AOS-W 8.10.0.7 Release Notes

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 to AOS-W 8.10.0.7 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 8.10.0.7 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 8.10.0.7

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

Unnecessary Logs are Reduced

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

OAW-AP535 PoE Support

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

Chapter 4
Supported Platforms

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 3: *Supported Mobility Conductor Platforms*

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

OmniAccess Mobility Controller Platforms

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

Table 4: *Supported OmniAccess Mobility Controller Platforms*

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

AP Platforms

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

Table 5: *Supported AP Platforms*

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

Table 5: *Supported AP Platforms*

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

Table 5: *Supported AP Platforms*

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

Chapter 5
End-of-Support

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

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

- OAW-AP200 Series
- OAW-AP203H Series
- OAW-AP203R Series
- OAW-AP205H Series
- OAW-AP207 Series
- OAW-AP210 Series
- OAW-AP 220 Series
- OAW-AP228 Series
- OAW-AP270 Series
- OAW-AP320 Series
- OAW-AP330 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_86916

Chapter 7
Resolved Issues

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-239115	An AP crashed and rebooted unexpectedly when IPM was enabled. The log file listed the reason for reboot as: **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the AP functions as expected when IPM is enabled. This issue was observed in APs running AOS-W 8.9.0.0 or later versions.	AOS-W 8.10.0.5
AOS-240920 AOS-242753	The **fpapps** process crashed randomly when querying an ifMIB OID with unknown index value using SNMP. The fix ensures **fpapps** does not crash when an invalid index value is used. This issue was observed on Mobility Conductors running AOS-W 8.9.0.3 or later versions.	AOS-W 8.9.0.3
AOS-240953	Some OAW-AP635 access points failed to send data frames when configured in tunnel mode using opmode wpa3-sae-aes encryption. The clients were also unable to get an IP address. This issue was caused by PMF drop when the **Prohibit IP Spoofing** policy was enabled. The fix ensures APs on opmode wpa3-sae-aes or tunnel mode work as expected. This issue was observed on APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240958	Multiple sapd process error messages: **Error opening/proc/sys/net/aruba_asap/aruba001/bw_stats : No such file or directory** were observed on OAW-AP503H remote access points with backup SSID configured. The fix ensures that the OAW-AP503H remote access points work as expected. This issue was observed in OAW-AP503H remote access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-240995	While downloading the VIA subnets, the endian conversion did not happen as expected. This resulted in the VIA subnet routes getting installed in reverse order. The fix ensures the feature works as expected. This issue was observed in OmniAccess Mobility Controller running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-241088	In the WebUI **Dashboard > Infrastructure > Access Points**, the status of the APs appeared to be in an incorrect state when checked from the Mobility Controller. The fix ensures the status is accurate in the WebUI. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241120	Personal registered device was visible to all users even when no username was specified in the CPPM configured policy. The fix ensures the personal registered device is visible to only the owner and the specified intended users. This issue was observed in managed devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-241218	Users experienced multiple mDNS process crashes in systems running AOS-W 8.10.0.5 or later versions. The issue was related to memory corruption when processing certain incoming packets in the mDNS process. The fix ensures that there is no memory corruption and the process executes as expected.	AOS-W 8.10.0.5
AOS-241313	Zebra TC21 barcode scanners were unable to maintain a connection and send traffic when connected to OAW-AP505 devices running AOS-W 8.10.0.5 or later versions. The fix ensures TC21 barcode scanners can successfully connect to APs and pass traffic as intended.	AOS-W 8.10.0.5
AOS-241434	The **show running-config** command could not be executed and displayed an error **Module DHCP Daemon is busy. Please try later.** The fix ensures the **show running-config command** works as expected. This issue was observed on OmniAccess Mobility Controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-241454	APs that were part of an AP group were incorrectly set in the D flag. The fix ensures that 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-240279	Mobility Conductors running AOS-W 8.10.0.4 or later versions pushed additional IGMP and OSPF configurations to managed devices. This issue occurred when a VLAN configuration was edited. The fix ensures that additional configurations are not sent and Mobility Conductors work as expected.	AOS-W 8.10.0.4
AOS-240954	Some OAW-AP555 access points running AOS-W 8.10.0.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.10.0.5
AOS-242606	The **show iot-manager ble-services beacon-info** command showed incorrect and sometimes repeating information. The fix ensures this command displays accurate information as intended. This issue was seen in systems running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-240185	Clients were unable to obtain user roles from ClearPass Policy Manager and fell into their initial role. This issue occurred due to radius accounting. This issue was observed in managed devices running AOS-W 8.7.1.10 or later versions. The fix ensures that clients can obtain their accurate user roles from CPPM.	AOS-W 8.7.1.10
AOS-240931	Ascom i62/i63 VoIP phones experienced connectivity issues in the form of low-quality audio output when connected to OAW-AP515 access points running AOS-W 8.10.0.4 or later versions. The issue was related to compatibility with a Broadcom patch. The fix ensures Ascom devices output the expected quality audio.	AOS-W 8.10.0.4

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-241957	The WebUI required specifying a category when adding a logging server in **Configuration > System > Logging**. This should not be mandatory for logging server configuration. Thus, the fix excludes this requirement from the WebUI and allows users to add a logging server without a category. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-237883	OAW-AP535, OAW-AP555, OAW-AP585, OAW-AP635, and OAW-AP655 access points drop the ESP packet causing RADIUS timeout for tunnel mode SSID. This happens when setting a new key or rekey fails with NSS FW. This issue was observed in APs running AOS-W 8.8.0.0 or later versions. The fix ensures that all related entry is cleared on NSS FW side, including SA entry, IPv4 IPsec rule, and IPsec tunnel device.	AOS-W 8.8.0.0
AOS-239183	In some switchesrunning AOS-W 8.6.0.10 or later versions, the WebUI was showing daylight saving when configured for certain time zones, after daylight saving was over. This fix ensures the correct time is displayed in the WebUI.	AOS-W 8.6.0.10
AOS-239498	Some OAW-AP515 access points running AOS-W 8.6.0.19 or later versions, crashed and rebooted unexpectedly. The log files listed the reason for the event as **AP Reboot reason: BadPtr:0000000f PC:wlc_get_txh_info+0x118/0x210 [wl_v6] Warm-reset.** This fix ensures the APs work as expected.	AOS-W 8.6.0.19
AOS-240211	After a Radar detection in a particular channel, the ARM feature caused access points to return to the original channel, ignoring the 30-minute backoff period that is required after a radar detection which led beacons not being transmitted. The fix ensures the APs works as expected and does not return to Radar affected channel until 30 min. This issue is observed in OAW-AP535 running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-241497	Some OAW-AP275 access points running AOS-W 8.10.0.5 or later versions interconnected in a mesh topology crashed and rebooted unexpectedly. The log files recorded the event as, **Process /aruba/bin/sapd has too many open files**. The issue occurred when the AP sockets remained in open state even if they were already allocated. The fix ensures the APs work as intended.	AOS-W 8.10.0.5
AOS-241669	Guest SSID sessions did not disconnect even after the session timeout. The fix ensures no connections are allowed to users when their session times out. This issue was observed in some controllers running AOS-W 8.6.0.9 or later versions connected through a split-tunnel.	AOS-W 8.6.0.9
AOS-242066	Some OAW-AP535 access points running AOS-W 8.6.0.19 or later versions crashed and rebooted unexpectedly. The log files registered the event as, **core.lldpd.API_06F_06.AP-535.85031**. The fix ensures the APs work as expected.	AOS-W 8.6.0.19

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-242238	Some users connected to open SSIDs were able to access video services even after their session timed out. The issue occurred due to session expiration times not supported in datapath. The fix ensures no video services are allowed to users when their sessions time out. This issue was observed in APs in split tunnel mode running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-236821 AOS-241769	Some OAW-AP535 access points running AOS-W 8.9.0.3 or later versions crashed and rebooted unexpectedly. The log files recorded the event as **dog_hb.c:210 DOG_HB detects starvation of task "WLAN RT1", triage with its owner (d.dump 0x4b55cb20)**. The fix ensures the APs work as intended.	AOS-W 8.9.0.3
AOS-217194	The WebUI displayed the error message, **access-group is not configured** while configuring BCMC optimization. The fix ensures the WebUI behaves as expected. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-238656 AOS-239832 AOS-240893 AOS-242252	Some APs crashed and rebooted unexpectedly with the reason for the event as: **Kernel panic - not syncing: Take care of the TARGET ASSERT first**. The crash-info showed that AP firmware was asserted at ratectrl.c:999. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points on AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-241364	The output of the **show audit-trail | include admin** command displayed, **COMMAND: – command execution failed** repeatedly. The fix ensures the output of the command does not display the error for “show switches” anymore.This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-241464 AOS-242568	Some OAW-AP535, OAW-AP555, OAW-AP585, OAW-AP635, and OAW-AP655 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-239321 AOS-240598	Some OAW-AP635 access points crashed and rebooted unexpectedly. The log files listed the event as, **Reboot caused by kernel panic: Take care of the TARGET ASSERT**. The crash-info showed that the AP firmware was asserted at whal_recv.c:1656. The fix ensures that the APs work as expected. The issue was observed on APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239328 AOS-239828	Some OAW-AP535 access points crashed and rebooted unexpectedly. The log files listed the event as, **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The crash-info showed that the AP firmware was asserted at whal_recv.c:1656. The fix ensures that the APs work as expected. The issue was observed on APs running AOS-W 8.9.0.3 or later versions.	AOS-W 8.9.0.3

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-240433	The **ISAKMPD process** crashed with VIA clients terminated using DHCP servers for internal IP allocation. The fix ensures that the ISAKMPD process work as expected. The issue was observed in standalone OAW-4030 controllers running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-242594	The **profmgr** process crashed on Mobility Conductors running AOS-W 8.10.0.6 or later versions. The issue occurred when provisioning **BLE** service profiles in the Mobility Conductor. The fix ensures the profmgr process works as expected.	AOS-W 8.10.0.6
AOS-233941 AOS-239833	Some OAW-AP535, OAW-AP555, OAW-AP635 and OAW-AP655 access points were unable to send beacon packets using the Airgroup feature when multicast aggregation was enabled on the APs. The fix ensures APs can select one AP to forward MDNS packets to multiple VLANs. The issue was observed on APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
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-239452	Some OmniAccess Mobility Controllers reported the wrong AP BSSID when sending the **wlsxNAuthServerAcctTimedOut** SNMP trap. The fix ensures that OmniAccess Mobility Controllers report the correct BSSID when sending a server request timed out event. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-240149	Some OAW-AP635 access points running AOS-W 8.10.0.5 rebooted and crashed unexpectedly. The log files listed the event as, **Reboot caused by FW crash**. The fix ensures the APs work as expected. The issue was observed on APs running AOS-W 8.10.0.5 versions.	AOS-W 8.10.0.5
AOS-239836	**Nbapi-Helper** process crashed in some OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions. This prevented users from obtaining the feeds from the Analytics and Locations Engine (ALE) servers. The fix ensures **Nbapi-Helper** works as expected.	AOS-W 8.10.0.2
AOS-240014	In some switches running AOS-W 8.7.1.4 or later versions, an invalid AP console password was displayed in the AP System profile. This issue was caused by an incorrect password string length. This fix ensures only valid passwords can be set.	AOS-W 8.7.1.4
AOS-240646	The output of the **show ap ble_ibeacon_info** command did not display the name of the AP. This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions. This The fix ensures the AP name is displayed.	AOS-W 8.10.0.2

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-240858	In some OAW-AP303H Series remote access points, cellular IP was not obtained, since it could not create an IPSEC tunnel with the controller. This made the RAP not to come up. This issue was observed in devices running AOS-W 8.10.0.5 or later versions. This fix ensures the OAW-RAP3 Series comes up as expected in this environment.	AOS-W 8.10.0.5
AOS-241312	Some OAW-AP387 access points running AOS-W 8.10.0.5 or later versions were dumping the SCP server with test SCP files. This caused the Dump server to become accumulated with a large number of files, making it difficult to monitor. This fix ensures test files are sent as expected.	AOS-W 8.10.0.5
AOS-241754	Some OAW-AP303H access points running AOS-W 8.10.0.5 or later versions lost heartbeats, where IPv6 was set in /tmp/lms. This caused the AP to crash. The fix ensures the AP performs as expected in this environment.	AOS-W 8.10.0.5
AOS-242651	In some APs running AOS-W 8.10.0.6 or later versions, an issue was observed where all ZigBee ZED were off the APs client-table when pairing more than 12 ZEDs. The fix ensures the right number of ZED devices can be paired without issues.	AOS-W 8.10.0.6
AOS-242119	In some switches running AOS-W 8.10.0.4 or later versions, policy names were not displaying in alphabetical order in the switch WebUI. The fix ensures the information is displayed in alphabetical order.	AOS-W 8.10.0.4
AOS-242468	In some switches running AOS-W 8.10.0.4 or later versions, the outputs of the show configuration effective and show configuration committed commands were blank because the parser was in multi-line mode after execution show configuration datastore. The fix ensures the output values are correctly populated.	AOS-W 8.10.0.4
AOS-242852	In some switches running AOS-W 8.10.0.4 or later versions, tunneled_user creation failed upon a bridge miss. This fix ensures tunneled_user is created, even if bridge miss happens.	AOS-W 8.10.0.4
AOS-219164	YouTube sessions were not properly classified, hence the deny policy was not working despite configuring an ACL. The fix ensures the ACL configuration works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-227981	A few OAW-4010, OAW-4024, OAW-4450 and OAW-4850 controllers running AOS-W 8.7.1.6 or later versions incorrectly route the incoming external subnet traffic on management port to data ports. The fix ensures the controllers work as expected.	AOS-W 8.7.1.6

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-231206	The **wpa3_sae process** crashed or was stuck in **PROCESS_NOT_RESPONDING_CRITICAL** state. This issue occurred due to timer corruption. However, this issue did not affect the connectivity of already connected clients. The fix ensures the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.017 or later versions.	AOS-W 8.6.0.17
AOS-232493	The entries of deny listed clients were not synchronized between the managed devices. The fix ensures the entries are synchronized. This issue was observed in managed devices running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-241550	Multiple OAW-AP535 access points crashed unexpectedly. The log files listed the reason for the event as: **Kernel panic - not syncing: Take care of the TARGET ASSERT at ru_allocator.c:3166 Assertion (((rt_tbl))->info[((rix))].phy == WHAL_MOD_IEEE80211_T_HE_20**. The fix ensures that the APs work as expected. This issue was observed on OAW-AP535 running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-240561	Some APs unexpectedly showed an error: **MDIO Error: MDIO got failure status on phy 30**. A regulation of the clock frequency solved the issue. The fix ensures the APs work as expected. This issue was observed in OAW-AP505H and OAW-AP503H running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
AOS-239291	OmniAccess Mobility Controllers unexpectedly crashed and rebooted. The log files listed the reason for the event as: **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures the controller works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-242013	Some VIA clients were not able to establish tunnels with controllers as the data path tunnel table reached maximum capacity. The fix ensures that the tunnel entries are created and deleted properly in data path tunnel table. This issue was observed on OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241863	The ACL was incomplete in the SAPD and data path modules, and it caused connectivity issues. The fix ensures that the process works 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-236164	The **Dashboard** > **Infrastructure** page of the Mobility ConductorWebUI displayed an incorrect number of APs, as such duplicate APs were observed on the Mobility Conductor WebUI. The same issue was observed in the MON_SERV CLI. The fix ensures that the correct number of As is displayed in the WebUI and the MON_SERV CLI. This issue was observed on Mobility Conductors running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-236503	The Cisco Firepower IPS dropped traffic between the dynamic IAP-VPN tunnels because of the detection of nonzero reserved bits in GRE header. The fix ensures that the traffic is not dropped. This issue was observed in controllers running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-237549	Some controllers were blocking EAPOL frames from passing to a wired RAP interface. The fix ensures the controllers work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-238557	The SNMP MIB trap **wlsxUser6Table** returned incorrect values and did not increase the OID. The fix ensures the correct value is shown in the table. This issue was observed on OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-238815	The modules of some APs appeared as **busy** when collecting system event logs making them unavailable. The fix ensures the system event logs are displayed as expected. This issue was observed on OAW-AP515 running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-239324	In some OAW-AP535 access points running AOS-W 8.10.0.2 or later versions, users were unable to associate to neighboring APs, with deauthentication message **Reason Class 2 frames from non authenticated STA**. This issue was occurred in the 5GHz SSIDs. The fix ensures the APs perform as expected.	AOS-W 8.10.0.2
AOS-240601	In some OAW-AP500 Series access points running AOS-W 8.10.0.2 or later versions, the Scheduler Algorithm caused a delay, which introduced latency in the MU schedule for multiple clients. This fix ensures the algorithm works as expected.	AOS-W 8.10.0.2
AOS-239238	The AP-provisioning process failed for some of the APs, preventing them from being configured properly. The fix ensures the process work as expected. This issue was observed in APs running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1
AOS-235420	The numbers shown in **Rx Good Frames** and **Rx Frames Received** in the radio stats were the same in OAW-AP555. The fix ensures that the two stats work as expected. This issue was observed inOAW-AP555 running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1
AOS-240425	The HTTPS connection was interrupted and the ICMP communication was blocked for some VIA clients. This issue occurred when: ■ The default size of 1452 bytes was used for MTU ■ The DF bit was set for IP packets The fix ensures the connection works as expected. This issue was observed in controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-238964	In some controllers running AOS-W 8.10.0.2 or later versions, the wireless client count on the GUI was not consistent with the client count obtained through the CLI. This prevented proper monitoring of client count. This fix ensures the client count is displayed correctly.	AOS-W 8.10.0.2
AOS-243222	The **Auth** module crashed on managed devices. The issue occurred due to insufficient memory allocated to the devices in a 6 node cluster and AP/client scale. The fix ensures the **Auth** module works as expected. This issue was observed in 9240 Series devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-239687 AOS-240767	Some clients were unable to connect to the 5 GHz radio on OAW-AP515 access points. This issue occurred due to an error in the AP's Broadcom wireless driver. This issue was observed in APs running AOS-W 8.7.1.9 or later versions. The fix includes an update to the APs' Broadcom wireless driver, which ensures that APs work as expected.	AOS-W 8.7.1.9
AOS-242985 AOS-242254	Some OAW-AP635 access points running AOS-W 8.10.0.5 or later versions crashed and rebooted unexpectedly. The issue was related to incomplete TLV, which resulted in an invalid scheduler ID and queue ID and caused the firmware crash. The log files listed the reason for the error as: **kernel panic with ar_wal_tx_sch_status.c:645 Assertion (PPDU_QUEUE_ID(tx_ctxt) != TX_INVALID_QUEUE || PPDU_SCH_ID(tx_ctxt)**. The fix ensures the APs work as expected.	AOS-W 8.10.0.5
AOS-239643 AOS-237332	The **show running-config** command displayed zero IPv6 interfaces for layer 3 VLANS instead of 128. An increase in the amapi buffer size ensures the command displays the expected number of IPv6 interfaces, which is 128 for L3 VLANS. The issue was observed in stand-alone controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-243036	Some managed devices crashed due to a limited memory of cluster_mgr when adding nodes in a cluster environment. The fix ensures the process works as expected. This issue was observed in managed devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-243442	Some managed devices unexpectedly displayed an error message for WLAN users. The log files listed the reason as: **INVAL_HDR_HDR_TYPE: arp [25316] Found incorrect hardware type in ARP header: 256**. A correction of the endian sequence solved the issue. This issue was observed in x86 based platforms (OAW-41xx Series Controllers, 9200 Series Controllers, and VMCs) running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.5
AOS-236164	The **Dashboard** > **Infrastructure** page of the Mobility Conductor WebUI displayed an incorrect number of APs. The same issue was observed in the **MON_SERV** CLI. The fix ensures that the correct number of APs is displayed in the WebUI and the MON_SERV CLI. This issue was observed in Mobility Conductors running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-237549	Some controllers were blocking EAPOL frames from passing to a wired RAP interface. The fix ensures the controllers work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-234207	Some mobility devices running AOS-W 8.10.0.0 or later versions experienced unexpected TM crashes. The issue was related to internal memory allocation management. The fix ensures no unexpected TM crashes occur.	AOS-W 8.10.0.0
AOS-241937	A few user-based tunnelled users failed to come up on managed devices due to certain race condition in the sequence of events during the user bootstrap process. This issue was observed in managed devices running AOS-W 8.10.0.2 or later versions. The fix ensures user-based tunneling works as expected.	AOS-W 8.10.0.2
AOS-242054	Some Mobility Conductors displayed incorrect Share Group values in the CLI when using CPPM features. The values were displayed correctly in the control plane. The fix ensures that the value is displayed correctly in the CLI. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241056	Some clients were unable to connect to the controller after upgrading to AOS-W 8.10.0.5 or later versions. This issue occurred due to the auth_mgr process crashing. The fix ensures the clients can connect to the controller as expected.	AOS-W 8.10.0.5
AOS-241228	In some standby controllers the **disable allowlist-sync** command was executed, causing the controllers to enter a CONFIG_FAILURE state. This command is intended for primary controllers only. This issue was observed in controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-242638	In some controllers running AOS-W 8.9.0.3 or later versions, Security Association attributes (SAs) were not cleared when crypto-map is disabled. This caused IKE/IPSec tunnels to block traffic in Site-to-Site connections. The fix ensures IKE/IPSec SAs are properly cleared and built after disabling and re-enabling crypto-maps.	AOS-W 8.9.0.3
AOS-244284	Some controllers running AOS-W 8.10.0.0 or later versions were dropping incoming encrypted AESCCM data packets from client devices due to the following reason – **Invalid Replay Counter**. The fix ensures that the packets are not dropped even if the Replay Counter is found to be invalid. The controller will keep a count of the number of packets where this error is seen.	AOS-W 8.10.0.0
AOS-241086	Some clients were unable to connect to the controller due to crashes of the auth_mgr process after upgrading from AOS-W 8.6.0.7 to AOS-W 8.10.0.5 or later versions. The fix ensures the clients can connect as expected.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-242054	Some Mobility Conductors displayed incorrect Shared Group values in the CLI when using CPPM features. The fix ensures that the value is displayed correctly in the CLI. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241841	Some OmniAccess Mobility Controllers were unable to ping their default gateway and display neighbor entries when using IPv6. The fix ensures the process works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-243221	Some controllersrunning AOS-W 8.10.0.5 were sending **KNI: Out of memory** error logs to the Syslog server. The error logs were building up and prevented the controllersfrom communicating with the network devices. The fix ensures the error logs are properly handled.	AOS-W 8.10.0.5

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

Limitations

Following are the limitations observed in this release.

IP Default-Gateway Management Address

Alcatel-Lucent recommends to not configure the IP default-gateway management address for OAW-4010, OAW-4024, OAW-4450, and OAW-4850 switches running AOS-W 8.10.0.0.

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 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-221018 AOS-220919	Some users are unable to connect to SSIDs. This issue occurs in 802.11r and MultiZone enabled configurations. This issue is observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
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-219423	Honeywell Handheld 60SL0 devices are unable to connect to 802.1X SSIDs. This issue is observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-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-217948	Some APs experience issues with Wi-Fi uplink 802.1X authentication due to a conflict in certificate validity period verification. This issue is observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-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-209580	The output of the **show ap database** command does not display the **o** or **i** flags, which indicate whether an AP is an outdoor AP or an indoor AP. This issue occurs when the AP installation type is not set to default. This issue is observed in Mobility Conductors running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-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

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-199724 AOS-214805	Reverse Policy Based Routing (PBR) is not working when applied to the VPN tunnel's Access Control List (ACL) in hub and spoke setups. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-198829 AOS-199188	An incomplete route cache causes the 9004 gateway to not learn the client's ARP. This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-190071 AOS-190372	A few users are unable to access websites when WebCC is enabled on the user role. This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of the user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0 or later versions. **Workaround:** Perform the following steps to resolve the issue: 1.Remove web category from the ACL rules and apply **any any any permit** policy. 2. Disable WebCC on the user role. 3. Change the VLAN of user role from trunk mode to access mode.	AOS-W 8.4.0.0
AOS-182073 AOS-183743	An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT: rcRateFind+229; ratectrl_ 11ac.c:2394**. This issue is observed in OAW-AP315 access points running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
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-151022	The output of the **show datapath uplink** command displays incorrect session count. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
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-230900	Some OAW-AP530 Series and OAW-AP550 Series access points running AOS-W 8.6.0.0 or later versions crash and reboot unexpectedly. The log files list the reason for reboot as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**.	AOS-W 8.7.1.7
AOS-230156	Due to some users' misconfiguration, some virtual mobility conductors running AOS-W 8.6.0.13 or later versions do not retrieve any VLAN IP information in a cluster setup.	AOS-W 8.6.0.13
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

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-229024	Some OAW-AP505 access points running AOS-W 8.7.1.5, or later versions crash and reboot unexpectedly. The log files list the reason for the event as PC is at **wlc_mbo_parse_ie+0x15c/0x2b0 [wl_v6]**.	AOS-W 8.7.1.5
AOS-228704	A few APs running AOS-W 8.6.0.15 or later versions crash and reboot unexpectedly. The log file lists the reason for event as **Reboot Time and Cause: Reboot caused by kernel panic: Take care of the TARGET ASSERT first**.	AOS-W 8.6.0.15
AOS-227154	Mobility Conductors running AOS-W 8.7.1.5 or later versions incorrectly route traffic from external subnets to different ports.	AOS-W 8.7.1.5
AOS-226850	Some Mobility Conductors running AOS-W 8.7.1.5 or later versions incorrectly route traffic to different ports when the client subnet is configured in the same subnet as in the controller port.	AOS-W 8.7.1.5
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-225263 AOS-232589 AOS-242807	L2 database synchronization fails on standby controllers. This issue is observed in stand-alone controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.8.0.1
AOS-224143 AOS-221378	The output of the **show ap debug radio-stats** command displays incorrect Rx data frame statistics. This issue is observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-222469	The number of APs in a network are higher than the number of licenses installed. This issue is observed in stand-alone controllers running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
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-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-236200	Some OAW-AP374 access points configured as mesh are crashing 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-236171	Some OAW-AP635 access points running AOS-W 8.10.0.5 or later versions crash due to a PoE power supply change from AF to AT.	AOS-W 8.10.0.5
AOS-235479	The commands, **copy ftp** and **copy tftp** do not work as expected for the management interface. This issue is observed in Managed Devices running AOS-W 8.6.0.17 or later versions. **Workaround**: Ensure that the file server is reachable via OOB if OOB is configured for platforms that support the OOB Management port.	AOS-W 8.6.0.17

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-234761 AOS-240612 AOS-240809	The **Dashboard > Overview > Wireless** Clients page of the WebUI does not display the IP address of the **Active Controller** and **Standby Controller**. However, the CLI displays the IP address of the active and standby controllers. This issue is observed in Mobility Conductor running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
AOS-234315	A few APs send PAPI messages to external IP addresses, and the log displays 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-233809	Users are unable to add GRE tunnels to a tunnel group and an 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-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-232997	Some managed devices running AOS-W 8.7.1.9 or later versions are stuck after an upgrade and the **aaa** process crashes.	AOS-W 8.7.1.9
AOS-232897	The **wlan ht-ssid-profile** command overrides the radio frequencies from 80 MHz to 40 MHz, although the **show ap bss-table** 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-232620	A discrepancy is observed between the total number of APs and the total number of AP BLE devices reported. This issue is observed in stand-alone controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.8.0.2
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-231473	The **Dashboard > Overview > Wired Clients** page of the WebUI does not display the details of the APs to which clients are connected. This issue occurs in a pure IPv6 deployment. This issue is observed in Mobility Conductor running AOS-W 8.8.0.2 or later versions.	AOS-W 8.8.0.2
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 8.10.0.4

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
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
AOS-239492	APs are rebooting randomly. The log file lists the reason for the event as Reboot Time and Cause: **AP rebooted Tue Oct 11 21:49:53 CEST 2022; Critical process /aruba/bin/sapd [pid 32165] DIED**, process marked as RESTART. This issue is observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-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-237479	Some APs running AOS-W 8.7.1.7 or later versions are unable to form standby tunnels with the cluster nodes. This issue occurs due to a race condition.	AOS-W 8.7.1.7
AOS-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 8.10.0.2
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 Conductor running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-232233	Some 9004-LTE switch 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 8.7.0.0
AOS-232092	Some OAW-AP305 and OAW-AP505 access points are not discoverable by Zigbee devices. The southbound traffic is giving the error in as **AP not found**. This issue is observed on devices running AOS-W8.8.0.1 or later versions.	AOS-W 8.8.0.1
AOS-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-241256	The Global User-Table record displays the MAC addresses of some clients to be associated with multiple APs. The issue is observed in Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.5

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
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 listed the reason for the event as: **Nanny rebooted machine - low on free memory**.	AOS-W 8.10.0.4
AOS-241160 AOS-242900 AOS-243302	Some OAW-AP535 access points running AOS-W 8.10.0.5 or later versions crash and reboot unexpectedly. The log files listed the reason for the event as: **Kernel panic: "Fatal exception in interrupt" and "Take care of the TARGET ASSERT first"**.	AOS-W 8.10.0.5
AOS-241158	The running configuration does not match the previous configuration after upgrading from 6.5.x to 8.x versions. Restarting the Profile Manager may resolve the issue temporarily, but reloading the controller causes the issue again. This issue is observed in standalone 7010 controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.19
AOS-240740	Some OAW-AP635 access points running AOS-W 8.10.0.4 or later versions crash and reboot unexpectedly. The log files listed the reason for the event as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**.	AOS-W 8.10.0.4
AOS-240653	The size of **/mswitch/logs/fpapps.log** file increases indefinitely by 40 MB per month, consuming unnecessary memory resources. This issue is observed in 7210 standalone controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-240435 AOS-242244	Some APs send random false alerts to the OmniVista 3600 Air Manager's monitor to display their status as Down while remaining Active on the controller. The issue is observed in AP-OAW-AP303H Series access points running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
AOS-240419	Some packets loss is observed when sending traffic over a network secured using WPA3 and CNSA. This issue occurs when downloading files from a SMB server in a PC running Windows 10. This issue is observed in OAW-AP505 access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-239821 AOS-243932	The output of the **show running-config** command displays with no left indentations. This issue is observed in AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-239814 AOS-239815	In some switches running AOS-W 8.6.0.11 or later versions, IPv4 and IPv6 Accounting Messages are using the same session ID with Passpoint. This causes multiple Accounting Messages to be sent repeatedly.	AOS-W 8.6.0.11
AOS-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 listed the reason for the event as **Datapath timeout (SOS Assert).**	AOS-W 8.7.1.9

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
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-238817	In some controllers running AOS-W 8.6.0.19 or later versions, the **Dashboard>Security>Suspected Rogue and Authorized** section of the WebUI displays the error message: **Error retrieving information. Please try again later.** This causes the list of APs to not populate correctly. This issue occurs due to non UTF-8 characters being used in external BSSIDs.	AOS-W 8.6.0.19
AOS-238604	The AP regulatory domain profile displays different information in the WebUI and CLI. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17
AOS-238103	Some OAW-AP635 access points are reporting high path loss values when compared to earlier models. This issue is observed in OAW-AP635 access points running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
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
AOS-237710	During ARP discovery, devices with the same IP as the AP's default gateway cause the MAC address of the IP to be overwritten in the ARP cache, leading to unexpected rebootstrap processes. This issue is observed in APs running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-236889 AOS-243540	Some managed devices running AOS-W 8.5.0.13 or later versions are unable to fetch user information through controller API calls. The **show user** command output often states: **This operation can take a while depending on number of users. Please be patient**, with no following response.	AOS-W 8.5.0.13
AOS-235239 AOS-240499	The **Profiles>RF Management>6GHz radio** section in the WebUI does not allow the **Allowed bands for 40MHz channels** option to be set to **None**. 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-232733 AOS-236309 AOS-237431 AOS-237795 AOS-237631	OAW-4650 gateways 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 on 7220 Gateways running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-232717	The VPNC crashes and reboots with reboot cause: **Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:60)**. This issue is observed in VPNCs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-232541 AOS-242776	The WebUI **Configuration>AP Groups>APs** section does not show or apply any configurations beyond the first page. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232208 AOS-241285	The **Maintenance>Software Management>Upload AOS image for controller** page of the WebUI does not allow for image upgrades in OEM builds, yet the WebUI displays it as an option. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-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-239130	The **TOTAL HIT** and **NEW HIT** information in the **Configuration > Authentication > User Rules > Rules-set** page of the WebUI displays as **--**. However, the **show aaa derivation-rules user** command in the CLI displays the information accurately. This issue is observed in Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17
AOS-244664	Dual stack managed devices with ipv6 cluster and Ipv4 APs do not pass traffic after cluster failover when the AAC uplink is shut down on two-node clusters. This issue is observed on APs running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-242983	VPN Concentrator crashes and reboots with the reason **Reboot Cause: Datapath timeout (SOS Assert)**. This issue is observed in some gateways running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-242804	Some AP access points configured as spectrum-monitor or AM incorrectly display as **LOW** performing AP in the switch dashboard. Those APs have been excluded from the AP performance chart. This issue is observed in APs running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-240312	The **arci-cli-helper** process crashes on OAW-4750XM switches running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
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-237174	Some 9240 controllers record informational logs, even though the system log level is configured as **warning**. This issue is observed in 9240 controllers runningAOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-243621	OmniAccess Mobility Controllers send incorrect channel bandwidth data for mesh radios reported in SNMP **wlsxWlanRadioTable**. This issue is observed in Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.10.0.7*

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-244274	OmniAccess Mobility Controllers are truncating the attributes of a query when it forwards a request to an ACL server. This issue is observed only in 8.0.1.0-sp branch.	AOS-W 8.0.1.0
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-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-243722	Some managed devices are unable to display auth-survivability cache entries when certain time zone is configured, like Asia/Jakarta (WIB). This issue is observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS 243536	Some OmniAccess Mobility Controllers display incorrect values in **Discovery State** and **Transport State** for Airgroup services. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-243338	Some APs are randomly shutting down due to IKEv2 exchange timeout. This issue is observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
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 8.6.0.20
AOS-243265	Some OAW-AP515 access points unexpectedly create AP panic dumps, the log files list the reason as: **Unable to handle kernel NULL pointer dereference at virtual address 00000014**. This issue is observed in OAW-AP515 running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-243164	Standalone controllers are unexpectedly crashing in a corner case scenario of **show_auth_tracebuf** process. This issue is observed in standalone controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-243162	Controllers restricted to Egypt, do 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

Table 7: *Known Issues in AOS-W 8.10.0.7*

New Bug ID	Description	Reported Version
AOS-243132	Standalone controllers are not aging out captive portal users from the user table when connected to a wired split tunnel. This issue is observed in standalone controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-243064	Some OAW-AP535 access points crash unexpectedly. The log files list the reason as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first:Excep :0 Exception detectedparam0 :zero, param1 :zero, param2 :zero**. This issue is observed in OAW-AP535 running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-242694	Some APs running AOS-W 8.10.0.5 or later versions create unnecessary syslog events as a warning or error event.	AOS-W 8.10.0.5
AOS-242363	In a Hub-Spoke structure, if a single VLAN is configured in the VPN IP command, VPN Concentrators lose connectivity after a spoke reboots. This issue occurs only when the spoke is rebooted and is not seen under normal operation. This issue is observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-242343	Some wired AirGroup servers are randomly removed from the AirGroup server list. This issue occurs as mDNS advertisement packets having unsupported services are sent from the wired server. 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-241498	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 contains a duplicate of the **logon** role. This prevents the AP from passing user traffic.	AOS-W 8.10.0.5
AOS-242469	Mobile devices are unable to connect to Passpoint SSID. This issue is observed when EAP transactions are sent across two different Radsec connections to cloud guest server. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-242696	An issue is observed when Campus APs running AOS-W 8.6.0.21 or later versions, where they are unable to be converted to Instant APs, while attempting to upgrade. The analysis reveals when the **ap convert** command is run with pre-validation enabled, the process is interrupted before pre-validation completion.	AOS-W 8.10.0.6
AOS-243572	The **WMS** process crashes unexpectedly during bootup of the switch. The process recovers automatically and there is no functionality impact. This issue is observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.7
AOS-241653	Setting the TCP MSS value to 1372 when using an IPSec tunnel triggers a DF-Flag, causing certain websites to be inaccessible. This issue is observed in OAW-4005 switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

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 40 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 40 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 40 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 37.

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

In the WebUI

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

1. Download the AOS-W image from the customer support site.
2. Upload the AOS-W image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-W image:
   a. Download the **Alcatel.sha256** file from the download directory.
   b. Load the AOS-W image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the customer support site.

NOTE

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

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

NOTE

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

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

In the CLI

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

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

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

or

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

or

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

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

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Conductor.

```
(host)#reload
```

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

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

Verifying the AOS-W Upgrade

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

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 40 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 40 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 40.
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.