AOS-W 8.11.1.1 Release Notes

Contents

Chapter 1
Revision History

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

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 2
Release Overview

This AOS-W release notes includes the following topics:

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

Related Documents

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

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

Supported Browsers

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

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

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE engineering terminology to reflect our belief system of diversity and inclusion. Some

legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our ALE culture and moving forward, ALE will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

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

Chapter 3
What's New in AOS-W 8.11.1.1

There are no new features or enhancements introduced in this release.

Chapter 4
Supported Platforms in AOS-W 8.11.1.1

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 3: *Supported Mobility Conductor Platforms*

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

OmniAccess Mobility Controller Platforms

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

Table 4: *Supported OmniAccess Mobility Controller Platforms*

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

AP Platforms

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

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP303H Series	OAW-AP303H, OAW-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP318
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP370EX Series	OAW-AP375EX, OAW-AP377EX, OAW-AP375ATEX
OAW-AP500 Series	OAW-AP504, OAW-AP505
OAW-AP503 Series	OAW-AP503
OAW-AP500H Series	OAW-AP503H, OAW-AP503HR, OAW-AP505H, OAW-AP505HR
OAW-AP510 Series	OAW-AP514, OAW-AP515, OAW-AP518
OAW-AP518 Series	OAW-AP518
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577
OAW-AP580 Series	OAW-AP584, OAW-AP585, OAW-AP585EX, OAW-AP587, OAW-AP587EX
OAW-AP610 Series	OAW-AP615
OAW-AP630 Series	OAW-AP635
OAW-AP650 Series	OAW-AP655

Chapter 5
Regulatory Updates in AOS-W 8.11.1.1

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_86916

Chapter 6
Resolved Issues in AOS-W 8.11.1.1

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
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 This issue was observed in controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.6
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 and running AOS-W 8.7.1.10 or later versions.	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 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
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 s running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-241497	Some 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-242696	Users were unable to convert OAW-AP APs running AOS-W 8.10.0.5 or later versions to Instant APs and AOS-W 10.x APs, while attempting to upgrade. This issue occurred when the **ap convert** command was run with pre-validation enabled, and the pre-validation process was interrupted before completion. The fix ensures that users are able to convert OAW-AP to OAW-IAP and AOS-W 10.x APs even if the pre-validation process is interrupted.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.11.1.1*

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 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-238656	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Kernel panic - not syncing: Take care of the TARGET ASSERT first (ratectrl.c:999).** The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-238815	Some OAW-AP515 APs displayed the status as **busy** when attempting to collect tech-support logs. This issue occurred during the transmission of large packets over the devices. The fix ensures tech-support data can be collected without the AP showing as busy. This issue was observed in APs running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-239183	The WebUI for some OmniAccess Mobility Controllers incorrectly applied daylight savings and displayed an inaccurate time for certain time zones. This behavior was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.10 or later versions. The fix ensures the WebUI is displayed in the correct time according to the set time zone.	AOS-W 8.6.0.10
AOS-240433	ISAKMPD process crash was seen with VIA clients terminated using DHCP server for internal IP allocation. The fix ensures that the ISAKMPD process crash in not seen. 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-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 the WLAN users. The log files listed the reason as **INVAL_HDR_HRD_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-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 Conductor running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
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-243164	Standalone controllers were unexpectedly crashing due to **show_auth_tracebuf** process. The fix ensures the process works as expected. This issue was observed in standalone controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
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-242594	The **profmgr** process crashed on mobility conductors running AOS-W 8.10.0.6. 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-242606	The **show iot-manager ble-services beacon-info** command displayed incorrect and sometimes repeating information. The fix ensures this command displays accurate information as intended. This issue was observed in systems running AOS-W 8.10.0.6.	AOS-W 8.10.0.6
AOS-238817	In some controllers running AOS-W 8.6.0.19, the **Dashboard>Security>Suspected Rogue and Authorized** section of the WebUI displayed an error message: **Error retrieving information. Please try again later.** This caused the list of APs to not populate correctly. This issue occurred because non-UTF-8 characters were added to the backend. The fix ensures the WebUI displays the information correctly.	AOS-W 8.6.0.19
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 mobility controllers running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
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-242379 AOS-243585	Some users were unable to connect to OAW-AP535 access points running AOS-W 8.11.0.1 or later versions. The AP driver log flushed with **NAPI[#ctx]CPU[#]**. The error was related to the AP hardware traffic rings getting stuck and failing to pass traffic successfully. The fix ensures APs work as expected.	AOS-W 8.11.0.1

Table 6: *Resolved Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
AOS-237710	During ARP discovery, devices with the same IP as the AP's default gateway caused the MAC address of the IP to be overwritten in the ARP cache, leading to unexpected rebootstrap processes. The fix ensures the ARP process is executed successfully and APs work as expected. This issue was observed in APs running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-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 mobility controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-242638	In some switches running AOS-W 8.9.0.3 or later versions, Security Association attributes (SAs) were not cleared when crypto-map was 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-241550	Multiple OAW-AP535 access points crashed and rebooted 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 in OAW-AP535 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.0
AOS-241669	A session established with a guest SSID 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 connected through split-tunnel.	AOS-W 8.6.0.9
AOS-241754	Some access points running AOS-W 8.10.0.5 or later versions lost heartbeats, where IPv6 was set in **/tmp/lms**. This caused the APs to crash. The fix ensures the AP performs as expected in this environment.	AOS-W 8.10.0.5
AOS-241870	The **Dashboard > Infrastructure** page displayed APs as **Down** even after being cleared by executing the **clear gap-db ap-name** command. The fix ensures the WebUI displays the expected information. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242066	The **LLDPD** process on some 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 AP **LLDPD** process works as expected.	AOS-W 8.6.0.19

Table 6: *Resolved Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
AOS-241737	The **RADIUS User-Name** attribute contained an empty value in the RADIUS Accounting-Stop packet when an authenticated Captive-Portal client clicked the logout button. The fix ensures the User-Name attribute contains user-name value in the RADIUS Accounting-Stop packet. This issue was observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-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 Alcatel-Lucent Series devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.5
AOS-243132	Standalone controllers did not age out captive portal users from the user table when connected to a wired split tunnel. The fix ensures wired clients are required to re-authenticate to access the network and their status is not active in the user table after certain time. This issue was observed in standalone controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-240435	Some APs sent random false alerts to the OmniVista 3600 Air Manager monitor to display their status as **Down** while remaining **Active** on the controller. The fix ensures the APs send only correct alerts to **Airwave**. This issue was observed in OAW-AP303H access points running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
AOS-241160	Some OAW-AP535 access points running AOS-W 8.10.0.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Kernel panic: "Fatal exception in interrupt" and "Take care of the TARGET ASSERT first"**. The fix ensures the APs work as expected.	AOS-W 8.10.0.5
AOS-240419	Some packets loss was observed when sending traffic over a network secured using WPA3 and CNSA. This issue occurred when downloading files from a SMB server in a PC running Windows 10. This issue was observed in OAW-AP505 access points running AOS-W 8.10.0.5 or later versions. The fix ensures the APs work as expected.	AOS-W 8.10.0.5
AOS-242343	Some wired AirGroup servers were randomly removed from the AirGroup server list. This issue occurred as mDNS advertisement packets having unsupported services were sent from the wired server. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions. The fix ensures OmniAccess Mobility Controllers work as expected.	AOS-W 8.10.0.5
AOS-241801	Some 802.11r client devices running AOS-W 8.10.0.4 or later versions were unable to FT-roam. This issue was related to the PTKSA/GTKSA ReplayCounters in RSNE mismatching with the same in Probe-Response/Beacon packets. The fix ensures that 802.11r client devices are able to roam as expected.	AOS-W 8.10.0.4
AOS-241086 AOS-241860 AOS-242572 AOS-243185	Some clients were unable to connect to the switch 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 are able to connect to the switch as expected.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
AOS-244123		
AOS-243221	9xxx and VMC controllers running AOS-W 8.10.0.5 or later versions were sending **KNI: Out of memory** error logs to the Syslog server. The error logs indicates that the controller is not functioning. The fix ensures controllers stability.	AOS-W 8.10.0.5
AOS-242759	In some devices using curl, the endpointURL parameter was not configured in the IoT radio profile for ASSA ABLOY. This caused memory leaks in the Bluetooth Low Energy (BLE) relay process. The fix ensures that the connection using curl works as expected. This issue was observed in AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-240740	Some OAW-AP635 access points running AOS-W 8.10.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures the APs work as expected.	AOS-W 8.10.0.4
AOS-240653	The size of **/mswitch/logs/fpapps.log** file increased indefinitely by 40 MB per month, consuming unnecessary memory resources. The fix ensures the log files are handled as expected. This issue is observed in standalone controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-242013	Some VIA clients were not able to establish tunnels with controllers as the datapath tunnel table reached maximum capacity. The fix ensures that the tunnel entries are created and deleted properly in datapath tunnel table. This issue was observed on running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244284	Some switches 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-245142	switches were unable to establish a HTTPS connection with the Meridian server. This issue occurred when the software was upgraded to 8.11.0.0 or later versions. The fix ensures that the switches establish a connection with the Meridian server as expected. This issue was observed in switches running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0
AOS-242469	Mobile devices were unable to connect to Passpoint SSID. This issue occurred when EAP transactions were sent across two different Radsec connections to cloud guest server. The fix ensures that mobile devices connect to Passpoint SSID as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2

Chapter 7
Known Issues in AOS-W 8.11.1.1

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

Limitations

Following are the limitations observed in this release.

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

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

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

Airtime Fairness Mode

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

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
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-219315 AOS-223786 AOS-223787 AOS-234981 AOS-240010 AOS-220422	Some OAW-4104 switches running AOS-W 8.7.1.0 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause: 86:50)**.	AOS-W 8.7.1.10
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

Table 7: *Known Issues in AOS-W 8.11.1.1*

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 OAW-4104 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-4005switches 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-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-138608 AOS-243123	A few clients experience packet loss due to high datapath utilization in the CPU. This issue is observed in OAW-4750 switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-239289	The output of the **show datapath cluster details** command displays an incorrect time stamp. This issue occurs when the managed devices are up for more than 49 days. This issue is observed in managed devices running AOS-W 8.10.0.2 or later versions in a cluster setup.	AOS-W 8.10.0.2
AOS-239291 AOS-240342 AOS-241393 AOS-242378 AOS-243717 AOS-244878	OmniAccess Mobility Controllers unexpectedly crash and reboot. The log files list the reason for the event as: **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-236721	The **Configuration** > **Roles & Policies** > **Roles** page of the WebUI does not display ACLs configured for the role. However, the CLI displays the list of ACLs. This issue is observed in Mobility Conductors running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-236235	Multiple APs crash due to a mismatch between **wmm_ eap_ac** and **eapol_ac_override** in the configuration. This issue is observed in OAW-AP535 access points running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2

Table 7: *Known Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
AOS-235744	Some managed devices are unable to receive any configuration from the Mobility Conductor. This issue occurs when changes to a few group names are not synchronized on the standbyMobility Conductor before a reboot. This issue is observed in Mobility Conductors running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-235420	The numbers shown in **Rx Good Frames** and **Rx Frames Received** in the radio stats are the same in OAW-AP555 access points. This issue is observed in APs running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1
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-232717 AOS-243103 AOS-245030	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 managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-230900 AOS-231081 AOS-234940 AOS-238156	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 8.6.0.0
AOS-242983 AOS-242554	The 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-239836	**Nbapi-Helper** process crashes in some OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions. This prevents users from obtaining the feed from the Analytics and Locations Engine (ALE) servers.	AOS-W 8.10.0.2
AOS-239687	Some clients are unable to connect to the 5 GHz radio on OAW-AP515 access points. This issue occurs due to an error in the AP's Broadcom wireless driver. This issue is observed in APs running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-239321 AOS-240598 AOS-243974	Some OAW-AP635 access points crash and reboot unexpectedly. The log files list the event as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT**. The crash-info shows that the AP firmware is asserted at whal_recv.c:1656. The issue is observed on APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239165	Some OAW-AP635 access points running AOS-W 8.10.0.2 or later versions crash and reboot unexpectedly. The log files list the reason for the event as, **Reboot caused by kernel panic with "sched_algo_qos.c:3794 Assertion (rtxop > 0) failed"**.	AOS-W 8.10.0.2

Table 7: *Known Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
AOS-238968	Some APs fail to send the IDS deauthentication frames even when the protect valid station parameter is enabled. This issue occurs when the APs are connected in AM mode on the 5 GHz channel. This issue is observed in OAW-AP515 and OAW-AP505 access points running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-238681	The RADIUS request access packets contain the IP address of the Mobility Conductor as the NAS IP address instead of the CoA VRRP IP address of the managed device. Hence, some clients may experience connectivity issues. This issue is observed in managed devices running AOS-W 8.9.0.1 or later versions in a cluster setup.	AOS-W 8.9.0.1
AOS-238150	Users who are connected through IAP-VPN are not listed in the SNMP table. This issue is observed in switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-241228	In some standby switches, the **disable allowlist-sync** command may be executed causing the switches to enter a CONFIG_FAILURE state. This command is intended for primary switches only. This issue is observed in switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-240995	While downloading the VIA subnets, the endian conversion may not happen as expected. This may result in the VIA subnet routes getting installed in reverse order. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-240954	Some OAW-AP555 access points running AOS-W 8.10.0.5 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**.	AOS-W 8.10.0.5
AOS-240953	Some OAW-AP635 access points may fail to send data frames when configured in tunnel mode using opmode wpa3-sae-aes encryption. Clients may also be unable to obtain IP addresses. This issue is caused by PMF drop when the **Prohibit IP Spoofing** policy is enabled. This issue is observed on APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240601	In some OAW-AP500 Series access points running AOS-W 8.10.0.2 or later versions, the Scheduler Algorithm causes a delay which may introduce latency in the MU schedule for multiple clients.	AOS-W 8.10.0.2
AOS-240347	Users may be unable to collect the tech support logs of the Mobility Conductor. This issue is observed in Mobility Conductors running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240279	Mobility Conductors running AOS-W 8.10.0.4 or later versions may push additional IGMP and OSPF configurations to managed devices. This issue occurs when a VLAN configuration is edited.	AOS-W 8.10.0.4

Table 7: *Known Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
AOS-240185	Clients may be unable to obtain user roles from ClearPass Policy Manager and may fall into their initial role. This issue occurs due to radius accounting. This issue is observed in managed devices running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
AOS-240149	Some OAW-AP635 access points running AOS-W 8.10.0.5 reboot and crash unexpectedly. The log files list the event as, **Reboot caused by FW crash**. The issue is observed on APs running AOS-W 8.10.0.5 versions.	AOS-W 8.10.0.5
AOS-240014	In some controllers running AOS-W 8.7.1.4 or later versions, an invalid AP console password may be displayed in the AP system profile. This issue is caused by an incorrect password string length.	AOS-W 8.7.1.4
AOS-239238 AOS-239728 AOS-241834 AOS-243671 AOS-243803 AOS-244598	The AP-provisioning process fails for some of the APs, preventing them from being configured properly. This issue is observed in APs running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1
AOS-239324 AOS-238844 AOS-243905	In some OAW-AP535 access points running AOS-W 8.10.0.2 or later versions, users are unable to associate to neighboring APs, with deauthentication message **Reason Class 2 frames from non authenticated STA**. This issue occurs in 5 GHz SSIDs.	AOS-W 8.10.0.2
AOS-242852	In some controllers running AOS-W 8.10.0.4 or later versions, tunneled_user creation fails upon a bridge miss.	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 are blank because the parser was in multi-line mode after executing show configuration datastore.	AOS-W 8.10.0.4
AOS-242119	In some switches running AOS-W 8.10.0.4 or later versions, policy names are not displaying in alphabetical order in the controller WebUI.	AOS-W 8.10.0.4
AOS-241957	The WebUI requires specifying a category when adding a logging server in **Configuration > System > Logging**. This should not be mandatory for logging server configuration. This issue is observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241937	A few user-based tunnelled users fail to come up on managed devices due to certain race condition in the sequence of events during the user bootstrap process. This issue is observed in managed devices running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-241863	The ACL is incomplete in the SAPD and data path modules, and it causes connectivity issues. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 7: *Known Issues in AOS-W 8.11.1.1*

New Bug ID	Description	Reported Version
AOS-241841	Some OmniAccess Mobility Controllers are unable to ping their default gateway and display neighbor entries when using IPv6. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241464 AOS-242568	Some OAW-AP535, OAW-AP555, OAW-AP585, OAW-AP635, and OAW-AP655 access points crash and reboot unexpectedly. The log files list the event as, **kernel panic: Fatal exception, PC is at nss_ipsecmgr_sa_add_sync+0x4c/0x400 [qca_nss_ipsecmgr].** The issue is observed in APs running AOS-W 8.10.0.4 or later versions in a cluster setup.	AOS-W 8.10.0.4
AOS-241313	Zebra TC21 barcode scanners are unable to maintain a connection and send traffic when connected to OAW-AP505 devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
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-228445	Alcatel-Lucent 9012 Branch Gateways running AOS-W 8.6.0.4 or later versions do not show **Usage and Throughput** information in the WebUI, under **Overview > WAN > WAN SUMARRY**. A **No data to display right now** error message is shown.	AOS-W 8.6.0.4
AOS-227306	Some managed devices respond to the ARP probe frames with the SRC MAC address of the clients that are not connected to the network. This issue is observed inmanaged devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-227154	Mobility Conductor 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 Conductor 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-222469	The number of APs in a network are higher than the number of licenses installed. This issue is observed in standalone switches running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12

Chapter 8
Upgrade Procedure

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

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

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

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

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

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 27 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 27 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 27 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Low Free Flash Memory

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

Prerequisites

Before you proceed with the freeing up the flash memory:

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

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

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

Freeing up Flash Memory

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

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

   Table 8: *Flash Memory Requirements*

Upgrading from	Upgrading to	Minimum Required Free Flash Memory Before Initiating an Upgrade
8.3.x	8.11.x	360 MB
8.5.x	8.11.x	360 MB
8.6.x	8.11.x	570 MB
8.7.x	8.11.x	570 MB
8.8.x	8.11.x	450 MB
8.9.x	8.11.x	450 MB
8.10.x	8.11.x	450 MB

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

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

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

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

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

     Please clean up the /flash and try upgrade again.

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

     Please clean up the /flash and try upgrade again.

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

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

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

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

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

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

```
*****************************************************************
* WARNING:  An additional image upgrade is required to complete the *
```

```
* installation of the AP and WebUI files. Please upgrade the boot   *
* partition again and reload the controller.                         *
**********************************************************************
```

- Repeat steps 1 through 5. If sufficient free flash memory is available, proceed with the standard AOS-W upgrade procedure. See Upgrading AOS-W.
- If sufficient free flash memory is not available, issue the **dir** and **dir flash** commands to identify large files occupying the flash memory.

Exercise caution while deleting files. Contact Technical Support if you are not sure which large files in the **/flash** directory could be safely deleted to free up the required space.

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 24.

NOTE

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.

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 27 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 27 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 27.
2. Verify that the control plane security is disabled.
3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Conductor or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. From **Select destination file** drop-down list, select **Flash file system**, and enter a file name (other than default.cfg).
   c. Click **Copy**.
2. Determine the partition on which your pre-upgrade AOS-W version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade AOS-W version is not stored on your system partition, load it into the backup system partition by performing the following steps:


CAUTION

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot Controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, and click **Reboot**.

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

In the CLI

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

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

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

   or

   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the Mobility Conductor or managed device to boot with your pre-upgrade configuration file.

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

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

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

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.