed from the AirGroup server list. This issue occurred as mDNS advertisement packets, which had unsupported services, were sent from the wired server. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions. The fix ensures OmniAccess Mobility Controllers work as expected.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-242363	In a Hub-Spoke structure, if a single VLAN was configured in the VPN IP command, VPN Concentrators lost connectivity after a spoke reboot. This issue occurred only when the spoke was rebooted and was not seen under normal operation. The fix ensures the process works as expected. This issue was observed in controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-242469	Mobile devices were unable to connect to Passpoint SSID. This issue occurred when EAP transactions were sent across two different Radsec connections to cloud guest server. The fix ensures that mobile devices connect to Passpoint SSID as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-242694 AOS-242773	Some APs created unnecessary syslog events as a warning or error event. The fix ensures the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242696	Users were unable to convert OAW-AP APs running AOS-W 8.10.0.5 or later versions to Instant APs and AOS-W 10.x APs, while attempting to upgrade. This issue occurred when the **ap convert** command was run with pre-validation enabled, and the pre-validation process was interrupted before completion. The fix ensures that users are able to convert OAW-AP to OAW-IAP and AOS-W 10.x APs even if the pre-validation process is interrupted.	AOS-W 8.10.0.5
AOS-242759	In some devices using curl, the **endpointURL** parameter was not configured in the IoT radio profile for ASSA ABLOY. This caused memory leaks in the Bluetooth Low Energy (BLE) relay process. The fix ensures that the connection using curl works as expected. This issue was observed in AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-242804	Some APs configured as spectrum-monitor or AM were incorrectly displayed in **Overview** > **Usage** > **LOW PERFORMING Wi-Fi** page of the WebUI, and were excluded from the AP performance chart. The fix ensures the correct information is displayed. This issue was observed in APs running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-242983 AOS-242554	The VPN Concentrator crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Reboot Cause: Datapath timeout (SOS Assert)**. The fix ensures that the VPN Concentrator works as expected. This issue was observed in some gateways running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-243049	Some BLE beacons from OAW-AP515 access points were undetected by clients. The fix ensures the BLE beacons work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-243064	Some OAW-AP535 access points crashed unexpectedly. The log files listed the reason as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first:Excep :0 Exception detectedparam0 :zero, param1 :zero, param2 :zero**. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.6 or later versions. The fix ensures that APs work as expected.	AOS-W 8.10.0.6
AOS-243132	Standalone controllers did not age out captive portal users from the user table when connected to a wired split tunnel. The fix ensures wired clients are required to re-authenticate to access the network and their status is not active in the user table after certain time. This issue was observed in standalone controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-243162	Controllers restricted to Egypt did not display the country code in the output of the **show version** command. The fix ensures the correct information is displayed. This issue was observed in controllers running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-243164	Some OmniAccess Mobility Controllers unexpectedly crashed due to **show-auth-tracebuf** process. A correction in the segmentation fixed the issue. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-243265	Some OAW-AP515 access points running AOS-W 8.10.0.5 or later versions unexpectedly generated AP panic dump files. The log files listed the reason for the event as: **Unable to handle kernel NULL pointer dereference at virtual address 00000014**. The fix ensures that NULL values are handled correctly, and the AP performs as expected.	AOS-W 8.10.0.5
AOS-243338	Some APs were randomly shutting down due to IKEv2 exchange timeout. The fix ensures the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-243617	In switches running AOS-W 8.10.0.5 or later versions, invalid configuration profiles were pushed through MM WebUI to MD child nodes with no error messages in a corner case scenario. This issue was observed when the **Allow-fail-through** option was enabled. The fix ensures the incorrect settings are not pushed, and an error message is thrown as expected.	AOS-W 8.10.0.5
AOS-243621	OmniAccess Mobility Controllers sent incorrect channel bandwidth data for mesh radios reported in SNMP **wlsxWlanRadioTable**. The fix ensures the controller works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-243722	Some managed devices running AOS-W 8.6.0.20 or later versions, were unable to display **auth-survivability** cached data when certain time zones were configured, like Asia or Jakarta (WIB). The fix ensures that the data is cached correctly.	AOS-W 8.6.0.20

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-243749 AOS-243146	Some standalone switches running AOS-W 8.10.0.6 or later versions did not allow users to make changes through the WebUI when using standard admin credentials. The fix ensures that standard admin users can make changes using the WebUI.	AOS-W 8.10.0.6
AOS-243761	The commands **perf-test server start controller** and **perf-test server stop controller** showed the error **Command Failed:Iperf Server cannot be Master IP**. The issue was related to null IPs being taken into consideration during the command execution. The fix ensures the commands work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.7.	AOS-W 8.10.0.7
AOS-243959 AOS-245982	Some OAW-AP555 running AOS-W 8.10.0.0 or later versions crashed while running the **show ap arm scan_times ap-name** command. This issue led to client devices disconnection. The fix ensures the AP performs as expected in this scenario.	AOS-W 8.10.0.0
AOS-244165	OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions included spurious messages stating **TOKEN WAS ABSENT** as error logs. These messages were intended to appear as debug logs, not error logs. The fix ensures these messages do not come up in error logs anymore, but instead are included in debugging logs.	AOS-W 8.10.0.6
AOS-244247	The value for **attack-rate tcp-syn <#>** was unable to be set over 255, causing clients to not be blacklisted. The fix ensures the value can be set over 255. This issue is observed in controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-244264	Some access points crashed unexpectedly. The issue occurred due to high memory utilization causing users to be unable to obtain IP addresses or associate the APs with SSIDs. The fix ensures no memory leaks occurs while BLE transport profile is trying to connect to external servers. This issue was observed in OAW-AP345 access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244321	Some RADIUS server users were unable to connect to Passpoint due to an **Exhausted reqids** error. The fix ensures switches work as expected. This issue was observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244358	In the WebUI **Dashboard** > **Overview** > **Clients** > **Name**, the SSID of the clients incorrectly displayed the IP or the MAC address. The fix ensures the SSID displays correctly. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.5
AOS-244436	Some APs running AOS-W 8.9.0.3 and configured with a valid BSSID were incorrectly identified as rogue APs. After upgrading to AOS-W 8.10.0.6, IDS incorrectly reported AP impersonation events for valid BSSIDs. The fix ensures no false positives are reported by IDS. This issue was observed in APs running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-244628	Some access points were unable to upgrade using the **apflash ap31x-ap32x backup partition** command. The fix ensures the command works as expected. This issue was observed in OAW-AP315 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.4
AOS-244736	Some OmniAccess Mobility Controllers using UBT feature were incorrectly forwarding unicast traffic to other UBT tunnels. The fix ensures the feature works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.6
AOS-244800 AOS-244803 AOS-245378	Some OmniAccess Mobility Controllers unexpectedly crashed. The log files listed the reason as: **Reboot Cause: Kernel Panic (Intent:cause:register12:86:b0:4)**. The fix ensures the controllers work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21
AOS-244855	The output of the **show airmatch optimization** command returned no information when there are more than 200 optimization records in database. The fix ensures the command works as expected. This issue can be observed on Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.6
AOS-245011	After upgrading to AOS-W 8.10.0.6, systems experienced periodic WebSocket disconnections every 5 minutes when transmitting BLE telemetry data to third-party servers. The issue was especially prevalent at a data reporting interval of 3 seconds, where certain telemetry updates were missing due to packet drops. The fix ensures WebSocket stability, reducing disconnections during high packet loss scenarios. This issue was observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245123 AOS-245396 AOS-245831	In the WebUI, under **Managed Network > Configuration > Roles & Policies > Roles**, the **Show Advance View** option did not load any information. The information is expected to load after selecting a role from the list. The fix ensures that the advanced role policies is loaded. This issue was observed in controllers running AOS-W 8.10.0.7.	AOS-W 8.10.0.7
AOS-245191	In some controllers running AOS-W 8.6.0.18 or later versions, OmniVista 3600 Air Manager sessions were not timing out. Also, it was not possible to connect to the controllers using direct SSH. The fix ensures the sessions are timed out as expected.	AOS-W 8.6.0.18
AOS-245266 AOS-244968	Some access points automatically disabled their 6 GHz radio bands. The issue occurred due to a discrepancy in the enumeration values of the 6 GHz band. The fix ensures the access points work as expected. This issue was observed in OAW-AP635 and OAW-AP655 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245458	The ports 0/0/6 to 0/0/11 of the OAW-41xx Series controllers did not transmit traffic as expected. The fix ensures the ports work as expected. This issue was observed in controllers running AOS-W 8.10.0.7.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-244875	In some OAW-4550 controllers running AOS-W 8.6.0.18 or later versions, the 802.1x module crashed. This issue was observed in controllers with a Branch Gateway role. The fix ensures that the module works as expected.	AOS-W 8.6.0.18

Chapter 8
Known Issues in AOS-W 8.10.0.8

This chapter describes the known issues and limitations observed in this release.

Limitations

Following are the limitations observed in this release.

OAW-AP650 Series and OAW-AP630 Series Access Points

The OAW-AP650 Series and OAW-AP630 Series access points have the following limitations:

- No spectrum analysis on any radio
- No Zero-Wait DFS
- No Hotspot and Air Slice support on the 6 GHz radio
- No 802.11mc responder and initiator functionality on any radio
- Only 4 VAPs on the 6 GHz radio instead of 16
- Maximum of 512 associated clients on any radio, instead of 1024

6 GHz Channel Information in Regulatory Domain Profile

AOS-W does not display the 6 GHz channel information in the existing regulatory domain profile of Wi-Fi 6E APs by default.

To include 6 GHz channel information, ensure that you change the country code to a different country code, apply the change, and then revert it to the original country code. Another option is to create a new regulatory domain profile that includes the 6 GHz channel information by default, or copy the existing regulatory domain profile into a new regulatory domain profile to save the configuration.

The following example configures a regulatory domain profile and specifies a valid 6 GHz band.

```
host) [mynode](config) #ap regulatory-domain-profile reg-635
host) [mynode] (Regulatory Domain profile "reg-635") #country-code US
host) [mynode] (Regulatory Domain profile "reg-635") #valid-6ghz-channel 165
```

Air Slice

Air Slice is partially enabled on OAW-AP500 Series access points and OAW-AP510 Series access points. However, WMM boost will be functional even if Air Slice high-priority queuing is disabled.

Airtime Fairness Mode

Airtime Fairness Mode is not supported in 802.11ax access points.

OAW-40xx Series and OAW-4x50 Series switches

The **cpboot** command does not upgrade the AOS-W software version of OAW-40xx Series and OAW-4x50 Series controllers.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-138608 AOS-243123	A few clients experience packet loss due to high datapath utilization in the CPU. This issue is observed in OAW-4750 switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-156537	Multicast streaming fails when broadcast and multicast optimization is enabled on the user VLAN. This issue is observed in managed devices running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-195434	Some APs crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is observed in APs running AOS-W 8.5.0.0 or later versions in a OmniAccess Mobility Controller-managed device topology.	AOS-W 8.5.0.2
AOS-199724 AOS-214805	Reverse Policy Based Routing (PBR) is not working when applied to the VPN tunnel's Access Control List (ACL) in hub and spoke setups. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-205650 AOS-231536	DHCP traffic from relay agent is not forwarded through the next-hop list configured in Layer 3 GRE tunnel. This issue is observed in managed devices running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-209580	The output of the **show ap database** command does not display the **o** or **i** flags, which indicate whether an AP is an outdoor AP or an indoor AP. This issue occurs when the AP installation type is not set to default. This issue is observed in Mobility Conductors running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-215875	The **show ap arm state** command displays deprecated information such as Edge, Relevant Neighbors, Valid Neighbors, Neighbor Density, and Client Density. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.7.1.1 later versions.	AOS-W 8.7.1.1
AOS-216536 AOS-220630	Some managed devices running AOS-W 8.5.0.11 or later versions are unable to come up on the Mobility Conductor. This issue occurs when the managed devices receive the branch IP address as the controller IP address in a VPNC deployment.	AOS-W 8.5.0.11
AOS-217751	Some switches running AOS-W 8.6.0.6 or later versions crash and reboot unexpectedly. The log files list the reason for the crash as **Reboot Cause: Unknown reboot reason (238:238:2) (Intent:cause:register ee:ee:50:2)**. The issue is related to the external PDU powering the controller's PSU, which may be faulty.	AOS-W 8.6.0.6
AOS-217948	Some APs experience issues with Wi-Fi uplink 802.1X authentication due to a conflict in certificate validity period verification. This issue is observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219150	The Mobility Conductor fails to push the SRC NAT pool configuration to the managed devices. This issue occurs when the ESI redirect ACL is configured using the WebUI. This issue is observed in Mobility Conductors running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219423	Honeywell Handheld 60SL0 devices are unable to connect to 802.1X SSIDs. This issue is observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-219791	The aggressive scanning mode under ARM profile settings is enabled by default. This issue is observed in APs running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-221308	The **execute-cli** command does not work as expected for a few show commands. This issue is observed in Mobility Conductors running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-228445	9012 Branch Gateways running AOS-W 8.6.0.4 or later versions do not show **Usage** and **Throughput** information in the WebUI, under **Overview** > **WAN** > **WAN SUMARRY**. A **No data to display right now** error message is shown.	AOS-W 8.6.0.4
AOS-228704	A few APs running AOS-W 8.6.0.15 or later versions crash and reboot unexpectedly. The log file lists the reason for event as **Reboot Time and Cause: Reboot caused by kernel panic: Take care of the TARGET ASSERT first**.	AOS-W 8.6.0.8

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-229024	Some OAW-AP505 access points running AOS-W 8.7.1.5 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **PC is at wlc_mbo_parse_ie+0x15c/0x2b0 [wl_v6]**.	AOS-W 8.7.1.5
AOS-229770	Controllers may not display information on 802.1 connection statuses if 802.1 connection fails. This issue is observed on devices running AOS-W 8.7.1.8 or later versions.	AOS-W 8.7.1.8
AOS-229828	Some managed devices face issues while supporting weak ciphers during SSL/TLS negotiations. This issue is observed in managed devices running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-230156	Due to some users' misconfiguration, some virtual Mobility Conductors running AOS-W 8.6.0.13 or later versions do not retrieve any VLAN IP information in a cluster setup.	AOS-W 8.10.0.7
AOS-231283	The log files of few Wi-Fi 6E APs incorrectly display the 6 Ghz radio 2 disabled due to mfg configuration message during reboot of the APs, even though the 6 GHz radio is not disabled when the APs boot up. This issue is observed in OAW-AP630 Series and OAW-AP650 Series access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232092	Some AP-305 and OAW-AP505 access points are not discoverable by Zigbee devices. The southbound traffic is giving the error **apNotFound**. This issue is observed on devices running AOS-W 8.8.0.1 or later versions.	AOS-W 8.8.0.1
AOS-232208 AOS-241285	The **Maintenance** > **Software Management** > **Upload AOS image for controller** page of the WebUI does not allow image upgrades in OEM builds, yet the WebUI displays it as an option. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232233	Some OAW-4104-LTE switches cache the LAN side MAC address during boot up, preventing the gateway from getting an IP address from the modem. This issue is observed in devices running AOS-W 8.7.0.0 later versions.	AOS-W 8.7.0.0
AOS-232443	Server derivation rules are not assigned correctly and an error message **Missing server in attribute list** is displayed. This issue occurs when there is a delay in response from the RADIUS server. This issue is observed in stand-alone controllers running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-232717 AOS-245030 AOS-243103	The VPNC crashes and reboots with reboot cause: **Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:60)**. This issue is observed in VPNCs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-232733 AOS-236309 AOS-237431 AOS-237795 AOS-237631	Some access points crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. This issue is observed in OAW-AP535 access points running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-232875 AOS-239469	The **mon_serv** process crashes in certain high-load scenarios, particularly with a large number of APs and users with high roaming rates. The issue occurs in OmniAccess Mobility Controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232897	The **wlan ht-ssid-profile** command overrides radio frequencies from 80 MHz to 40 MHz, although the **show ap bsstable** command displays the radio frequencies as 80 MHz. This issue is observed in OAW-AP515 and OAW-AP535 access points running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-232997	Some managed devices running AOS-W 8.7.1.9 or later versions are stuck after an upgrade and the **aaa** process crashes.	AOS-W 8.7.1.9
AOS-233582	The licensing server fails to update the IP address of the secondary Mobility Conductor. This issue occurs when the secondary Mobility Conductor becomes the primary Mobility Conductor. This issue is observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-233809	Users are unable to add GRE tunnels to a tunnel group and the incorrect error message **Error: Tunnel is already part of a different tunnel-group** is displayed. This issue is observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-234315	A few APs sent PAPI messages to external IP addresses, and the logs displayed a random IP address for the **PAPI_Send failed** error message. This issue is observed in APs running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-236171	Some OAW-AP635 access points running AOS-W 8.10.0.5 or later versions crash due to a PoE power supply change from AF to AT.	AOS-W 8.10.0.5
AOS-236200	Some OAW-AP374 access points configured as mesh crash with reason: **kernel panic: Fatal exception**. This issue is observed in switches running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-236380	Some OAW-AP535 access points running 8.7.1.7 or later versions crashed repeatedly. The log files list the reason for the issue as**: Reboot caused by kernel panic: Fatal exception. AP rebooted caused by warm reset**.	AOS-W 8.7.1.7
AOS-236471	Alcatel-Lucent OAW-4740 switches running AOS-W 8.10.0.1 or later versions do not show the configured banner information in GUI login page.	AOS-W 8.10.0.1
AOS-236852	The error log: **ofa: |ofa| ofa_gsm_ event_user_ process: port not found:19, tnm50c4ddb3b194 end point is not configured or is down** is displayed when a client connects to an IAP-VPN tunnel. This issue is observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-236889 AOS-243540	Some managed devices running AOS-W 8.5.0.13 or later versions are unable to fetch user information through controller API calls. The **show user** command output often states: **This operation can take a while depending on number of users. Please be patient**, with no following response.	AOS-W 8.5.0.13
AOS-237174	Some 9240 switches record informational logs, even though the system log level is configured as **warning**. This issue is observed in 9240 switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-237348	Some switches record information logs, even though the system log level is configured as warning. This issue is observed on Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 10.0.2
AOS-237479	Some APs running AOS-W 8.7.1.7 or later versions are unable to form standby tunnels with the cluster nodes. This issue occurs due to a race condition.	AOS-W 8.7.1.7
AOS-238407	AppRF application or application category ACL is not blocking YouTube on devices connected to APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-238727	Users are unable to reset the IPsec MTU value through the **no crypto ipsec mtu** command. This issue is observed on Mobility Conductors running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-238846	The error message **Exceeds the max supported vlans 128** displays when creating layer 2 VLANs at folder level. This issue is observed in Mobility Conductors running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-239382	Some OAW-4750XM Mobility Conductors running AOS-W 8.7.1.9 or later versions configured in a cluster setup crash and reboot unexpectedly. The log files list the reason for the event as **Datapath timeout (SOS Assert)**.	AOS-W 8.7.1.9
AOS-239492	APs are rebooting randomly. The log file lists the reason for the event as **Reboot Time and Cause: AP rebooted Tue Oct 11 21:49:53 CEST 2022; Critical process /aruba/bin/sapd [pid 32165] DIED**, process marked as RESTART. This issue is observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239521	Users are unable to add a tunnel to a tunnel group and an error message is displayed: **Error: All tunnels must have same vlan membership.** This issue occurs when the VLANs are configured in a different order when compared to the order configured for other tunnels in the same group. This issue is observed in managed devices running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-239724	Some APs unexpectedly increase the response times when using a DHCP configuration. This issue is observed in APs running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-239814 AOS-239815	In some controllers running AOS-W 8.6.0.11 or later versions, IPv4 and IPv6 Accounting Messages use the same session ID with Passpoint. This causes multiple accounting messages to be sent repeatedly.	AOS-W 8.6.0.11
AOS-239872	WebUI does not allow users to live upgrade a cluster. However, the CLI allows users to upgrade to a cluster. This issue occurs when the name of the cluster contains spaces. This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.10.0.4
AOS-241212	Some OAW-4650 controllers running AOS-W 8.10.0.4 or later versions crash and reboot unexpectedly. The log files list the reason for the event as: **Nanny rebooted machine - low on free memory**.	AOS-W 8.10.0.4
AOS-242003	Moving files from OmniAccess Mobility Controllers to FTP using API POST causes the error: **/mm/mynode" COMMAND: -- command execution failed**. This issue is observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242635	When using the **Submit As** button or de-selecting options, the de-selected options are not generated properly. This issue is observed in devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-242888	OmniAccess Mobility Controllers are unable to use SSH when IPv4 fourth octet is 0 or 255. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-243266	APs upgraded through TFTP get stuck in **Upgrading** status due to an incorrect automatic change of UDP ports. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.20 or later versions	AOS-W 8.6.0.20
AOS-243536	Some OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions display incorrect values in **Discovery State** and **Transport State** for AirGroup services, after running the **show airgroup switches** command. This occurs due to a race condition. Therefore, users connected to the affected APs are unable to use AirGroup services.	AOS-W 8.10.0.6
AOS-244167	OmniAccess Mobility Controllers are incorrectly sending ACK messages for RFC-5176 Disconnect-Message Request on Bridge Mode which is not supported. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244210	Users are unable to configure a negative value for the transmit power setting in the **Overview** > **Profiles** > **IoT Profile** > **BLE Transmit Power** page of the WebUI. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244659	Some clients experience unexpected issues while roaming when the OpenFlow protocol is enabled. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-244965	An unnecessary debugging log appears as **Received ICMP (DEST_UNREACH, PROT_UNREACH) from X.X.X.X for heartbeat tunnel**. This issue is observed in controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-245001	The **wired aaa-profile** configuration disappears after reload due to incorrect case sensitive checks. This issue is observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245334	Some RAPs are intermittently bootstrapping. This issue is observed in OAW-AP503H and OAW-AP303H access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-245401	HE bit is set on beacon and probe response for **2.4GHz** radio even though the HE knob is disabled from the configuration. This issue is observed in OAW-AP500 Series access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6

Table 7: *Known Issues in AOS-W 8.10.0.8*

New Bug ID	Description	Reported Version
AOS-245656	In the **Configuration** > **Interfaces** > **Ports** page of the WebUI, the port configuration is not displayed. This issue is observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245657	The **show airmatch optimization** command incorrectly displays the sequence number, showing 4 digits instead of 5. This issue is observed in controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.11
AOS-245853	Managed devices are ignoring Radius VSA for Aruba-Admin-Role in a cluster environment. This issue is observed in managed devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245931	In the **Configuration** > **System** > **Logging** page of the WebUI, the error **Duplicate combination of IP address and Category** is displayed when adding arm-user-debug entry if arm entry already exists. This issue is observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7

Chapter 9
Upgrade Procedure

This chapter details software upgrade procedures. It is recommended that you schedule a maintenance window for the upgrade.

CAUTION

Read all the information in this chapter before upgrading your Mobility Conductor, managed device, or stand-alone switch.

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Conductor Licensing Guide*.
- With the introduction of the Long Supported Release (LSR) and Short Supported Release (SSR) terminology in AOS-W 8.10.0.0, a Mobility Conductor running an LSR release supports managed devices running the same release and the three preceding releases. This is considered as N-3 support. This allows a customer to run the latest LSR, the previous SSRs and the previous LSR simultaneously. A Mobility Conductor running an SSR release supports managed devices running the same release and the two preceding releases. This would be considered N-2 support and is the same behavior as the pre-AOS-W 8.10.0.0 MultiVersion support.

- Only for the AOS-W 8.10.0.0 LSR release, AOS-W 8.6.0.0 is treated as an LSR despite being beyond N-3. As such a Mobility Conductor running AOS-W 8.10.0.0 supports managed devices running AOS-W 8.10.0.0, AOS-W 8.9.0.0, AOS-W 8.8.0.0, AOS-W 8.7.0.0 and AOS-W 8.6.0.0.

Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. Following are best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 37 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 37 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 37 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

In certain situations, a reboot or a shutdown could cause the managed device to lose the information stored in its flash memory. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

From the Mobility Conductor, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups.

In the CLI

```
(host) #delete filename <filename>
```

Low Free Flash Memory

Sometimes, after extended use, the flash memory might get used up for logs and other files. The AOS-W image has increased in size and this may cause issues while upgrading to newer AOS-W images without cleaning up the flash memory.

Prerequisites

Before you proceed with the freeing up the flash memory:

- Ensure to always backup the configuration and flash memory. Issue the **backup configuration** and **backup flash** commands to backup the configuration and flash.
- Copy the **flashbackup.tar.gz** and **configbackup.tar.gz** files out of the switch. Then delete the **flashbackup.tar.gz** and **configbackup.tar.gz** files from the flash memory of the switch.
- Use only one partition for the upgrade activity and keep the other partition unchanged.

If you use the WebUI to perform an upgrade, a banner on the **Maintenance** page provides the following reminder to have sufficient free flash memory before initiating an upgrade.

For a healthy and stable system it requires free space of 360 MB for AOS v8.3 and 8.5, 570 MB for AOS 8.6 and 8.7 and 450 MB for AOS 8.8 and higher version in the /flash directory. Please make sure minimum required memory is available in /flash before upgrading to newer version.

Freeing up Flash Memory

The following steps describe how to free up the flash memory before upgrading:

1. Check if the available memory in **/flash** is greater than the limits listed in Table 8 for all supported switch models:

Table 8: *Flash Memory Requirements*

Upgrading from	Upgrading to	Minimum Required Free Flash Memory Before Initiating an Upgrade
8.3.x	8.10.x	360 MB
8.5.x	8.10.x	360 MB
8.6.x	8.10.x	570 MB
8.7.x	8.10.x	570 MB
8.8.x	8.10.x	450 MB
8.9.x	8.10.x	450 MB
8.10.x	8.10.x	450 MB

To check the available free flash memory, issue the **show storage** command. Following is the sample output from a switch with low free flash memory:

```
(host) [mynode] #show storage
Filesystem              Size    Available       Use     %       Mounted on
/dev/usb/flash3         1.4G    1014.2M         386.7M  72%     /flash
```

2. If the available free flash memory is less than the limits listed in Table 8, issue the following commands to free up more memory.
   - **tar crash**
   - **tar clean crash**
   - **tar clean logs**
   - **tar clean traces**

3. Issue the **show storage** command again to check if the available space in **/flash** is more than the minimum space required for AOS-W upgrade as listed in Table 8
4. **If you are unable to free up sufficient flash memory, contact Technical Support. Do not reboot the switch.**
5. If sufficient flash memory is available, proceed with the standard AOS-W upgrade. See Upgrading AOS-W.
6. If a reboot was performed, you may see some of the following errors. Follow the directions below:
   - Upgrade using standard procedure. You may see some of the following errors:

     Error upgrading image: Ancillary unpack failed with tar error (tar: Short header).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Ancillary unpack failed with tar error (tar: Invalid tar magic).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Need atleast XXX MB space in /flash for image upgrade, please clean up the /flash and try upgrade again.

     Failed updating: [upgradeImageNew.c] extractAncTar (dev: /dev/usb/flash1 imgLoc: /flash/config/ArubaOS_70xx_8.8.0.0-mm-dev_78066
   - If any of the above errors occur, issue the **show image version** command to check for the default boot partition. The partition which was upgraded should become the default partition. Following is the sample output of the **show image version** command:

```
(host) [mynode] #show image version
----------------------------------
Partition               : 0:0 (/dev/usb/flash1) **Default boot**
Software Version        : AOS-W 8.9.0.0 (Digitally Signed SHA1/SHA256 - Production
Build)
Build number            : 81046
Label                   : 81046
Built on                : Thu Aug 5 22:54:49 PDT 2021
----------------------------------
Partition               : 0:1 (/dev/usb/flash2)
Software Version        : AOS-W 8.7.0.0-2.3.1.0 (Digitally Signed SHA1/SHA256 -
Developer/Internal Build)
Build number            : 0000
Label                   : arpitg@sdwan-2.3_arpitg-3-ENG.0000
Built on                : Tue Aug 10 15:02:15 IST 2021
```

   - If the default boot partition is not the same as the one where you performed the upgrade, change the default boot partition. Issue the **boot system partition <part_number>** command to change the default boot partition. Enter **0** or **1** for **part_number** representing partition 0:0 or partition 0:1, respectively.
   - Reload the switch. If any of the errors listed in step 4 were observed, the following errors might occur while booting AOS-W 8.9.0.0.

```
Sample error:
[03:17:17]:Installing ancillary FS                    [ OK ]
Performing integrity check on ancillary partition 1   [ FAIL : Validating new
ancillary partition 1...Image Integrity check failed for file
/flash/img1/mswitch/sap/arm32.ari. Digest Mismatch]
Extracting Webui files..tar: Short read
chown: /mswitch/webui/*: No such file or directory
chmod: /mswitch/webui/wms/wms.cgi: No such file or directory
```

   - After the switch reboots, the login prompt displays the following banner:

```
********************************************************************
```

```
* WARNING:  An additional image upgrade is required to complete the *
* installation of the AP and WebUI files. Please upgrade the boot    *
* partition again and reload the controller.                         *
*********************************************************************
```

- Repeat steps 1 through 5. If sufficient free flash memory is available, proceed with the standard AOS-W upgrade procedure. See Upgrading AOS-W.
- If sufficient free flash memory is not available, issue the **dir** and **dir flash** commands to identify large files occupying the flash memory.
- > Exercise caution while deleting files. Contact Technical Support if you are not sure which large files in the **/flash** directory could be safely deleted to free up the required space.

  Issue the **delete filename <filename>** command to delete large files to free more flash memory.
- Check if sufficient flash memory is free as listed in Table 8.
- Proceed with the standard AOS-W upgrade procedure in the same partition. See Upgrading AOS-W.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the flash memory to an external server or mass storage device. You should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Log files
- Flash backup

Backing up and Restoring Flash Memory

You can backup and restore the flash memory using the WebUI or CLI.

In the WebUI

The following steps describe how to back up and restore the flash memory:

1. In the Mobility Conductor node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the flash memory to the **flashbackup.tar.gz** file.
3. Click **Copy Backup** to copy the file to an external server.

   You can copy the backup file from the external server to the flash memory using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the flash memory, navigate to the **Maintenance > Configuration Management > Restore** page and click **Restore**.

In the CLI

The following steps describe how to back up and restore the flash memory:

1. Execute the following command in the **enable** mode:

```
(host) #write memory
```

2. Execute the following command to back up the contents of the flash memory to the **flashbackup.tar.gz** file.

```
(host) #backup flash
Please wait while we take the flash backup.......
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```

3. Execute either of the following command to transfer the flash backup file to an external server or storage device.

```
(host) #copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>


(host) #copy flash: flashbackup.tar.gz usb: partition <partition-number>
```

You can transfer the flash backup file from the external server or storage device to the flash memory by executing either of the following command:

```
(host) #copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz

(host) #copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
```

4. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the flash memory.

```
(host) #restore flash
Please wait while we restore the flash backup........
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 34.

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message is displayed ccurs when you upgrade using the WebUI and navigate to the **Configuration** tab after the managed device reboots. This message disappears after clearing the Web browser cache.

In the WebUI

The following steps describe how to upgrade AOS-W from a TFTP server, FTP server, or local file.

1. Download the AOS-W image from the customer support site.
2. Upload the AOS-W image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-W image:
    a. Download the **Alcatel.sha256** file from the download directory.

    b. Load the AOS-W image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.

    c. Verify that the output produced by this command matches the hash value found on the customer support site.

NOTE

The AOS-W image file is digitally signed and is verified using RSA2048 certificates preloaded at the factory. The Mobility Conductor or managed device will not load a corrupted AOS-W image.

4. Log in to the AOS-W WebUI from the Mobility Conductor.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

NOTE

The upgrade does not take effect until reboot. If you chose to reboot after upgrade, the Mobility Conductor or managed device reboots automatically.

9. Select **Save Current Configuration**.
10. Click **Upgrade**.
11. Click **OK**, when the **Changes were written to flash successfully** message is displayed.

In the CLI

The following steps describe how to upgrade AOS-W from a TFTP server, FTP server, or local file.

1. Download the AOS-W image from the customer support site.
2. Open an SSH session to your Mobility Conductor.
3. Execute the **ping** command to verify the network connection between the Mobility Conductor and the SCP server, FTP server, or TFTP server.

```
(host)# ping <ftphost>
```

or

```
(host)# ping <tftphost>
```

or

```
(host)# ping <scphost>
```

4. Execute the **show image version** command to check if the AOS-W image is loaded on the flash partition. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(host) #show image version
```

5. Execute the **copy** command to load the new image to the non-boot partition.

```
(host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy usb: partition <partition-number> <image filename> system: partition
<0|1>
```

6. Execute the **show image version** command to verify that the new image is loaded.

```
(host)# show image version
```

7. Reboot the Mobility Conductor.

```
(host)#reload
```

8. Execute the **show version** command to verify that the upgrade is complete.

```
(host)#show version
```

Verifying the AOS-W Upgrade

Verify the AOS-W upgrade in the WebUI or CLI.

In the WebUI

The following steps describe how to verify that the Mobility Conductor is functioning as expected:

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 37 for information on creating a backup.

In the CLI

The following steps describe how to verify that the Mobility Conductor is functioning as expected:

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the AOS-W image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 37 for information on creating a backup.

Downgrading AOS-W

A Mobility Conductor or managed device has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the Mobility Conductor or managed device from the other partition.

Pre-requisites

Before you reboot the Mobility Conductor or managed device with the pre-upgrade AOS-W version, perform the following steps:

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 37.
2. Verify that the control plane security is disabled.

3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.

4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

When you specify a boot partition or copy an image file to a system partition, Mobility Conductor or managed device checks if the AOS-W version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the AOS-W version and configuration files.

5. After switching the boot partition, perform the following steps:

- Restore the pre-upgrade flash backup from the file stored on the Mobility Conductor or managed device. Do not restore the AOS-W flash backup file.
- Do not import the WMS database.
- If the RF plan is unchanged, do not import it. If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded AOS-W version.
- If any new certificates were added in the upgraded AOS-W version, reinstall these certificates in the downgraded AOS-W version.

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the AOS-W version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Conductor or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.

a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.

b. From **Select destination file** drop-down list, select **Flash file system**, and enter a file name (other than default.cfg).

c. Click **Copy**.

2. Determine the partition on which your pre-upgrade AOS-W version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade AOS-W version is not stored on your system partition, load it into the backup system partition by performing the following steps:

CAUTION

You cannot load a new image into the active system partition.

a. Enter the FTP or TFTP server address and image file name.

b. Select the backup system partition.

c. Enable **Reboot Controller after upgrade**.

d. Click **Upgrade**.

3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, and click **Reboot**.

The Mobility Conductor or managed device reboots after the countdown period.

4. When the boot process is complete, verify that the Mobility Conductor or managed device is using the correct AOS-W version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the AOS-W version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, use the following command to copy it to the Mobility Conductor or managed device:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
```

or

```
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```

2. Set the Mobility Conductor or managed device to boot with your pre-upgrade configuration file.

(host) # boot config-file `<backup configuration filename>`

3. Execute the **show image version** command to view the partition on which your pre-upgrade AOS-W version is stored.

```
(host) #show image version
```

CAUTION

You cannot load a new image into the active system partition.

4. Set the backup system partition as the new boot partition.

```
(host) # boot system partition 1
```

5. Reboot the Mobility Conductor or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Conductor or managed device is using the correct AOS-W version.

```
(host) # show image version
```

Before Calling Technical Support

Provide the following information when you call the Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with IP addresses and interface numbers.
- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information.