AOS-W 8.10.0.10 Release Notes

Alcatel·Lucent Enterprise

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.

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
Overview

This release includes new features, enhancements, bug fixes, and a regulatory update.

Important Upgrade Information for OAW-41xx Series and 9200 Series switches

Upgrading from AOS-W 8.10.0.6 or earlier 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.

Cluster Rolling Upgrade is not supported when a BIOS upgrade is required. AOS-W 8.10.0.10 must be manually upgraded for these controllers.

Release Date: February 2024

Supported Platforms
End-of-Support
Upgrade Procedure

Important

- As mandated by the Wi-Fi Alliance, AOS-W 8.10.0.0 and later versions require Hash-to-Element (H2E) for 6 GHz WPA3-SAE connections. H2E is supported on Android 12 or later versions, Linux wpa_ supplicant version 2.10 or later versions, macOS Catalina or later versions, Windows 11 or later versions. Users must upgrade their clients to support 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 from AOS-W 8.10.0.6 or earlier 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.

  

  Cluster Rolling Upgrade is not supported when a BIOS upgrade is required. AOS-W 8.10.0.10 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
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 8.10.0.10

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

Added Support for Telematrix IP Phones with OAW-AP505H Access Points

Improved OAW-AP505H PSE port compatibility with early generation Telematrix IP phones.

Enhancement to VAPs

The processing time for manually created VAPs to transition from **interfering** to **valid** has been enhanced.

RADIUS Authentication Server Profile Configurations Added to AirGroup Version 2

The AirGroup version 2 module now accepts RADIUS authentication profile changes such as **nas-IP** and **source-interface** through the **aaa authentication-server radius** command. Rather than depending on the Mobility Conductor's settings, this feature allows for specific authentication-related configurations to be applied to managed devices.

The configuration varies depending on the AirGroup mode used:

- **Centralized mode** requires configurations to be applied on both the Mobility Conductor and managed device. In the case of having different profiles configured, the managed device's profile will take priority.
- **Distributed mode** requires node-specific configuration. In the case of having governing managed devices, the configuration will apply to all member nodes. However, node-specific configuration can still be applied to member nodes if needed.

Clear all Stale AP Records from Mobility Conductor

By using the **clear gap-db ap-name** and **clear gap-db wired-mac** commands, it is now possible to clear AP's in a DOWN state in the Mobility Conductor and all Managed Devices. If needed, issue the **clear gap-db stale-ap ap-name <ap-name> lms lms-ip <lms-ip>** command to clear the a stale entry on a particular managed device.

Behavioral Changes

Removal of ssh-rsa Signature Scheme from SSH Cryptographic Settings

The **ssh-rsa** parameter has been removed to eliminate any security concerns with the SHA-1 hash algorithm and RSA public key algorithm.

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

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP203H Series	OAW-AP203H
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

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577
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_88954

Chapter 7
Resolved Issues in AOS-W 8.10.0.10

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-229828	Some switches faced issues when supporting weak ciphers during SSL/TLS negotiations. This issue was observed in switches running AOS-W 8.7.1.6 or later versions. The fix ensures that the cipher suites can be enabled and disabled as a part of the web server configuration to ensure secure SSL/TLS negotiations.	AOS-W 8.7.1.6
AOS-232445	The PPE configuration was incorrectly displayed as enabled. The fix ensures the PPE configuration is disabled due to a conflict with NSS offload. This issue was observed in OAW-AP530 Series, OAW-AP550 Series, OAW-AP580 Series APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-232527	Some users experienced issues when the deletion of an aged-out IPv4 address for a client inadvertently led to the deletion of all associated IPv6 addresses for the same client. This issue was observed when the **aaa user fast-age** command was enabled. The fix ensures that IPv6 addresses are not idled out when fast-age is enabled. This issue was observed on Mobility Conductors running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-233627 AOS-248613	Some APs were sending broadcast traffic to AAC instead of UAC for split tunnel mode, causing wireless connection issues. The fix ensures broadcast traffic is sent to UAC and APs work as expected. The issue was observed in OAW-AP315 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-234315	A few APs sent PAPI messages to external IP addresses. The log files listed the reason as **PAPI_Send failed**. The fix ensures that the APs display the correct IP addresses in the logs. This issue was observed in APs running AOS-W 8.6.0.15 or later versions in a Mobility Conductor-managed devices topology.	AOS-W 8.6.0.15
AOS-236894	The OmniVista 3600 Air Manager usage graph did not update. The BSSID Tunnel Status on the switches was disabled. Enabling the BSSID Tunnel Statistics through AOS-W commands resulted in an inconsistency, where the standby switch's AMON status was enabled, but the OmniAccess Mobility Controller's remained disabled. The fix ensures the OmniVista 3600 Air Manager graph displays real-time updates. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.7.1.7 or later versions.	AOS-W 8.7.1.7

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-237373 AOS-248873	The OAW-AP655 remote access point crashed unexpectedly when the PMTU value was set to 1200 or 1300 bytes. The log files listed the reason for the event as **PC is at skb_copy_and_csum_bits+0x24/0x274**. The fix ensures the AP works as expected. This issue was observed in OAW-AP655 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-238160 AOS-246310	Some access points running AOS-W 8.10.0.7 or later versions crashed and rebooted unexpectedly. The log files listed the reason of the event as **AP Reboot reason: BadPtr: 00000000 PC: anul_probe_req_find_by_mac+0x88/0x1d4 [anul] Warm-reset**. The fix ensures APs work as expected.	AOS-W 8.10.0.7
AOS-238648 AOS-250171 AOS-247454	The WebUI displayed incorrect Tx station throughput statistics for the client. The fix ensures statistics are accurately shown in the WebUI. This issue was observed in APs running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-239872	WebUI did not allow users to live upgrade a cluster. However, the CLI allowed users to upgrade to a cluster. This issue occurred when the name of the cluster contained spaces. The fix ensures that users are allowed to live upgrade a cluster through the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-240240 AOS-245463 AOS-243291	The output of the **show ap radio-database** command did not display the correct information in the topology of Mobility Conductors and managed devices. The fix ensures the command displays the expected information. This issue was observed in Mobility Conductors and managed devices running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-242126	Managed devices were unable to download images on port 8089. The fix ensures the image can be downloaded successfully. This issue was observed in managed devices running AOS-W 8.10.0.5-FIPS or later versions.	AOS-W 8.10.0.5
AOS-242429 AOS-248682	Some switches failed after a system upgrade from AOS-W 6.5.x to 8.7.1.4 or later versions. Upon reboot, the error **Failed to set port as trusted, err=Module Process handling LAG and LACP functionality is busy. Please try later** was displayed. The fix ensures this error is no longer displayed. This issue was observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.10.0.7
AOS-243033	In some switches, the associated access points randomly disconnected. This issue occurred in a cluster setup with the **Bypass** function enabled where the AP would not try to re-authenticate. The tunnel to **Active AP Anchor Controller** was maintained, but the tunnel to the **Standby Active AP Anchor Controller** was dropped. This caused that the client devices were unable to pass traffic. The fix ensures **dot1x** authentication is restored in this scenario. This issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-243408	Some APs crashed and rebooted unexpectedly when powered by POE AF. The log files listed the reason as **Kernel panic - not syncing: Take care of the TARGET ASSERT first**. The fix ensures the APs work as expected. This issue was observed in access points running AOS-W 8.10.0.0.	AOS-W 8.10.0.7
AOS-243440 AOS-246926 AOS-247219 AOS-248180 AOS-248919	Some OAW-AP535 access points crashed and rebooted unexpectedly. The log files listed the reason of the event as **Kernel panic: "Take care of the TARGET ASSERT first"**. The crash-info displays **TARGET ASSERT occurred at ar_wal_ monitor.c:911**.The fix ensures the APs work as expected. The issue was observed in access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-243720	The WebUI did not display the correct output for the **show wms ap list** and **show wms rogue-ap list** commands. The fix ensures that the correct information is displayed in the WebUI. This issue was observed in Mobility Conductors running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-243789	Some access points crashed and rebooted unexpectedly. The log files listed the reason as **ar_wal_tx_send.c:8479 Assertion buffer_id == WAL_BUFFERID_TX_HOST_DATA_EXP || buffer_id == WAL_BUFFERparam0 :zero, param1 :zero, param2 :zero**. The fix ensures the access points work as expected. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244334 AOS-247602 AOS-247934	Some access points incorrectly displayed their power supply type as DC despite being connected to a PoE switch port and without DC supply. The fix ensures the AP displays its power supply type correctly. As a result, when client devices connected to the AP, power consumption exceeded the 802.3af limit, which in turn caused the AP to reboot. This issue was observed in OAW-AP655 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-244373	Some OAW-AP377 access points in as mesh topology with **opmode open-system** intermittently lost connectivity to the switch within an hour. The fix ensures the access points work as expected. This issue was observed in access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244576	The datapath route-cache information for L3 GRE tunnels was lost unexpectedly. This was caused as the IPSec tunnel pointed to the wrong IP address whenever it went down and re-established itself, causing uplink issues on the network. The fix ensures uplink works as expected. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-244949 AOS-249560	Some APs crashed and rebooted due to a mismatch in **Pending twt sessions** count and **current twt session** issues. This fix will count the number of **pending twt sessions** properly so that mismatch does not occur during WMI event-send instance. This fix ensures that the APs perform as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-245034	Some switches running AOS-W 8.10.0.5 or later versions unexpectedly crashed due to a memory leak issue of the FPAPPS process. The fix ensures switches work as expected.	AOS-W 8.10.0.5
AOS-245153	Some users were unable to send the AirGroup service configurations to Mobility Conductors. The fix ensures AirGroup configurations are sent to Mobility Conductors. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-245499	switches returned the wrong number of associated clients per SSID. This issue was related to an error in the SNMP table population process. The fix ensures the correct number of associated clients is returned by the switch. This issue was observed in switches running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21
AOS-245756	In some OAW-4008 switches, users that connected to a guest SSID were gaining access to the switches's WebUI through an IP address. Users were assigned a user role, under which the Access Control List was granting the access to the switches's WebUI. The fix ensures the correct privileges are assigned to these clients. This issue was observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-245788	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the crash as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The crash-info shows **TARGET ASSERT** occurred at **PC:0x00000000**. The fix ensures APs work as expected. The issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246176	When the auth process was unable to classify a client, the **Client Device Type** and **Client OS** version was displayed empty in the CLI. As a result, ClientMatch did not apply default settings. The fix ensures the process works as expected. This issue was observed in access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-246184	Some access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **ar_wal_tx_sch_status.c:645 Assertion (PPDU_QUEUE_ID(tx_ctxt) != TX_INVALID_QUEUE || PPDU_SCH_ID(tx_ctxt)**. The issue was related to the AP image version, which has been updated to fix the problem. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-246198	Some users received the error **There is no IP address configured for Vlan 220** when attempting to ping from a source VLAN. The issue occurred even if the L3 interface was configured correctly and the VLAN was up and running. The fix ensures the ping works as expected. This issue was observed in managed devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246358 AOS-243849	Provisioning failed for the UAC-AP when changing the CPsec mode from enable to disable.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
	This fix ensures the UAC-AP tunnel can be deleted correctly when keepalive timeout, and ensures the provision succeeds after disable the CPsec. This issue was observed in access points running AOS-W 8.10.0.6 or later versions.	
AOS-246557 AOS-246902 AOS-248917	Some OAW-AP635 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic with "dog_hb.c:210 DOG_HB detects starvation of task "WLAN RT0", triage with its owner(d.dump 0x4af49e00)"**. The fix ensures the APs work as expected. The issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246573	Some access points reported the maximum EIRP value on the 5 GHz radio inaccurately. The issue was related to the AP driver, which has been updated to fix the problem and report accurate maximum EIRP values. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246604	NVDA reader displayed toggle buttons as blank when the user selects the button. The fix ensures WebUI toggle buttons display as expected. This issue was observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-246628	Clients reported slow speed when connected to any of the SSIDs in the overlay network. The fix ensures that the uplink and downlink throughput is as expected. This issue was observed on the 5GHz radio on APs running AOS-W 8.6.0.23 or later versions.	AOS-W 8.6.0.23
AOS-246674	The NVDA reader did not announce WebUI links when the user selected the link. The fix ensures the links are announced as expected. This issue was observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-246730	Some OAW-AP535 access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **Reboot caused by kernel panic Take care of the TARGET ASSERT first (wlan_peer.c:3218 Assertion (vdev->bss->ni_chan.phy_mode >= peer_ratectrl_params.phymode)**. The fix ensures the access points work as expected. The issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246836	In some Mobility Conductors, it was not possible to add the OAW-4240-base switch. When attempted, the following errors displayed **Error 1 : Device (mac add) addition failed. Some effective configuration is not compliant to new device model** and **Error 2 : Device (mac add) addition failed. Configured VLANs count at Managed Network exceeds the max supported vlans-1**. The fix fix ensures this model can be added successfully in a MM-MD setup. This issue was observed in Mobility Conductors running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-246884	Some managed devices failed to download certificates when the name had a 31-character length in the **Configuration > System > Certificate** page of the WebUI. The fix ensures the certificates are downloaded as expected. This issue was observed in managed devices running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21
AOS-246929 AOS-248115 AOS-250304	Some APs crashed and rebooted due to TWT issues. The log files listed the reason for the crash as **dog_hb.c:210 DOG_HB detects starvation of task "WLAN_SCHED0", triage with its owner (d.dump 0x4b542f70)**. The fix ensures APs work as expected. The issue was observed in access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-246937	The mDNS module of switches crashed multiple times which caused an abnormal number of restarts. The fix ensures the switches work as expected. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247070	Some switches crashed and rebooted with the reason **Datapath timeout (Intent:cause: 86:56)**. The crash was related to sessions deleted due to a QAT response timeout. The fix ensures the switches work as expected. This issue was observed in OAW-4104 switches running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-247142 AOS-246453 AOS-247218 AOS-248231	Some OAW-AP535 and OAW-AP635 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic with "cmnos_ thread.c:3850 Assertion 0 failed"**. The fix ensures the APs work as expected. The issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247206	The OAW-AP535 access points had an EAP non-complete issue. The fix ensures the software works as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247326	The output of the **show running configuration** command displayed VLAN IDs and descriptions on separated lines instead of one. The fix ensures the information is displayed as intended. This issue was observed in managed devices running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-247335 AOS-247335 AOS-247967 AOS-248500 AOS-249709	Some 9240 Gateways rebooted with reason **Reboot Cause: Datapath timeout (Intent:cause: 86:56)**. This issue occurred due to passing DPI packets to CPU with id **0**. The fix ensures that these packets are not sent to the DPI engine. This issue was observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-247371	Some Korea-located APs detected false **typeid 43** radars due to an outdated DFS driver. The fix includes a patch with the latest Korean DFS standard, which eliminates these false detections. 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 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-247387	The **Configuration > Access Points > Allowlist** section of the WebUI did not appropriately sort the AP allowlist by **Name** when the entry list exceeded one page. The fix ensures that sorting works appropriately across all pages. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247457 AOS-248519 AOS-249153	Some OAW-4850 switches unexpectedly crashed. The log files listed the reason as: **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20)**. The fix ensures the controllers work as expected with ipv6 configurations and connections. This issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-247551	The output of the **show aaa auth-survivability-cache** command displayed station names in uppercase. The fix ensures the output is displayed in lowercase where expected. This issue was observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-247611	Some switches were displaying different channel assignments causing APs to not broadcast the datazone SSID. The fix ensures the correct information is displayed. This issue was observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-247648	Some OAW-AP315 access points incorrectly displayed an **r** flag in the standby AP Anchor (SAAC) switch when running the **show ap database** command. The issue occurred due to a regulatory domain mismatch between the primary and standby switches. The fix ensures **r** flags are displayed correctly in SAAC. This issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247727	**Netdestination** whitelist was not working on branch gateways. This issue occurred due to the DNS IP list not being cleared every 24 hours for x86 platforms. This resulted in the DNS IP table getting full and subsequently causing DNS IP allocation failures. The fix ensures that the DNS IP list is cleared at regular intervals. This issue was observed in branch gateways running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-247819	In SNMP walks IPv6 clients with no IP address caused that the SNMP table was not ended rightly, As a result, the OID was not increasing and the SNMP walk stopped and did not move the next client. The fix ensures the SNMP walk performs as expected in this scenario. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247823	Wired clients connected to some OAW-AP515 access points were unable to authenticate and were not seen on the switch. This issue was observed in Campus APs with multizone profile enabled on the AP. The fix ensures wired clients connect as expected in this scenario. This issue was observed in APs running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-247832	Some switches unexpectedly crashed and rebooted with the reason **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause: 86:34)**. The issue was related to the **ipv6 helper-address** parameter causing the crash when configured through the **interface vlan** command. The fix ensures the **ipv6 helper-address** configuration works as expected and does not cause the switch to crash. This issue was observed in 9240 switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-247899	AirGroup clients were unable to discover wired servers or they were not found in the server list under client device. This occurred due to an error in clearing entries of old users and, hence, no space for new users. The fix ensures old entries are deleted properly and entries are available for users with all information required to respond to client queries. This issue was observed in Mobility Conductors running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-248092	Some APs displayed their SSID incompletely if there were more than 31 characters when using an XML API query due to the location field being truncated. The fix ensures the SSID displays correctly. This issue was observed in APs running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248178 AOS-250372	The **Diagnostics > Tools > Spectrum Analysis** page of the WebUI did not display any data when a sensor from the **Connected Sensors** list was selected. The graphs displayed the message **No data to display**. However, this information was available through the CLI. The fix ensures the sensor data is displayed accurately in the WebUI. This issue was observed in switches running AOS-W 8.10.0.9.	AOS-W 8.10.0.9
AOS-248203 AOS-250675	Some AP-654 and AP-605 access points randomly crashed when configured in a 6 GHz mesh. This issue occurred due to a loop in the mesh link status. The fix ensures the access points work as expected. This issue was observed in access points running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-248337	Multiple APs failed to upgrade to AOS-W 8.10.0.7, causing rebootstraps and high CPU load. This issue was caused due to a calculation error when a large amount of ESSIDs were configured. The fix ensures the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248371	The OAW-4750XM switch failed to copy out **crash.tar** when the file size was larger than 2 GB. The fix ensures the switch works as expected. This issue was observed in OAW-4750XM switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248473	In some OAW-AP535 access points the **ANI Desense level (Min)** went higher than **ANI Desense level (Max)** level. This issue occurred due to a regulatory limitation. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-248537	PMF frames from client were corrupted by switch while decrypting and forwarding them to AP when client was connected to WPA3 Enterprise (GCM) (256 bit) Tunnel Mode SSIDs. As a result, devices experienced low throughput. This issue was observed in 9000 Series switches and VMC controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-248680 AOS-248673 AOS-249682 AOS-250174 AOS-250197 AOS-250829 AOS-249589	Some OAW-AP515 and OAW-AP575 access points crashed, rebooted and reconnected to the network. The log files listed the reason for the event as: **BUGSoftLockup:CPU#1 stuck for 22s! [kworker/1:3:27856] PC:wlc_bmac_suspend_mac_and_ wait+0x21c/0x440 [wl_v6**. This issue occurred on a MCR-MD setup after upgrading to from AOS-W 8.10.0.7 to AOS-W 8.10.0.8. The fix ensures the access points perform as expected. This issue was observed in access points running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248742	A BSSID mismatch was occurring during WPA3 SAE authentication, resulting in frames being sent to incorrect access points. The fix ensures that the values match. This issue was observed in switches running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248891	Some OAW-AP515 access points unexpectedly crashed and rebooted. The log files listed the reason for the event as **BadPtr:000000d8 PC:wlc_ampdu_dotxstatus_ regmpdu+0x700/0xba0**. The fix ensures the APs 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
AOS-248925	In the**System > General > Clock** page of the WebUI, the **Timezone** and **Date and Time** did not display the correct configuration. The fix ensures the correct information is displayed. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248972	Some OAW-AP534, OAW-AP535, OAW-AP555, AP-634, OAW-AP635 and OAW-AP655 access points unexpectedly rebooted. The log files listed the reason for the reboot as **Reboot caused by WLAN firmware TARGET ASSERT at twt_ap.c:847**. The fix ensures the access points work as expected. This issue was observed in access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-249123	Some switches crashed unexpectedly due to the **impystart** process. The fix ensures the process works as expected. The issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-249253	APs failed to establish standby tunnels upon DHCP failure which caused datapath user, route and route-cache information to be removed. The fix ensures the APs work as expected. This issue was observed in access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-249565	After an upgrade to 8.10.0.9, Central On-Premises was unable to monitor all managed devices and the error **Unknown Trusted Certificate. Please upload the certificate before configuring in the profile** was displayed when showing the profile error logs. The fix ensures the monitoring works as expected. This issue was observed in switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.9
AOS-249589	In some controllers the STM process was continuously crashing. As a result, it was not possible to terminate access points on the controllers. The fix ensures the controllers perform as expected. This issue was observed in 7210 OmniAccess Mobility Controllers running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-249754 AOS-249851	The SNMP walk failed to retrieve data for the fan tray OID. The fix ensures the fan tray OID is displayed correctly. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249755	Users were able to connect to Mobility Conductors through SSH despite the subnet being disallowed in the ACL port session. The fix ensures only ACL-allowed clients are able to connect. This issue was observed in Mobility Conductors running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249765	Some APs crashed and rebooted due to memory issues. The issue occurs when TWT statistics for pending session do not match the TWT statistics for reported session. The fix ensures that the APs will work as expected. This issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249970	The authentication module crashed repeatedly due to an error with the MAC address that was not validated. The fix ensures that the authentication module in the gateway works as expected. This issue was observed in 9240 switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0

Chapter 8
Known Issues in AOS-W 8.10.0.10

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 8.10.0.10*

New Bug ID	Description	Reported Version
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-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
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 or later versions.	AOS-W 8.7.1.1
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	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-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

Table 7: *Known Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
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-225614	Some OAW-AP505H access points running AOS-W 8.9.0.0 experience poor network bandwidth issues.	AOS-W 8.9.0.0
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-231283	The log files of few Wi-Fi 6E APs (OAW-AP630 Series and OAW-AP650 Series access points) running AOS-W 8.10.0.0 or later versions incorrectly display the **6G 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.	AOS-W 8.10.0.0
AOS-232092	Some OAW-AP305 and OAW-AP505 access points are not discoverable by Zigbee devices. The southbound traffic is giving the error in as **AP not found**. This issue is observed on devices running AOS-W8.8.0.1 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 for 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 controllers cache the LAN side MAC address during boot up. Thus, the gateway does not get an IP address from the modem. This issue is observed in devices running AOS-W 8.7.0.0 later versions.	AOS-W 8.7.1.4
AOS-232443	Server derivation rules are not assigned correctly and the 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 standalone switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
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

Table 7: *Known Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
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-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
AOS-236471	Alcatel-Lucent OAW-4740 controllers 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-237174	Some 9240 switches record informational logs, even though the system log level is configured as warning. This issue is observed in 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 OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.9.0.3
AOS-238407 AOS-236630 AOS-240428 AOS-241047 AOS-243539 AOS-249468	AppRF application or application category ACL is not blocking YouTube on devices connected to APs running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
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
AOS-239382	Some OAW-4750XMMobility 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-239521	Users are unable to add a tunnel to a tunnel group and an error message **Error: All tunnels must have same vlan membership** was displayed. 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

Table 7: *Known Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-239724	Some APs unexpectedly increase the response times when using 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 switches running AOS-W 8.6.0.11 or later versions, IPv4 and IPv6 Accounting Messages are using the same session ID with Passpoint. This causes multiple Accounting Messages to be sent repeatedly.	AOS-W 8.6.0.11
AOS-239850 AOS-249756	Some Mobility Conductors crash unexpectedly due to a memory leak in the **vmsvc** process. The log files list the reason as **[vmsvc] HostinfoOSData: Error: no distro file found**. This issue is observed in Mobility Conductors running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-241212 AOS-241537	Some OAW-4650 switches 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-241560	Accessing switches through the WebUI may lead to excessive logs regarding the **show uplink cellular details** command, including errors stating **Command not applicable for this platform (pos: 0),** which can be safely ignored. This issue is observed in standalone OAW-4650Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242404	The reason and timestamp of APs in a DOWN status is not displayed in the Mobility Conductor Dashbord under **Infraestucture > Access Devices**. The information displayed is **AP is down since - because of the following reason: None** or **AP is down since - because of the following reason: -**. This issue is observed in AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-242532	Some OAW-AP535 access points are not available on OAW-4550switches post power outage. This issue occurs when a USB converter and console cable are used, which interrupts the boot up process and results in the AP not showing up on the switch. The issue is observed in switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
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 8.6.0.17
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

Table 7: *Known Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
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-244218 AOS-245833 AOS-247849 AOS-248640 AOS-249157	Some APs crash and reboot due to memory allocation failure for the trigger frame, which drops the connection. This issue is observed in APs running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0
AOS-244659	Some clients are experiencing unexpected issues while roaming when using OpenFlow protocol. 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-244869	In some access points the 4-way handshake failed when WPA2 key-2 frames were re-transmitted by wireless client. This issue is observed in access points running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
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-245329 AOS-243275	The **resolvwrap** process continuously crashes whenever a VLAN that is set to **dhcp-client** fails to get an IP. This issue is observed in gateways running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-245367	In standalone controllers, it is not possible to configure application speed limit under the **Dashboard > Traffic Analysis > Applications** tab. This feature works if the controller is in Master role, but this error is not reported properly. This issue is observed in controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-245414	SNMP queries to controllers return valid traffic data for GigE interfaces but might show all zeroes for GRE tunnel interfaces. This issue is observed on OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17
AOS-245539	The **Configuration > Roles & Policies > Aliases > Network Aliases** section of the WebUI does not accept the complete set of host names provided when added simultaneously. Instead, only the last input host name is successfully configured. This issue is observed on devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-245777	In the controller **Dashboard**, under **Overview > Clients,** applying the **grouped by signal quality** filter does not correctly organize the client data or display the graph based on signal quality. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.6

Table 7: *Known Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-246103 AOS-247433 AOS-240688 AOS-250837	Some OAW-AP635 and OAW-AP535 access points reboot randomly with **reboot reason - kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_send.c:11778 first**. This occurs due to issues with M3 controllers recovery, to which the APs are connected to. This issue is observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-246606	The NVDA reader calls out only parameters that are not configured under the **Services > Firewall** page of the WebUI. This issue is observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-246960	OmniAccess Mobility Controller upgrades trigger license changes which cause the unintended loss of configured user roles and ACLs in managed devices. This issue is observed in OAW-4010 switches running AOS-W 8.6.0.21 or later versions. As a workaround, reload the managed device or restart the **profmgr** process to fix the issue.	AOS-W 8.6.0.21
AOS-247147	Virtual OmniAccess Mobility Controllers might consistently generate error logs pertaining to the WMS database on a daily basis. This issue is observed on virtual OmniAccess Mobility Controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247721	Mobility Conductor in a standby setup fails over and crashes unexpectedly. The log files list the reason as **Datapath Exception**. This issue is observed in Mobility Conductor running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247793	Some OAW-AP535 access points crash and reboot unexpectedly. The log file lists the reason for reboot as **AP crashed at ar_wal_vdev.c:3320 Assertion vdev_handle->type == WAL_VDEV_TYPE_STA**. This issue is observed in OAW-AP535 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.4
AOS-248151	Some OAW-AP535 access points crash and reboot unexpectedly. The log file lists the reason for reboot as **Ap crashed at sched_algo_txbf.c:1909 Assertion 0 failedparam0 :zero, param1 :zero, param2 :zero**. This issue is observed in OAW-AP535 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-248267 AOS-251592	The RADIUS/RADSec server could not connect to the FQDN host after rebooting the switch, resulting in IP loopbacks. This issue occurs due to replication problems during validation. The issue is observed in standalone switches running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248466	The switch discovery preference field disappears when changing it from ADP to Static, under **Dashboard > Configuration > Access Point > Provision**. This issue is observed in switches running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8

Table 7: *Known Issues in AOS-W 8.10.0.10*

New Bug ID	Description	Reported Version
AOS-248899	The syslog server of some wireless switches is flooded with error messages related to OpenFlow. Logs such as **ofa: <238503> <5843> |ofa| |sdn| ERRS ofml_openflow_mac_bridge_add_ap:322 AP client(mac-address) not found** are repeatedly displayed on switches with varying MAC addresses. These errors are related to roaming when connected to a OAW-RAP, and can be safely ignored. This issue is observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248905	Clients are assigned the wrong role when reconnecting to WPA3 Enterprise (GCM) SSIDs, in both CNSA and non-CNSA mode. The issue is related to PMK caching as part of dot1x authentication. This issue is observed in switches running AOS-W 8.10.0.0 or later versions. **Workaround:** Since this is a PMK caching issue, clearing the cache by using the **aaa authentication dot1x key-cache clear <unk>station-mac>** command solves the problem.	AOS-W 8.10.0.0
AOS-249066 AOS-250718	The **auth** process crashes and reloads, causing connectivity issues when more than 37 dormant IP addresses are associated with a single MAC address. This issue is observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249133	Some switches crash and reboot with **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause: 86:34)**. This issue is caused due to a known memory leak problem within the **fpapps** module. This issue is observed in switches running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-249197	Some AirGroup servers are not discovered by clients. For example, devices such as Mersive Solstice Pods do not appear in Apple clients' screen mirroring device list. This issue is related to AirGroup's refresh logic when using discovery packets, and is seen when there are 9 or more MDNS service profiles configured in the AirGroup profile. This issue is observed in managed devices running AOS-W 8.10.0.7 or later versions	AOS-W 8.10.0.7
AOS-249260	Some Mobility Controller Virtual Appliance deployments crash when running AOS-W 8.10.0.7 or later versions. This issue is observed whenever the CLI password is passed as **NULL**.	AOS-W 8.10.0.7
AOS-249749	Neighbor AP information is incomplete in the output of the **show ap arm state** command. This issue is observed in APs running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-250148	AirGroup's **Transport State** gets stuck on **initializing** status. The issue is related to the current handling of OpenFlow flows in AOS SDN controllers. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Chapter 9
Upgrade Procedure

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

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 36 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 36 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 36 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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 33.

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.

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.

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 36 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 36 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 36.

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:

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
```

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.