AOS-W 8.10.0.9 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
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 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 8.10.0.9 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 8.10.0.9

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

AAC will report AMON link status to other devices

In AOS-W 8.10.0.9, AAC will send AMON AP information messages to indicate the AP's standby AAC information.

Denylist clients in case of a security context override attempt with the denylist-sco-attack parameter

The **aaa-profile** command now accepts the **denylist-sco-attack** parameter, which enables denylisting for clients that attempt to perform a security context override, improving security against malicious authenticated clients. The default value of this parameter is set to **disabled**.

Jumbo Frames Support over IPSec Tunnels

In AOS-W 8.10.0.0 or later versions, jumbo frames support over site-to-site IPSec tunnels, is added for client devices. This enables devices to ping each other and allows larger download sizes.

Implementation of Port Monitoring on x86 Platforms

In AOS-W 8.10.0.9, port monitoring has been implemented on port channels interface on x86 platforms.

Introduction of the show datapath dpi counters command

Starting from AOS-W 8.10.0.9, a new command is being added to the CLI, **show datapath dpi counters**. This command displays additional DPI debug counters to improve debugging,.

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 8.10.0.9.

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_88424

Chapter 7
Resolved Issues in AOS-W 8.10.0.9

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-228598 AOS-246281	The **LINK/ACT** LED of OAW-4104 gateways remained off even when a working LAN cable was connected to the port. The fix ensures the LED works appropriately(solid green when link is established and blinking green when transmitting or receiving data). This issue was observed on OAW-4104 gateways running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-228764	A few OAW-AP655 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as: **PC is at cnss_wait_for_cold_boot_cal_done+0xe0/0x124**. The fix ensures the access points work as expected. This issue was observed in OAW-AP655 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232832 AOS-232962 AOS-233456 AOS-236010 AOS-236698 AOS-237445 AOS-240627 AOS-240765 AOS-241680 AOS-242454 AOS-242648 AOS-242649 AOS-242725 AOS-244622 AOS-245722	Some managed devices crashed and rebooted unexpectedly. The log files listed the reason of the event as, **Reboot Cause: soft Watchdog reset (Intent:cause:register de:86:70:4)**. The fix extracts additional data from the system at the time of the crash for further analysis. This issue was observed in managed devices running AOS-W 8.6.0.1 or later versions.	AOS-W 8.9.0.3
AOS-232997	Some managed devices running AOS-W 8.7.1.9 or later versions were stuck after an upgrade and the **aaa** process crashed. The issue occurred due to memory corruption. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.9
AOS-235285 AOS-242646	Some switches were sending commands from Central??? On-Premises to the APs, but the response was not received. This issue occurred since the port used by the handling process was closed for external communications. As a result, no response was received in **Analyze > Tools > Commands > Device Output** in Central??? UI. The fix ensures that the responses are received as expected. This issue was observed in switches running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-236889 AOS-243540	Some managed devices running AOS-W 8.5.0.13 or later versions were unable to fetch user information through controller API calls. The **show user** command output often displayed: **This operation can take a while depending on number of users. Please be patient**, with no following response. The fix ensures managed devices fetch the data as expected, without displaying the error message.	AOS-W 8.5.0.13
AOS-237479	Some APs were unable to form standby tunnels with the cluster nodes. This issue occurred due to a race condition. The fix ensures the APs work as expected. This issue was observed in access points running AOS-W 8.7.1.7 or later versions.	AOS-W 8.7.1.7
AOS-238424 AOS-247791	Some access points displayed the error, **file amon.c function amon_get_ant_gain line 4223 error invalid band 2**. The issue occurred when the 6 GHz radio band was disabled. The fix ensures the error is not displayed in such cases. This issue was observed in OAW-AP635 and OAW-AP655 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-238729 AOS-241593	In some APs, when the DNS traffic reached the Broadband gateway, the traffic was forwarded upstream but natting did not take place. As a result, the AP did not come online in Central???. The fix ensures the APs display as expected. This issue was observed in APs running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-238803 AOS-246511	switches running AOS-W 8.10.0.7 or later versions logged continuous error messages such as **|web_cc| Failed GSM publish web_cc_gsm_publish**. The fix ensures that the switches' web content classification functionality works as expected	AOS-W 8.10.0.7
AOS-239282	Clients were unable to connect to OAW-AP505H mesh access points. The log files listed the reason for this event as UAC Down. The fix ensures seamless connectivity. This issue was observed in OAW-AP505H mesh access points running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-239417	Some OAW-AP535 access points rebooted due a low memory condition. The reboot cause was **kernel panic: softlockup: hung tasks.** The fix ensures memory is handled properly. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239459 AOS-248389	Mobility Conductors running AOS-W 8.10.0.7 or later versions continuously logged multiple unnecessary errors related to the **mon_serv_fwv process**. The logs pre-fixed the errors as **|mon_serv_fwv| mon_serv_gsm_handle_device_config_add**. The fix ensures these unnecessary logs are not displayed in the CLI.	AOS-W 8.10.0.7
AOS-240026 AOS-236177 AOS-239232 AOS-240068 AOS-240633	Some customers were unable to access controllers through the CLI or WebUI. This issue was related to third-party monitoring tools such as Armis, which caused the CLI sessions to be kept open for a long time accumulating memory leaks, affecting the functioning of the controller. The fix ensures customers are able to access controllers as expected. This issue was observed in controllers running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-241083 AOS-242823	Some access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **ar_wal_tx_de.c:331 Assertion failed**. The issue was related to the AP image version found in previous versions of AOS-W. The fix contains a patch for the AP image that resolves the error. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241150	Branch Gateways running AOS-W 8.10.0.0 or later versions failed to send accounting information during TACACS authentication of management users. This issue occurred because, on gateway reload, the **ctrlmgt** process came up after the TACACS accounting packets were sent from the **auth** process. As a result, the accounting information was lost during authentication. The fix resolves the timing issue between the **ctrlmgt** and **auth** processes after gateway reload.	AOS-W 8.10.0.0
AOS-241158	The running configuration did not match the previous configuration after upgrading from 6.5.x to 8.x versions. The fix ensures that previous configurations are retained when upgrading to 8.x versions. This issue was observed in standalone OAW-4010 controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.19
AOS-241532 AOS-245370	Some Mobility Conductors repeatedly displayed the error message, **WMS PGRES_FATAL_ERROR**, which filled the logs. The fix ensures that the devices operate as expected. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241709	The **auth** process crashed unexpectedly when ACLs and downloadable-user roles assigned to a VIA client were configured from CPPM. 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 8.7.1.5
AOS-241833	OAW-RAPs operating in a dual-stack environment with an IPv4 IPSEC experienced heartbeat loss after IPSEC re-key when IPv6 was inadvertently used. The fix ensures no heartbeat misses are seen on RAPs when IPSEC re-keying happens. The issue was seen on Remote OAW-AP505H access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242003	Moving files from OmniAccess Mobility Controllers to FTP using API POST caused the error: **/mm/mynode" COMMAND: -- command execution failed**. The issue was fixed by adding a missing parameter in the UI mapping table. This issue was 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 were not generated properly. The fix ensures the configuration works as expected. This issue was observed in devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-242888	Users were unable to use the **SSH** command when the fourth octet of the IPv4 address was set to **0** or **255**. The fix ensures that the **SSH** command works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-243714 AOS-246688	The **syslogdwrap** process crashed when configuring the syslog server and the TLS option was not enabled. As a result, incorrect TLS flag values were set. The fix ensures that flag values are set correctly, even when TLS option is not enabled. This issue was observed in some Gateways running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-243888	Some OAW-4750XM switches crashed and rebooted unexpectedly. The issue was related to an STM process crash when several forward-mode bridge profiles were configured. The fix ensures the STM process executes as intended. This issue was observed in OAW-4750XM controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244091 AOS-244610 AOS-246131 AOS-246450	Some OAW-AP534 access points crashed and rebooted unexpectedly. The log files listed the reason of the event as, **Reboot caused by kernel panic: Take care of the TARGET ASSERT first. It's WLAN firmware assert at "wmi_tlv_ helper.c:305 Assertion (in_tlv_len + (1 * sizeof(A_ UINT32)))==attr_struct_ptr.tag_struct_size**).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-244167	OmniAccess Mobility Controllers incorrectly sent ACK messages in response to RFC-5176 Disconnect-Message Requests when in Bridge Mode, which is not supported. The fix ensures that no ACK messages for RFC-5176 are sent. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244231	Option 82 information was missing for the first DHCP discover packet in some controllers running AOS-W 8.11.0.0 or later versions. The fix ensures that the option 82 information is tagged correctly in the first DHCP discover packet.	AOS-W 8.11.0.0
AOS-244384	The Windows 10 Filesharing (SMBv2) download speed was slower when connected to OAW-AP515 access points, or 9240 controllers compared to other devices. The fix ensures an improvement in download speeds. This issue was observed in OAW-AP515 access points and 9240 controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244398 AOS-244429 AOS-244743 AOS-244767 AOS-246357 AOS-247460	The **amon udp** command was used to enable OmniVista 3600 Air Manager to allow traffic on UDP port 8211. Due to security change, PAPI drops some AMON feeds between the Mobility Conductor and Managed Devices. This issue is resolved after deprecating the **amon udp** command. This issue was observed in switches running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-244949	Some APs crashed and rebooted due to mismatch in **Pending twt sessions** count and **current twt session** issues. This fix will sccount the number of **pending twt sessions** properly so that mismatch doesn't occur during WMI event send instance. This fix will ensure that APs perform as expected. This issue was observed in OAW-AP535 AP-535 access points running AOS-W 8.10.0.6 and 8.11.1 or later versions.	AOS-W 8.10.0.6
AOS-245001	The **wired aaa-profile** configuration disappeared after the managed device restarted due to incorrect case sensitive checks. The fix ensures that the **wired aaa-profile** configuration is retained when the device restarts. This issue was observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245094	In some switches running AOS-W 8.6.0.21 or later versions, some Phone home log activity was observed although this feature was disabled. The logs were shown in the output of the **phonehome now** command. The fix ensures no logging activity occurs in this scenario.	AOS-W 8.6.0.21
AOS-245145 AOS-236547	In the WebUI, under **Configuration > Roles & Policies > role > Show Advanced View > Captive Portal**, the preview button for custom HTML captive portal page was not available. The fix ensures the preview button is present. This issue was observed in some OAW-4550 switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245260	Some OAW-AP325 access points were detecting radar signals only in 40 MHz DFS channels. No radar hits were detected when changed to 20 MHz channel. This issue occurred due to wireless interference in the environment. The fix ensures false radar signals are rejected. This issue was observed in APs running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-245334	Some OAW-RAPs were intermittently bootstrapping after a conflict with IP types received. The fix ensures IP types are checked and OAW-RAPs perform as expected. This issue was observed in OAW-AP503H and AP-OAW-AP303H Series access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-245379	Some access points crashed and rebooted unexpectedly. The log files listed the reason as, **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. **It's WLAN firmware crash at "wlan fw crash at sched_algo_qos.c:1530 sched_algo_choose_qos_tid_type".** The fix ensures the access points work as expected. This issue was observed in OAW-AP534, OAW-AP535, OAW-AP555, AP-634, OAW-AP635, and OAW-AP655 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245401	HE capabilities were configured on the beacon and probe response for **2.4GHz** radio even though the **HE** setting was disabled. The fix ensures that HE capabilities are not configured on the beacon and probe response when the **HE** setting is disabled. This issue was observed in OAW-AP500 Series access points running AOS-W 8.9.0.0 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-245409	Some users were unable to pass traffic to the captive portal after a rebootstrap. This issue occurred when APs could not source NAT the traffic due to Back-up LMS having more DNS entries than LMS. When the AP changed LMS to Back-up LMS, the DNS ID table was not downloaded correctly. A correction of the DNS ID table resolved the issue. This issue was observed in access points in split-tunnel mode running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-245516 AOS-246187 AOS-247197 AOS-247520 AOS-247521 AOS-248022	In some AP-634 access points the 5 GHz radio with traffic was continuously resetting. The unexpected number of resets may have introduced packets loss. The fix ensures the APs perform as expected. This issue was observed in devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245519	In some switches running AOS-W 8.10.0.0 or later versions, the system automatically restarted when the system was halted using the LCD menu. The fix ensures switch works as expected without restarting.	AOS-W 8.11.1.1
AOS-245656	In the **Configuration > Interfaces > Ports** page of the WebUI, selecting a port channel displayed the details, but after navigating to physical port, the configuration was not displayed. As a result, the page had to be reloaded. The fix ensures the information is displayed 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-245657	The **show airmatch optimization** command incorrectly displayed sequence of numbers, showing 4 digits instead of 5. The fix ensures that the command's output displays the correct sequence of numbers. This issue was observed in controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.6
AOS-245689	In some switches running AOS-W 8.10.0.7 or later versions, the **HA-flags** value was not shown in the output of the **show ha ap table** command. This fix ensures that this value is populated.	AOS-W 8.10.0.7
AOS-245853	Managed devices were ignoring Radius VSA for **Aruba-Admin-Role**. This issue occurred when authentication management was enabled and performing certificate authentication using the WebUI. The switch was getting updated with wrong role, even though **cppm** sent the correct one. The fix ensures the role is obtained from VSA and is updated accordingly. This issue was observed in devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245874 AOS-246405	Some AP-503 access points crashed and rebooted unexpectedly. The log files listed the reason of the event as, **Panic: MemLeak: mem low for 46593 seconds, under 0MB 927882 times, MB free 8 (1%), total 740 Warm-reset**. The fix ensures the access points work as expected. This issue was observed in access points running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-245931	In the **Configuration > System > Logging** page of the WebUI, the **Duplicate combination of IP address and Category** error was displayed when adding arm-user-debug entry, if arm entry already existed. The fix ensures the error message is not displayed in this scenario. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245939 AOS-245445	In some switches the **ap_crash_transfer_check error** log was generated when core file transfers failed using TFTP. As a result, unnecessary log files were accumulating. The fix ensures the log file is not generated in this scenario. This issue was observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-245976	In some controllers running AOS-W 8.10.0.4 or later versions, the admin management user entry could not be deleted on Mobility Conductors and standalone switches. The issue occurred because the deletion of the admin management user was not allowed nor supported by default. The fix ensures that the admin user can be deleted from Mobility Conductors or standalone switches, if there is at least one root user already configured.	AOS-W 8.10.0.4
AOS-245980	Some clients connected to OAW-AP535 access points on the 5 GHz band experienced significant packet loss to the gateway and increased latency during calls when LACP was enabled on the controller. The issue was observed when both the GRE-Stripping IP was configured and the AP-LACP was activated on the AP. The fix ensures APs work as expected. This issue was observed in access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-246003	Some OAW-AP505 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as: **BadAddr:fecf3ca8 PC:dev_get_iflink+0x0/0x28 Warm-reset**. This issue occurred in an IPsec environment, where a tunneled device was deleted after IPsec encryption. The fix ensures proper validations are made, preventing the AP crash. This issue was observed in devices running AOS-W 8.6.0.21.	AOS-W 8.6.0.21
AOS-246051	Some controllers were unable to copy an image from the flash memory to the system partition. The error seen for this operation was: **Error determining image version**. The fix ensures the controller copies an image successfully. This issue was observed in OAW-4x50 Series controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246097	Some OAW-AP535 access points randomly disabled the ANI feature. The issue was due to an unintended trigger of the ANI periodic check, which disabled the feature. The fix ensures that the ANI feature stays enabled when configured to do so. 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

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-246124 AOS-247640	In some OAW-4750XM switches, a Kernel crash was observed due to an incorrect memory assignment in the **rt6i_node pointer**. The fix converts the direct assignment of **rt6i_node pointer** to **rcu_assign_pointer**, to ensure that the pointer assignment never fails. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246203	Some OAW-AP635 access points unexpectedly rebooted. The log files listed the reason for the event as: **PC is at ieee80211_get_he_bsscolor_info+0xfc/0x7a8 [umac]**. The fix ensures the access points work as expected. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-246263	Mobility Conductors running AOS-W 8.10.0.7 or later versions experienced an unexpected mDNS process crash. The issue was related to buffer data corruption while responding to query packets having sub-ptr records. The fix ensures the mDNS process executes as expected.	AOS-W 8.10.0.7
AOS-246395	The 9240 controllers were not detecting SFP+ transceivers. The fix ensures the modules work as expected. This issue was observed in 9240 controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-246409 AOS-246862 AOS-246945 AOS-247150 AOS-248556	Some access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **FW assert PC:0x4b23a454 : ar_wal_tx_send.c:16021**. The issue was related to the AP image version found in previous versions of AOS-W. The fix contains a patch for the AP image that resolves the error. This issue was observed in OAW-AP500 Series APs running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246583	A OAW-4750XM OmniAccess Mobility Controller experienced unexpected crashes as a result of a failure in the **tnld_node_mgr** process. The fix ensures the process works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246617	After upgrading to AOS-W 8.10.0.7, some APs crashed and rebooted unexpectedly, disconnecting every 2-3 hours due to IPv6 packet synchronization problems. The crash logs listed the reason for the error as **Panic:Ktrace core monitor: cpu3 hung for 45 seconds, hung cpu count: 1 Warm-reset.** The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.21 or later versions.	AOS-W 8.10.0.7
AOS-246839	The usage of ECDSA certificates in a web-server profile caused the unavailability of the WebUI. The fix ensures the WebUI works as expected when using ECDSA certificates. This issue was observed in controllers running AOS-W 8.10.0.7 and 8.10.0.7-FIPS or later versions.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-246966	Some Mobility Conductors crashed and rebooted unexpectedly. The log files listed the reason of the event as, **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2) Supervisor Card.** The crash occurred due to the processing of a corrupted buffer, which was mistakenly interpreted as an IPv6 crypto SA, resulting in a datapath crash. The fix involves validating key parameters in the buffer before processing, thereby preventing the crash. This issue was observed in Mobility Conductors running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247718	Data traffic was not flowing through the tunnels between the APs and the controller, even though the tunnel was restored. The fix ensures data traffic seamlessly flows through the tunnels between devices. This issue was observed access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248121	The AVS process caused OAW-AP577 access points to crash after recovering from low temperatures, the AVS voltage was not high enough. An increase of the AVS default voltage fixed the issue. This issue was observed in OAW-AP577 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-248762	The Web Content Classification process was crashing due to segmentation. The fix ensures the **web_cc** process and its classification functionality works as expected. This issue was observed in switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Chapter 8
Known Issues in AOS-W 8.10.0.9

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 8.10.0.9*

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 Conductor 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 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

Table 7: *Known Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
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
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-226013 AOS-226012	Mobility Controller Virtual Appliance running AOS-W 8.7.1.4 or later versions respond with their own MAC address as the management IP address for ARP requests.	AOS-W 8.7.1.4
AOS-228445	Alcatel-Lucent9012 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-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 Conductor running AOS-W 8.6.0.13 or later versions do not retrieve any VLAN IP information in a cluster setup.	AOS-W 8.6.0.13
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-W 8.8.0.1 or later versions.	AOS-W 8.6.0.15
AOS-232208	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-W8.10.0.0 or later versions.	AOS-W 8.10.0.0

Table 7: *Known Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
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 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
AOS-232733	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-AP535access 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-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-233988 AOS-242222	Wired clients are unable to ping each other on the same VLAN when the ACL is set to **user any any permit** policy. This issue occurs because SIP is used as the user for both forward and reverse session creation during session ACL lookup. This issue is observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
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

Table 7: *Known Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
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-236380	Some OAW-AP535 access points running AOS-W 8.7.1.7 or later versions crashed repeatedly. The log files list the reason for the issue as: R**eboot caused by kernel panic: Fatal exception. AP rebooted caused by warm reset**.	AOS-W 8.7.1.7
AOS-236471	Alcatel-Lucent OAW-4740 controller running AOS-W 8.10.0.1 or later versions does 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 controllers record informational logs, even though the system log level is configured as warning. This issue is observed in 9240 controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-237348	Some controllers 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	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-238727	Users are unable to reset the IPsec MTU value the **no crypto ipsec mtu** command. This issue is observed on Mobility Conductor 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
AOS-239382	Some 7240XM 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-239521	Users are unable to add a tunnel to a tunnel group and an error message was 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 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 8.10.0.9*

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 controllers 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-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 8.5.0.0
AOS-240240 AOS-243291 AOS-245463	The output of the **show ap radio-database** command might not display the correct information in Mobility Conductor/managed device topologies. This issue is observed in Mobility Conductors and managed devices running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-241212 AOS-241537	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-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-4650 Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242429	Some controllers fail after a system upgrade from AOS-W 6.5.x to 8.7.1.4 version. Upon reboot, this error is displayed: **Failed to set port as trusted, err=Module Process handling LAG and LACP functionality is busy. Please try later.** This issue is observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-242532	Some AP-535 access points are not coming up on 7210 controller post power outage. This issue occurs when a USB converter and console cable are used, which interrupts the boot up process and results in AP not showing up on controller. The issue is observed in controllers 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-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

Table 7: *Known Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-244373	Some OAW-AP377 access points provisioned as Mesh point with **op-mode open-system** will intermittently lost connection to controller within an hour, followed by a reestablishment of the connection. This issue is observed in OAW-AP377 running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244575	In some switches, editing the captive portal profile in guest-logon without Policy Enforcement Firewall license is allowed, and the configuration is accepted. As a result, an error message is displayed stating: **Error: System role 'guest-logon' is not editable, without Next Generation Policy Enforcement Firewall.** This error message appears after running the **show configuration failure** command. This issue is observed in OAW-4750XMswitches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.0
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-245034	Some controllers running AOS-W 8.10.0.5 or later versions, unexpectedly crash due to a memory leak issue of the **FPAPPS** process.	AOS-W 8.10.0.5
AOS-245153	Some users might be unable to fetch Airgroup service configurations to Mobility Conductors. This issue is observed in Mobility Conductors 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 **Dashboard > Traffic Analysis > Applications** tab. This feature does work if 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-245499	switches return the wrong number of associated clients per SSID. This issue is related to an error in the SNMP table population process. This issue is observed in switches running AOS-W 8.6.0.21 or later versions	AOS-W 8.6.0.21
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

Table 7: *Known Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
AOS-246198	Some users might receive the error, **There is no IP address configured for Vlan 220** when attempting to ping from a source VLAN. The issue occurs even if the L3 interface is configured correctly and the VLAN that is up and running. This issue is observed in managed devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246231	In some OAW-4750XMswitches, the WLAN configuration is lost after upgrading to AOS-W8.10.0.7. As a result, AP-Group, VAP and SSID Profiles are missing due to an incorrect number of **ifmap cppm** servers created across the node hierarchy after the upgrade.	AOS-W 8.10.0.7
AOS-246604 AOS-246606 AOS-246674 AOS-246698 AOS-246706	NVDA reader does not announce certain parameters, toggle buttons, and pop-up windows correctly when the user navigates through 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-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-246884	Some Managed Devices fail to download CA certificates when the name reaches a string length of 31 characters. This issue is observed in Managed Devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-246937	The mDNS module of switches crashes multiple times, causing an abnormal number of restarts. This issue is observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
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-248537	Devices experience low throughput when connected to WPA3 Enterprise (GCM) (256 bit) Tunnel Mode SSIDs, in both CNSA and non-CNSA mode. This issue is observed in OAW-41xx Series switches and VMC switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0

Table 7: *Known Issues in AOS-W 8.10.0.9*

New Bug ID	Description	Reported Version
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

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.