AOS-W 8.11.2.1 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

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 8.11.2.1

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

New Features and Enhancements

This topic describes the features and enhancements introduced in this release.

The denylist-sco-attack Parameter is Disabled by Default

The **denylist-sco-attack** parameter under the **aaa-profile** command is set to **Disabled** by default when upgrading to AOS-W 8.11.2.1 or later versions.

show ap tech-support ap-name Command Enhancement

Starting with AOS-W 8.11.2.1, the output of the **show ap arm split-scan-history <ap-name>** command is added in the **show ap tech-support ap-name <ap-name>** command. This reduces the turn around time during data collection, improving customer service experience.

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

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

Behavioral Changes

This release does not introduce any changes in AOS-W behaviors, resources, or support that would require you to modify your existing system configurations after updating to 8.11.2.1.

Chapter 4
Supported Platforms in AOS-W 8.11.2.1

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-AP300 Series	OAW-AP304, OAW-AP305

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H, OAW-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP318
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-AP500 Series	OAW-AP504, OAW-AP505
OAW-AP503 Series	OAW-AP503
OAW-AP500H Series	OAW-AP503H, OAW-AP503HR, OAW-AP505H, OAW-AP505HR
OAW-AP510 Series	OAW-AP514, OAW-AP515, OAW-AP518
OAW-AP518 Series	OAW-AP518
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577
OAW-AP580 Series	OAW-AP584, OAW-AP585, OAW-AP585EX, OAW-AP587, OAW-AP587EX
OAW-AP610 Series	OAW-AP615
OAW-AP630 Series	OAW-AP635, AP-634
OAW-AP650 Series	OAW-AP655, AP-654

Chapter 5
Regulatory Updates in AOS-W 8.11.2.1

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_88505

Chapter 6
Resolved Issues in AOS-W 8.11.2.1

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
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-236721	The **Configuration > Roles & Policies > Roles** page of the WebUI did not display ACLs configured for the role. However, the CLI displayed the list of ACLs. The fix ensures the WebUI displays the expected information. This issue was observed in Mobility Conductors running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-236894	The OmniVista 3600 Air Manager usage graph did not update. The BSSID Tunnel Status on the controllers was disabled. Enabling the BSSID Tunnel Statistics through AOS-W commands resulted in an inconsistency, where the standby controller'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
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-237883 AOS-236808	Some access points dropped the ESP packet causing RADIUS timeout for tunnel mode SSID. This issue occurred when setting a new key or the rekey failed with NSS FW. The fix ensures that all related entries are cleared on NSS FW side, including SA entries, IPv4 IPsec rule, and IPsec tunnel device. This issue was observed in OAW-AP535, OAW-AP555, OAW-AP585, OAW-AP635, and OAW-AP655 access points running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-238604	The AP regulatory domain profile displayed different information in the WebUI and CLI. The fix ensures the WebUI and CLI display the same information. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-238729	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-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-239378	Some cluster nodes missed the cluster heartbeat from a different node. This caused both nodes to disconnect and isolate in a subcluster, creating an expected cluster split. The fix ensures that heartbeat misses do not derive in a cluster split. This issue was observed in managed devices running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-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-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-241158	The running configuration did not match the previous configuration when active standalone switch failed over to standby switch. The issue occurred in configurations which need license features, and these features were impacted. The fix ensures the previous configuration is retained as expected. This issue was observed in controllers running AOS-W 8.6.0.0 or later versions which supports standalone setup.	AOS-W 8.6.0.0
AOS-241464 AOS-242568	Some OAW-AP535, OAW-AP555, OAW-AP585, OAW-AP635, and AP-655 access points crashed and rebooted unexpectedly. The log files listed the event as **kernel panic: Fatal exception, PC is at nss_ipsecmgr_sa_add_sync+0x4c/0x400 [qca_nss_ipsecmgr]**. The fix ensures the APs work as expected. The issue was observed in APs running AOS-W 8.10.0.4 or later versions in a cluster setup.	AOS-W 8.10.0.4
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

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-241709	In some controllers, the authentication process crashed for VIA clients, after the Downloable User Role configuration was changed in ClearPass Policy Manager. As a result, the VPN connection was disrupted. The fix ensures the VPN works as expected in this scenario. This issue was observed in controllers running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-242126	Managed devices were unable to download images on port 8089 for FIPS. 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-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
AOS-242852	In some switches running AOS-W 8.6.0.0 or later versions, **tunneled_user** creation failed upon a bridge miss. This fix ensures **tunneled_user** is created, even if a bridge miss happens.	AOS-W 8.6.0.0
AOS-243497 AOS-245908 AOS-246725	Some access points crashed and rebooted unexpectedly. An index mismatch of the **cv_descriptor** between the firmware and ucode resulted in the error: **Take care of the TARGET ASSERT first**. This issue caused the loss of connectivity in the area of the affected AP. The fix ensures APs do not crash and work as expected. This issue was seen in APs running AOS-W 8.11.1.0 or later versions.	AOS-W 8.11.1.0
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 Branch 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-244373	Some OAW-AP377 access points provisioned as a mesh point with **opmode open-system** intermittently lost connectivity to the controller 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-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

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
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 a 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
AOS-244949 AOS-246630	Some APs crashed and rebooted due to 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 and 8.11.1 or later versions.	AOS-W 8.10.0.6
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 controllers work as expected.	AOS-W 8.10.0.5
AOS-245123 AOS-245396 AOS-245831	In the WebUI, under **Managed Network > Configuration > Roles & Policies > Roles > role-name**, the **Show Advanced View** option did not load any information. The information is expected to load after selecting a role from the list. The fix ensures that the advanced role policies is loaded. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245145 AOS-236547	In the WebUI, under **Configuration > Roles & Policies > Role > role-name > 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-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-AP303H and OAW-AP503H Series access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-245409	Some users were unable to pass traffic to the captive portal after rebootstrap. This issue occurred when APs could not source NAT 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-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

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
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 a 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-245874 AOS-246405	Some OAW-AP503 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
AOS-245931	In the **Configuration > System > Logging** page of the WebUI, the **Duplicate combination of IP address and Category** error was displayed when adding an **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 controllers 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-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 AOS-248886	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

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
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-246103 AOS-247433 AOS-240688	Some OAW-AP635 and OAW-AP535 access points rebooted randomly with **reboot reason - kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_send.c:11778 first**. This occurred due to issues with M3 controllers recovery, to which the APs are connected to. The fix ensures the access points perform as expected. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-246124	In some OAW-4750XM switch, a Kernel crash was observed due to a 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 does not fail. This issue was observed in controllers 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-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-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	Some switches did not detect 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-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

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-246836	OmniAccess Mobility Controllers running AOS-W 8.10.0.7 or later versions did not accept 4240 Gateways being added as managed devices. When attempted, the switches displayed two errors: ■ Error 1: **Device addition failed. Some effective configuration is not compliant to new device model**. ■ Error 2: **Device addition failed. Configured VLANs count at Managed Network exceeds the max supported vlans-1**. The fix ensures 4240 Gateways can be added to the network topology.	AOS-W 8.10.0.7
AOS-246884	Some managed devices failed to download CA certificates when the name reached a string length of 31 characters. The fix ensures CA certificates download as expected. This issue was 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 controllers crashed multiple times which caused an abnormal number of restarts. The fix ensures the controllers work as expected. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246966	Some 7240 OmniAccess Mobility Controllers crashed and rebooted unexpectedly. The log files listed the reason for the crash as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures the controllers work 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-247206	The OAW-AP535 access points has 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 8.11.2.0 or later versions.	AOS-W 8.11.2.0
AOS-247508	Whenever machine authentication and user authentication were enabled in conjunction, full 802.1X authentication took a long time to finish processing. This issue was related to a false trigger of the **denylist-sco-attack** process. The fix ensures the authentication process works as expected. The issue is observed in devices running AOS-W 8.11.2.0 or later versions.	AOS-W 8.11.2.0
AOS-247611	Some controllers 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 controllers 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) controller when running the **show ap database** command. The issue occurred due to a regulatory domain mismatch between the primary and standby controllers. 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

Table 6: *Resolved Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
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-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 controller to crash. This issue was observed in 9240 switches running AOS-W 8.11.1.1 or later versions.	AOS-W 8.11.1.1
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-248121	The AVS process caused OAW-AP577 access points to crash after recovering from low temperatures since 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-248196	In a two-node cluster using OSPF for AP-MD connectivity, disabling the AP's reachability to one of the controllers designated as S-AAC, resulted in the absence of AMON messages being sent from the AAC to the OmniAccess Mobility Controller. The fix ensures AMON messages are correctly sent to the OmniAccess Mobility Controller. This issue was observed in access points running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-248762	The Web Content Classification process was crashing due to segmentation. The fix ensures the **web_cc** process and its classification functionality work as expected. This issue was observed in controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Chapter 7
Known Issues in AOS-W 8.11.2.1

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

Limitations

Following are the limitations observed in this release.

OAW-AP615, OAW-AP635, and OAW-AP655 Access Points

The OAW-AP615, OAW-AP635, and OAW-AP655 access points have the following limitations:

- All radios for these APs currently do not support spectrum analysis.
- 802.11mc responder and initiator functionality, Hotspot configuration, and Air Slice configuration are not supported on the 6 GHz radio.
- Users can configure only up to 4 VAPs on the 6 GHz radio, instead of 16 VAPs.

Airtime Fairness Mode

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

AP-654 and AP-634 Access Points

For the current release of AOS-W, AP-654 and AP-634 access points do not support 6 GHz band operation. Support for 6 GHz will be enabled in a future software release, and will depend on the local regulatory status reflected in the DRT file.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
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-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 8.11.2.1*

New Bug ID	Description	Reported Version
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-233740	Some switches does not allow the deletion of system IPv6 address using the **no controller-ipv6** command. As a result, an error message is displayed: **Controller-IPv6 cannot be removed. Please configure controller-ipv6 on some other valid vlan or the loopback**. This issue is observed in controllers running AOS-W 8.11.0.0.	AOS-W 8.11.0.0
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-236235 AOS-241383 AOS-243840 AOS-235963 AOS-236237	Multiple APs crash due to a mismatch between **wmm_eap_ac** and **eapol_ac_override** in the configuration. This issue is observed in OAW-AP535 access points running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
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-237348	Some OAW-AP535 access points running AOS-W 8.9.0.3 or later versions crash and reboot unexpectedly. The log files list the reason for the reboot as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first at whal_recv.c:1656 Assertion.**	AOS-W 8.6.0.18
AOS-237373	The RAP-655 access point crashes unexpectedly when the PMTU value is set up to 1200 or 1300 bytes. The log files list the reason for the event as **PC is at skb_copy_and_csum_bits+0x24/0x274**. This issue is observed in RAP-655 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-237931 AOS-242118	A datapath crash is observed on Ubuntu 20_04 servers if OS type is set to RHEL 7.2 or above. This issue is observed in virtual machines running on AOS-W 8.7.1.11 or later versions.	AOS-W 8.7.1.11

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-238157	Some OAW-4750XM switches randomly reboot with **Reboot Cause: Kernel Panic (Intent:cause:register)**. This issue occurs after upgrading to AOS-W 8.10.0.3 due to a memory corruption issue.	AOS-W 8.10.0.3
AOS-238160 AOS-246310	Some access points running AOS-W 8.11.0.0 or later versions crash and reboot unexpectedly. The log files list the reason of the event as **AP Reboot reason: BadPtr: 00000000 PC: anul_probe_req_find_by_mac+0x88/0x1d4 [anul] Warm-reset**.	AOS-W 8.11.0.0
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 Conductors running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-238803 AOS-246511	switches running AOS-W 8.10.0.7 or later versions log continuous error messages such as **|web_cc| Failed GSM publish web_cc_gsm_publish**.	AOS-W 8.10.0.7
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-239165	Some OAW-AP635 access points running AOS-W 8.10.0.2 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic with "sched_algo_qos.c:3794 Assertion (rtxop > 0) failed".**	AOS-W 8.10.0.2
AOS-239321 AOS-240598 AOS-243974	Some OAW-AP635 access points crash and reboot unexpectedly. The log files list the event as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT**. The **crash-info** shows that the AP firmware is asserted at **whal_recv.c:1656**. The issue is observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239324 AOS-238844 AOS-243905	In some OAW-AP535 access points running AOS-W 8.10.0.2 or later versions, users are unable to associate to neighbor APs with deauthentication message **Reason Class 2 frames from non authenticated STA**. This issue occurs in 5 GHz SSIDs.	AOS-W 8.10.0.2
AOS-239382	Some OAW-4750XM Mobility Conductors running AOS-W 8.7.1.9 or later versions configured in a cluster setup crash and reboot unexpectedly. The log files list the reason for the event as **Datapath timeout (SOS Assert)**.	AOS-W 8.7.1.9
AOS-239459 AOS-248389	Mobility Conductors running AOS-W 8.10.0.7 or later versions continuously log multiple unnecessary errors related to the **mon_serv_fwv** process. The logs prefix the errors as **|mon_serv_fwv|mon_serv_gsm_handle_device_config_add**.	AOS-W 8.10.0.7

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-239504 AOS-245543	Some APs are showing multiple messages with **dp_find_ast_id_by_addr 3745 Invalid priority: ff** when **app_priority** is **0xff**. This issue is observed in OAW-AP535 access points running AOS-W 8.6.0.0 or later versions.	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
AOS-239687	Some clients are unable to connect to the 5 GHz radio on access points. This issue occurs due to an error in the AP's Broadcom wireless driver. This issue is observed in APs running AOS-W 8.7.1.9 or later versions	AOS-W 8.7.1.9
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-239836 AOS-239952 AOS-241189	The **Nbapi-Helper** process crashes in some OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions. This prevents users from obtaining the feed from the Analytics and Locations Engine (ALE) servers.	AOS-W 8.10.0.2
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-240026 AOS-236177 AOS-239232 AOS-240068 AOS-240633	Some customers are unable to access switches through the CLI or WebUI. This issue is related to third-party monitoring tools, such as Armis, causing the CLI sessions to remain open for a long time and accumulating memory leaks, affecting the functioning of the controller. This issue is observed in switches running AOS-W 8.6.0.18 or later versions. **Workaround:** Reboot the controller and periodically log out of the CLI session.	AOS-W 8.6.0.18
AOS-240149	Some OAW-AP635 access points running AOS-W 8.10.0.5 reboot and crash unexpectedly. The log files list the event as **Reboot caused by FW crash**. The issue is observed on APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-240240 AOS-243291 AOS-245463	The output of the **show ap radio-database** command might not display the correct information in Mobility Conductors and managed devices 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-240279	Mobility Conductors running AOS-W 8.10.0.4 or later versions might push additional IGMP and OSPF configurations to managed devices. This issue occurs when a VLAN configuration is edited.	AOS-W 8.10.0.4

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-240568 AOS-244716	In some controllers, saving the tunnel configuration takes longer than expected. This issue is observed in standby controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-240601 AOS-241185	In some OAW-AP500 Series access points running AOS-W 8.10.0.2 or later versions, the scheduler algorithm causes a delay. This may introduce latency in the MU schedule for multiple clients.	AOS-W 8.10.0.2
AOS-240953	Some OAW-AP635 access points fail to send data frames when configured in tunnel mode using opmode wpa3-sae-aes encryption. Clients are also unable to obtain IP addresses. This issue is caused by PMF drop when the **Prohibit IP Spoofing** policy is enabled. This issue is observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240954	Some OAW-AP555 access points running AOS-W 8.10.0.5 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**.	AOS-W 8.10.0.5
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-241228	In some standby switches, the **disable allowlist-sync** command can be executed, causing the switches to enter a **CONFIG_ FAILURE** state. This command is intended for primary switches only. This issue is observed in switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-241338 AOS-245793	The **show openflow ports** command does not show GE port information during soak testing. This issue is observed in Mobility Conductors running AOS-W 8.11.1.0 or later versions.	AOS-W 8.11.1.0
AOS-241498 AOS-245883 AOS-245217	A corrupt bridge ACL issue is observed in APs running AOS-W 8.10.0.5 or later versions, where some user roles are either missing or contain a duplicate of the **logon** role. This prevents the AP from passing user traffic.	AOS-W 8.10.0.5
AOS-241560	Accessing controllers 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-241833	Remote APs operating in a dual-stack environment with an IPv4 IPSEC might experience heartbeat loses after IPSEC re-key when IPv6 is inadvertently used. The issue is seen on remote OAW-AP505H access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-241841	Some OmniAccess Mobility Controllers are unable to ping their default gateway and display neighbor entries when using IPv6. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241863	The ACL is incomplete in the SAPD and datapath modules, causing connectivity issues. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241898	The **Configuration > WLANs > VLANs** section of the WebUI does not reflect changes made to VLANs. This issue is observed in controller running AOS-W 8.10.0.5 release or later versions.	AOS-W 8.10.0.5
AOS-241957	The WebUI requires specifying a category when adding a logging server in **Configuration > System > Logging**. This should not be mandatory for logging server configuration. This issue is observed in Mobility Conductors 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 causes the error: **/mm/mynode" COMMAND: -- command execution failed**. This issue is observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242119	In some controllers running AOS-W 8.10.0.4 or later versions, policy names are not displayed in alphabetical order in the controller WebUI.	AOS-W 8.10.0.4
AOS-242429 AOS-248682	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 OAW-AP535 access points are not available on OAW-4550 switches 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 controller. The issue is observed in switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-243033	In some OAW-4650 controllers in a cluster setup, APs fail to form a standby tunnel after a reboot. This issue occurs due to an interrupt in the **dot1x** process.	AOS-W 8.10.0.5
AOS-243162	Controllers restricted to Egypt might not display the country code in the output of the **show version** command. This issue is observed in controllers running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
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

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-243749	Some standalone controllers are unable to make changes through the WebUI when using standard admin credentials. This issue is observed in controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244091 AOS-244610 AOS-246131 AOS-246450	Some OAW-AP534 access points crash and reboot unexpectedly. The log files list 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)**. This issue is observed in access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244165	OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions include irrelevant messages stating **TOKEN WAS ABSENT** as error logs. These messages are intended to appear as debug logs and not error logs.	AOS-W 8.10.0.6
AOS-244210	Users are unable to configure a negative value for the transmit power setting in the **Overview > Profiles > IoT Profile > BLE Transmit Power** page of the WebUI. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-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-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-4750XM switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.0
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-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-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

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-245191	Some Mobility Conductors are unable to establish an SSH connection to the managed devices due to login sessions not timing out. This issue is observed in managed devices running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-245260	Multiple OAW-AP325 access points are not displaying radars in DFS channels when switched from 40 MHz to 20 MHz. This issue is observed in OAW-AP325 access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-245264	VAPs defined by the customer take a long time to show as **valid**. This issue is observed in APs running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-245266 AOS-244968 AOS-248279	Some access points automatically disable their 6 GHz radio bands. This issue is observed in OAW-AP635 and OAW-AP655 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-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-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-245976	In some controllers, end users can get locked out of configuration mode if there is only one root user present in the Mobility Conductor or standalone node that does not have the username as **admin**. Users are allowed to change the role of this sole root user to read-only, standard, or any other role. After this, users cannot make any configurations since there are no root users available in the node. This issue is observed in controllers running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-246097	Some OAW-AP535 access points randomly disable the ANI feature. The issue is due to an unintended trigger of the ANI periodic check, which disables the feature. This issue is observed in OAW-AP535 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246184	Some access points crash and reboot unexpectedly. The log files list 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 is related to the AP image version found in affected versions of AOS-W. This issue is observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-246583	Some OAW-4750XM OmniAccess Mobility Controllers may experience unexpected crashes as a result of a failure in the **tnld_node_mgr** process. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246839 AOS-247983	The usage of ECDSA certificates in a web-server profile may cause the unavailability of the WebUI. This issue is 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
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. **Workaround:** Reload the managed device or restart the **profmgr** process to fix the issue.	AOS-W 8.6.0.21
AOS-247070	Some controllers crash and reboot with the reason: **Datapath timeout (Intent:cause: 86:56)**. The crash is related to sessions being deleted due to a QAT response timeout. This issue is observed in OAW-4104 switches running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-247326	The output of the **show running configuration** command might display VLAN IDs and descriptions on separated lines instead of one. This issue is observed in managed devices running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-247335 AOS-247967 AOS-248500	Some 9240 controllers reboot with reason **Reboot Cause: Datapath timeout**. This issue occurs because **dpi packets** are sent to CPU with ID **0** in some flow. This issue is observed in controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-247551	The output of the **show aaa auth-survivability-cache** command displays station names in uppercase. This issue is observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-247602 AOS-247934 AOS-244334	Some access points incorrectly display their power supply type as DC despite being connected to a PoE switch port and without any DC supply. This issue is observed in OAW-AP655 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247721	Mobility Conductor in a standby setup fail over and crashed 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-248371	The OAW-4750XM controller fails to copy out **crash.tar** when the file size is larger than 2 GB. This issue is observed in OAW-4750XM controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248473	The OAW-AP535 access points mismatch **ANI Dense Level (Max)** statistics. This issue occurs due to an Rx sensitivity limitation. This issue is observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7

Table 7: *Known Issues in AOS-W 8.11.2.1*

New Bug ID	Description	Reported Version
AOS-248891	Some OAW-AP515 access points unexpectedly crash and reboot. The log files list the reason for the event as **BadPtr:000000d8 PC:wlc_ampdu_dotxstatus_regmpdu+0x700/0xba0**. This issue is 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 **System > General > Clock** page of the WebUI, the **Timezone** and **Date and Time** do not display the correct configuration. This issue is observed in controllers 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 reboot. The log files list the reason for the reboot as **Reboot caused by WLAN firmware TARGET ASSERT at twt_ap.c:847**.	AOS-W 8.10.0.6

Chapter 8
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 33 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 33 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 33 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	8.11.x	360 MB
8.5.x	8.11.x	360 MB
8.6.x	8.11.x	570 MB
8.7.x	8.11.x	570 MB
8.8.x	8.11.x	450 MB
8.9.x	8.11.x	450 MB
8.10.x	8.11.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 30.

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 33 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 33 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 33.

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.