AOS-W 8.9.0.3 Release Notes

Copyright Information

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 02	The bug **AOS-218873** has been added to the list of resolved issues.
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:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 on Windows 7, Windows 8, Windows 10, and macOS

Guidelines Before Upgrading 7000 Series Controllers to AOS-W 8.9.0.0

Customers with deployments containing the following 7000 Series switches should read the Low Free Flash Memory requirements prior to attempting an upgrade of the 7000 Series switches to AOS-W 8.9.0.0:

- 7005
- 7008
- 7010

If you are unable to free up sufficient flash memory, contact Technical Support. Do not reboot the switch.

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

Contact Center Online	
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

Chapter 3
New Features and Enhancements in AOS-W 8.9.0.3

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

CLI

apflash command

Starting from AOS-W 8.9.0.3, the **apflash ap31x-ap32x backup partition** command upgrades the backup partition of Alcatel-Lucent OAW-AP310 Series and 320 Series access points running AOS-W 6.4.x or earlier versions to the AOS-W version running on the Mobility Conductor.

```
(host) [mynode] #apflash ap31x-ap32x backup partition
```

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	OAW-MM-HW-1K, OAW-MM-HW-5K, OAW-MM-HW-10K
Virtual Mobility Conductor	OAW-MM-VA-50, OAW-MM-VA-500, OAW-MM-VA-1K, OAW-MM-VA-5K, OAW-MM-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 Hardware OmniAccess Mobility Controllers	OAW-4005, OAW-4010, OAW-4030
OAW-4x50 Series Hardware OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series Hardware OmniAccess Mobility Controllers	OAW-4104
MC-VA-xxx Virtual OmniAccess Mobility Controllers	OAW-MC-VA-10, OAW-MC-VA-50, OAW-MC-VA-250, OAW-MC-VA-1K

AP Platforms

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

Table 5: *Supported AP Platforms*

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

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP203H Series	OAW-AP203H
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, 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
500 Series	OAW-AP504, OAW-AP505
500H Series	AP-503H, AP-505H
510 Series	OAW-AP514, OAW-AP515, AP-518
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555
560 Series	AP-565, AP-567
570 Series	AP-574, AP-575, AP-577
630 Series	AP-635

Chapter 5
Regulatory Updates in AOS-W 8.9.0.3

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_83211

Chapter 6
Resolved Issues in AOS-W 8.9.0.3

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.9.0.3*

New Bug ID	Description	Reported Version
AOS-199971 AOS-229489	Mobility Conductors running AOS-W 8.5.0.6 or later versions generated a lot of httpd debug messages. This issue occurred when the logging levels configured using the CLI were not updated on the Mobility Conductor. The fix ensures that the logging levels are updated correctly and the Mobility Conductor works as expected.	AOS-W 8.5.0.6
AOS-212772 AOS-221882	Some IPv6 clients were unable to access websites that had only IPv4 addresses. The fix ensures that the IPv6 clients are able to access websites that have only IPv4 addresses. This issue was observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-214524	Some APs running AOS-W 8.6.0.6 or later versions detected its own BSSIDs as rogue BSSIDs. Enhancements to the driver resolved the issue. **Duplicates:** AOS-225132, AOS-226070, AOS-226617, AOS-218317	AOS-W 8.6.0.6
AOS-217653 AOS-224031 AOS-222483	Some OAW-AP535 access points running AOS-W 8.7.1.4 or later versions did not respond to the fragmented ping requests from a few clients. This issue occurred when the APs operated in tunnel mode. The fix ensures that the APs respond to the fragmented ping requests.	AOS-W 8.7.1.4
AOS-218435	The status of the VRRP switch changed to **INIT** state after adding a VLAN. The fix ensures that the VRRP instance functions as expected. This issue was observed in managed devices running AOS-W 8.2.2.2 or later versions.	AOS-W 8.2.2.2
AOS-218873 AOS-230672	High SAPD memory utilization was observed and APs dropped DHCP packets. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.9.0.1 or later versions	AOS-W 8.9.0.1
AOS-219255 AOS-227048	The **show running-config** command did not display information related to session ACL. However, the **show configuration effective** command displayed information about the session ACL. The fix ensures that the **show running-config** command displays information related to session ACL. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-219702	A few APs incorrectly reported a hotspotter attack. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7

Table 6: *Resolved Issues in AOS-W 8.9.0.3*

New Bug ID	Description	Reported Version
AOS-219739	The **profmgr** process crashed on the backup Mobility Conductors running AOS-W 8.7.1.0 or later versions. The fix ensures that the Mobility Conductor works as expected.	AOS-W 8.7.1.0
AOS-220254	Users were unable to pass traffic to the internet. This issue occurred when APs could not source NAT the traffic as the traffic got incorrectly tunneled to the switch. The fix ensures that the users are able to pass traffic to the internet. This issue was observed in stand-alone switches running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-220841	Some clients were unable to connect to OAW-AP535 access points that operated on A band. This issue occurred due to false radar detection on non-DFS channels. The fix ensures that there is no false radar detection on non-DFS channels. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-220982	A few wireless clients were unable to pass traffic during a cluster failover. The fix ensures that the clients are able to pass traffic during a cluster failover. This issue was observed in managed devices running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-221307	Adding a new VLAN removed all the existing VLANs on the port channel. This issue occurred when the existing VLAN list exceeded 256 characters. The fix ensures that the VLAN list supports up to 1024 characters. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.8
AOS-221313 AOS-230746	A few AP-635 access points running AOS-W 8.9.0.0 or later versions did not send core files to the dump server. The fix ensures that the APs transfer core files to the dump server.	AOS-W 8.9.0.0
AOS-222037	The cellular handoff assist feature did not work as expected on APs running AOS-W 8.7.1.3 or later versions. The fix ensures that the cellular handoff assist feature works as expected.	AOS-W 8.7.1.3
AOS-222152	A few clients faced connectivity issues. This issue occurred due to a race condition where the PHY mode of the initially configured virtual AP was incorrectly applied to all the other virtual APs. The fix ensures that the 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-222589	Some OAW-AP535 access points running AOS-W 8.7.1.3 or later versions crashed unexpectedly. The log files listed the reason for the event as **kernel panic: Fatal exception in interrupt**. This issue occurred when the UCC RTPA configuration was enabled. The fix ensures that the APs work as expected. **Duplicates:** AOS-222575, AOS-222576, AOS-223063, AOS-223138, AOS-224724, AOS-228455, AOS-229030, AOS-231082, and AOS-231084	AOS-W 8.7.1.3
AOS-222936	A few clients were unable to connect to AP-565 mesh access points running AOS-W 8.7.1.4 or later versions. The log files listed the reason for this event as **UAC Down**. The fix ensures seamless connectivity.	AOS-W 8.7.1.4

Table 6: *Resolved Issues in AOS-W 8.9.0.3*

New Bug ID	Description	Reported Version
AOS-223094 AOS-220190 AOS-224240 AOS-224792 AOS-226989 AOS-228434	A few users were unable to login to the captive portal page that was hosted on ClearPass Policy Manager server. This issue occurred when the netdestination ID, which was added to the captive portal allowlist, was incorrectly changed to 0 after a reboot of the Mobility Conductor Virtual Appliance. This issue is observed in Mobility Conductor Virtual Appliances running AOS-W 8.5.0.10 or later versions.	AOS-W 8.6.0.9
AOS-223320	The mesh QoS queues were not transmitted as expected. The fix ensures that the Mobility Conductors work as expected. This issue was observed in Mobility Conductors running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-223656 AOS-227360	Some OAW-RAPs were unable to come up on managed devices after a reboot. The fix ensures that the OAW-RAPs are able to come up on managed devices. This issue was observed in managed devices running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-223817	The **auth** process crashed on Mobility Conductors running AOS-W 8.6.0.9 or later versions. The fix ensures that the Mobility Conductors work as expected. **Duplicates:** AOS-225761, AOS-226316, AOS-226846, AOS-227879, AOS-225878, and AOS-229146	AOS-W 8.6.0.9
AOS-224019 AOS-226123	High dpagent memory utilization was observed on managed devices running AOS-W 8.6.0.9 or later versions. The fix ensures that the managed devices work as expected. **Duplicates:** AOS-224821, AOS-225436, AOS-225976, AOS-226123,AOS-227558, AOS-228839, AOS-228983, AOS-229064, AOS-229981, AOS-230241, and AOS-230509	AOS-W 8.6.0.9
AOS-224105	The **wlsxVoiceClientLocationUpdate** SNMP traps were not generated when the clients roamed to a new AP. The fix ensures that the SNMP location update traps are generated when clients roam between APs. This issue was observed in Mobility Conductors running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-224296	A few clusters got disconnected from the network. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.7.1.3 or later versions. Duplicates: AOS-225598, AOS-225876, AOS-226115, AOS-227314, and AOS-230041	AOS-W 8.7.1.3
AOS-224470 AOS-226745	A few APs running AOS-W 8.9.0.0 or later versions did not generate the AP containment logs. The fix ensures that the APs generate the appropriate logs.	AOS-W 8.9.0.0
AOS-224491	A few OAW-AP515 access points running AOS-W 8.9.0.0 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at ina2xx_get_value+0x110/0x168**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.0

Table 6: *Resolved Issues in AOS-W 8.9.0.3*

New Bug ID	Description	Reported Version
AOS-225508	Some managed devices running AOS-W 8.7.1.4 or later versions sent ARP requests with an incorrect MAC address. The fix ensures that the managed devices do not send ARP requests with an incorrect MAC address.	AOS-W 8.7.1.4
AOS-225659 AOS-226682	The **auth** process crashed on managed devices running AOS-W 8.6.0.10 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.10
AOS-225817	Some AP-315 access points running AOS-W 8.5.0.13 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Reason: Reboot caused by kernel panic: assert**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.13
AOS-226016	Some clients were able to access the internet even if the denyall user role was applied. The fix ensures that the clients are unable to access the internet if the denyall user role was applied. This issue was observed in managed devices running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-226320 AOS-228465	Some users were unable to perform the 802.1X authentication. This issue occurred when a few host IP addresses were removed from the netdestination list. The fix ensures that the users are able to perform the 802.1X authentication. This issue was observed in managed devices running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-226331	The MTU discovery did not work as expected when the OAW-RAP connected to the VRRP virtual IP of the switch. The fix ensures that the MTU discovery works as expected. This issue was observed in stand-alone switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-226440	The **auth** process crashed on stand-alone switches running AOS-W 8.5.0.11 or later versions. This issue occurred after changing the downloadable role configuration. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.5.0.11
AOS-226467 AOS-229346	The stale AirGroup server entries were not deleted even when the server was disconnected from the network. The fix ensures that the managed devices remove the stale AirGroup server entries. This issue was observed on managed devices running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-226475 AOS-229726	A few APs displayed flag **D**, indicating **Dirty or no config** state while provisioned to an AP group. The fix ensures that the APs do not display the D flag. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-226555 AOS-224165	The **WMS** process crashed on Mobility Conductors running AOS-W 8.7.1.3 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.7.1.3

Table 6: *Resolved Issues in AOS-W 8.9.0.3*

New Bug ID	Description	Reported Version
AOS-226683	The **show running-config** command did not display information related to IP RADIUS source-interface loopback. However, the **show configuration effective detail** command displayed information about the IP RADIUS source-interface loopback. The fix ensures that the **show running-config** command displays information related to IP RADIUS source-interface loopback. This issue was observed in managed devices running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-226787	Configuration failure was observed on managed devices running AOS-W 8.8.0.0 or later versions and an error message, **Error: System role 'default-iap-user-role' is not editable** was displayed. This issue occurred after configuring the PEFNG license. The fix ensures that the managed devices work as expected.	AOS-W 8.8.0.0
AOS-226824 AOS-227422	A few clients were unable to connect to APs running AOS-W 8.6.0.10 or later versions. This issue occurred when, ■ HT and VHT radio profiles were disabled but when HE configuration was enabled on the APs. ■ the 4-way handshake was not successful. The fix ensures seamless connectivity.	AOS-W 8.6.0.10
AOS-226932 AOS-228418 AOS-229018	Some OAW-AP515 access points running AOS-W 8.7.1.5 crashed unexpectedly. The log files listed the reason for the event as **wlc_pktq_stats_free+0x48**.The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-226970 AOS-228931	The bandwidth limit configured for a user role was not applied correctly for clients connected in bridge forwarding mode. The fix ensures that the bandwidth limit is applied correctly for clients connected in bridge forwarding mode. This issue was observed in managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-226978	L2 option-82 did not work as expected on Mobility Controller Virtual Appliances running AOS-W 8.6.0.6 or later versions. This issue occurred due to incorrect endianness. The fix ensures that the Mobility Controller Virtual Appliances work as expected.	AOS-W 8.6.0.6
AOS-227032	When AirMatch intermittently tried to update the EIRP values for 5Ghz radio, the virtual APs went down. The fix ensures that the Mobility Conductors work as expected. This issue was observed in Mobility Conductors running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-227039	Some AP-505H mesh access points running AOS-W 8.7.1.5 or later versions were stuck in **D** flag after an upgrade. The fix ensures that the APs work as expected.	AOS-W 8.7.1.5
AOS-227081 AOS-226543 AOS-213220	DPI failed to classify traffic and hence, application traffic was categorized as Port 0. The fix ensures that DPI classifies traffic as expected. This issue was observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-227457 AOS-227613	Data frames that were larger in size were dropped unexpectedly. This issue occurred when managed devices routed traffic through IPsec tunnels. The fix ensures that the managed devices do not drop data frames. This issue was observed in managed devices running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10

Table 6: *Resolved Issues in AOS-W 8.9.0.3*

New Bug ID	Description	Reported Version
AOS-227660	The second user that got connected to the network was unable to download the VIA profile. This issue occurred when the client was marked with the **D** flag in the datapath session for logon role. The fix ensures that the users are able to download the VIA profile. This issue was observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227858	Users were unable to load the XML file while configuring DHCP option 82 and an incorrect error message, **Error: Filename my_dhcp_option_82_mod2.xml has invalid keywords** was displayed. The fix ensures that the users are able to load the XML file and the Mobility Conductor displays appropriate error messages. This issue was observed in Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-227905 AOS-227848	A few APs running AOS-W 8.6.0.14 or later versions generated a lot of kernel messages. The log files listed the reason for the event as **ipv6: Neighbour table overflow**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.14
AOS-228112	The AirGroup server table incorrectly displayed duplicate AirGroup server entries with the same host name. The fix ensures that the AirGroup server table does not display duplicate entries. This issue was observed in Mobility Conductors running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-228138	A few clients were unable to perform authentication and incorrectly got reverted to the initial role. The fix ensures that the clients are able to perform authentication and they are assigned the correct role. This issue was observed in APs running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-228148	A few APs running AOS-W 8.9.0.0 or later versions failed to generate the RSA key. The fix ensures that the APs work as expected.	AOS-W 8.9.0.0
AOS-228319	Some OAW-AP535 access points running AOS-W 8.7.1.6 or later versions crashed unexpectedly. The log files listed the reason for the event as **FW Exception :Excep :0 Exception detected, Thread ID: 0x00000069 Thread name : WLAN BE**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.6
AOS-228390	A few managed devices running AOS-W 8.6.0.11 or later versions delayed in sending the IGMP report to the multicast server. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.11
AOS-228466 AOS-224923	Some managed devices running AOS-W 8.8.0.0 or later versions incorrectly sent the inner IP address as the calling station ID for VIA authentication. The fix ensures that the managed devices do not send the inner IP address as the calling station ID for VIA authentication.	AOS-W 8.8.0.0
AOS-228579	A few clients were disconnected from the network while roaming between APs. This issue occurred when the 802.11r option was enabled on APs. The fix ensures that the clients are not disconnected from the network. This issue was observed in APs running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0

Table 6: *Resolved Issues in AOS-W 8.9.0.3*

New Bug ID	Description	Reported Version
AOS-228631	The TEXTUAL-CONVENTION and Timeticks MIBs were incorrectly defined and were imported from incorrect SNMP traps. The fix ensures that the MIBs are defined correctly. This issue was observed in Mobility Conductors running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-228818	A few APs that operated in bridge mode dropped SMB packets. This issue occurred when the APs and clients were on different VLANs. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535, OAW-AP555, and AP-635 access points access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.8.0.2
AOS-228949 AOS-229237 AOS-229497	The cfg database was not available on managed devices running AOS-W 8.6.0.14 or later versions. This issue occurred when the managed devices failed to remove the old log files. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.14
AOS-229015 AOS-227266	A few clients were disconnected from the network with an error message, **Unspecified Failure**. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-229620	Some AP-635 access points running AOS-W 8.9.0.1 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as R**eboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.1
AOS-230850	The wireless drivers of a few APs did not have a few files required for debugging. Enhancements to the wireless driver resolved the issue. This issue was observed in APs running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-230957	Mobility Conductor Hardware Appliance running AOS-W 8.9.0.1 or later versions was unable to monitor and provision managed devices and /tmp folder was fully utilized. The fix ensures that the Mobility Conductor Hardware Appliance works as expected.	AOS-W 8.9.0.1

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

Limitation

Following is the limitation observed in this release.

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
```

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	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-153742 AOS-194948	188871	A stand-alone switch crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in OAW-4010 switchesrunning AOS-W 8.5.0.1 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.5.0.1
AOS-156428 AOS-211063	–	All managed devices in a cluster respond to the ARP request of the client. This issue occurs when either local proxy or broadcast-multicast optimization is enabled on managed devices. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
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 user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0. **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-190621	–	WebUI does not filter the names of the APs that begin with the special characters, + and %. This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2
AOS-195434	–	An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is observed in APs running AOS-W 8.5.0.0 o or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.5.0.2
AOS-196042 AOS-217995 AOS-221263	–	The **show ucc dns-ip-learning** command displays **Unknown** for **Service Provider**. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-203682	–	The **Dashboard > WLANs** page of the WebUI does not display the list of all clients and APs. This issue is observed in Mobility Conductors running AOS-W 8.5.0.2 or later versions. **Duplicates:** AOS-195432, AOS-195433, AOS-218290, and AOS-220829	AOS-W 8.6.0.15
AOS-205140	–	The AppRF ACLs using a voice role block WebRTC calls. This issue occurs when WebRTC audio and video ACLs are not part of the default **voip-applications-acl**. This issue is observed in Mobility Conductors running AOS-W 8.6.0.8 or later versions. **Workaround**: Add WebRTC audio and video ACLs to the user role using the following command: **ip access-list session webrtc** **any any app alg-webrtc-audio permit** **any any app alg-webrtc-video permit**	AOS-W 8.6.0.8
AOS-208853	–	Some OAW-AP555 access points in bridge mode do not transmit multicast traffic at the configured multicast rate and continue to transmit multicast traffic at the lowest default tx-rate. This issue is observed in OAW-AP555 access points running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-214041	–	A few APs running AOS-W 8.5.0.5 or later versions are unable to establish S-AAC tunnel with the managed devices. This issue occurs after configuring 802.1X authentication.	AOS-W 8.5.0.5
AOS-214575 AOS-228506	–	A few APs running AOS-W 8.3.0.13 or later versions take a long time to come up on the Mobility Controller Virtual Appliance. This issue occurs when, ■ factory reset APs are re-provisioned from Mobility Conductor Hardware Appliances. ■ the IP address of the Mobility Controller Virtual Appliance is configured as the LMS IP address in the AP system profile .	AOS-W 8.3.0.13
AOS-215063	–	The output of the **show gsm debug channel cluster_aac** and **show gsm debug channel cluster_ap** commands is not filtered correctly. This issue is observed in Mobility Conductors running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-215357 AOS-220057	–	A few managed devices are unable to transmit IPv4 traffic to the Mobility Conductor intermittently. This issue is observed in Mobility Conductors running AOS-W 8.5.0.10 or later versions in a Mobility Conductor – Managed devices dual stack deployment.	AOS-W 8.5.0.10
AOS-215727 AOS-216896 AOS-217593	–	Stale AP entries that were cleared using the **clear gap-db** command prior to the upgrade reappears on the Mobility Conductor after the upgrade. This issue is observed in Mobility Conductors running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
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 get the branch IP address as the switch IP address in a VPNC deployment.	AOS-W 8.5.0.11
AOS-217628 AOS-221178 AOS-226513 AOS-226575 AOS-226753	–	Some managed devices running AOS-W 8.5.0.11 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Kernel Panic (Intent:cause:register 12:86:b0:2**.	AOS-W 8.5.0.11
AOS-218988	–	Some managed devices running AOS-W 8.5.0.10 or later versions incorrectly use the VRRP IP address as the source interface to transmit PAPI traffic to the AMON server.	AOS-W 8.5.0.10
AOS-219483	–	The output of the **show ap debug receive-config** command displays incorrect value for **VLAN**. This issue is observed in Mobility Conductors running AOS-W 8.6.0.0 or later versions.	AOS-W 8.9.0.0

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219619	–	Configurations inherited from the Mobility Conductor are incorrectly displayed as **local/mm** indicating that the configurations are locally enabled on the managed devices. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-219803	–	The XML query done on a non-existing user results in an invalid response. This issue is observed in managed devices running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-220706	–	The Mobility Conductor assigns duplicate IP addresses to the managed devices. This issue occurs after a failover. This issue is observed in Mobility Conductors running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-221789 AOS-223052	–	The 802.1X authentication is initiated twice. This issue is observed in APs running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.9
AOS-221883 AOS-221884	–	Users are unable to add ACLs using the **firewall cp** command and an error message, **Error: Max CP firewall limit (97) reached** is displayed. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-221982	–	Some VIA users experience connectivity issues. This issue is observed on IKEV2 EAP-GTC terminated VIA clients that use external CPPM authentication. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-222267 AOS-212114 AOS-217474 AOS-219497 AOS-225306	–	A few managed devices go down intermittently. This issue occurs when the traffic between Mobility Conductor and managed devices is transmitted without IPsec encryption. This issue is observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-222469	–	The number of APs in a network are higher than the number of licenses installed. This issue is observed in stand-alone switches running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-222499	–	Clients that perform only four-way handshake are unable to update their VSA role derived after machine and user authentication. This issue is observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-222578	–	L2TP IP address leak is observed and the VLAN pool is exhausted. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-223273	–	The UBT users list is not available in the user table after a cluster failover. This issue is observed in Mobility Conductor running AOS-W 8.7.1.4 or later versions in a cluster setup.	AOS-W 8.7.1.4
AOS-223274	–	Packet drop is observed on LACP configured OAW-AP535 access points running AOS-W 8.7.1.4 or later versions. This issue occurs when the outer IP header TOS value is different than the original inner IP header in ICMP error frame since the switch sends the ICMP destination unreachable frames back to the sender.	AOS-W 8.7.1.4
AOS-223337	–	The clients added to the client match unsupported list are still considered for client match steers. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-223452	–	There is a delay observed in the update of the ARP table. This issue occurs when clients use same IP address but different MAC addresses. This issue is observed in switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-223577	–	The user table entries display only the IPv6 link local address. This issue is observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.6.0.5
AOS-223667	–	High CPU utilization is observed on managed devices running AOS-W 8.5.0.13 or later versions. This issue occurs when the network is scanned for security vulnerabilities.	AOS-W 8.5.0.13
AOS-223669	–	Some users are unable to complete captive portal authentication. This issue occurs when ipv6-user snmpwalk populates IPv4 user details. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-223709	–	Mobility Conductors running AOS-W 8.5.0.0 or later versions crash unexpectedly. This issue occurs due to a race condition. The log files list the reason for the event as **nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**.	AOS-W 8.8.0.0
AOS-223945	–	A managed device is discovered by both primary and secondary Mobility Conductors in a Layer 3 redundancy deployment. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-223988 AOS-230744	–	The **cli** process crashes on managed devices running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-224275 AOS-215206	–	The predefined v6-control policy does not allow DHCPv6 traffic. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.9

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-224326 AOS-226350	–	A few OAW-AP514 access points running AOS-W 8.7.1.5 or later versions crash unexpectedly. The log files list the reason for the event as **PC is at wlc_ratesel_set_link_bw+0x0**.	AOS-W 8.7.1.5
AOS-224402	–	The **OSPF** process crashes on Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-224538	–	A few APs running AOS-W 8.5.0.11 or later versions incorrectly fall back to the default AP group.	AOS-W 8.5.0.11
AOS-224676	–	Some managed devices running AOS-W 8.8.0.0 or later versions log the error message, **httpd[2413]: Could not retrieve the CSRF token from db inside mod_aruba_auth**. This issue occurs when the IP address of an OmniVista 3600 Air Manager server is added.	AOS-W 8.8.0.0
AOS-224688	–	The HE enabled APs are incorrectly displayed as **HTT None** in OmniVista 3600 Air Manager. This issue is observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-224901	–	A few APs terminating in the backup LMS cluster do not move to the LMS cluster after a reboot. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-224961	–	The global user entries table is not updated when clients roam to a different AP. This issue occurs when 802.11r is enabled. This issue is observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-225070	–	The AirGroup server table incorrectly displays duplicate host names. This issue is observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-225135	–	Clients connected to a few APs are unable to send or receive data packets from APs. This issue occurs when the ACL changes are not updated on APs. This issue is observed in APs running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-225214	–	A few managed devices incorrectly send the VPNC IP address as 0.0.0.0 to the OmniVista 3600 Air Manager server. This issue is observed in managed devices running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-225231	–	The captive portal redirection URL does not display the complete ESSID. This issue occurs when the ESSID has 32 characters. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-225268	–	Some OAW-RAPs are assigned to incorrect nodes. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions in a cluster setup.	AOS-W 8.7.1.3

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-225517	–	Some APs running AOS-W 8.5.0.12 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **DHCP Lease expired**.	AOS-W 8.5.0.12
AOS-225538	–	Some OAW-AP335 access points running AOS-W 8.6.0.9 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic:Fatal exception in interrupt with Target Assert**.	AOS-W 8.6.0.9
AOS-225549	–	Some stand-alone switches running AOS-W 8.6.0.8 or later versions lose its netdestination aliases, user roles, and ACLs after a reboot.	AOS-W 8.6.0.8
AOS-225563	–	Low throughput issue is observed on OAW-AP515 access points running AOS-W 8.7.1.4 or later versions. This issue occurs when AP LACP is configured on OAW-AP515 access points.	AOS-W 8.7.1.4
AOS-225660	–	The **UCM** process crashes on Mobility Conductors running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.1.4
AOS-225707	–	The **Configuration > License > License Inventory** page of the WebUI incorrectly displays the date of the present day as the expiration date for EVAL license. This issue is observed in Mobility Conductors running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-225856 AOS-228686	–	The **im_helper** process is stuck in **Busy** state and high CPU utilization is also observed. This issue occurs after configuring a ble-service profile. This issue is observed in Mobility Conductors running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-225873	–	Some managed devices running AOS-W 8.7.1.4 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Datapath timeout (sos_xlp_process_poe_msg)**.	AOS-W 8.7.1.4
AOS-226012 AOS-226013	–	Mobility Controller Virtual Appliances running AOS-W 8.7.1.4 or later versions respond with its own MAC address as the management IP address for ARP requests.	AOS-W 8.7.1.4
AOS-226075	–	The logs generated by the stand-alone switch do not have source and destination port details and the logs also indicate that all TCP packets are fragmented. This issue is observed in stand-alone switches running AOS-W 8.6.0.12 or later versions.	AOS-W 8.6.0.12
AOS-226177	–	The **firewall deny-reserved-ip** and **ipv6 firewall deny-reserved-ip** commands incorrectly deny non-reserved IP addresses. This issue is observed in Mobility Conductors running AOS-W 8.6.0.9-FIPS or later versions.	AOS-W 8.6.0.9-FIPS

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-226343	–	L2TP users are randomly assigned to different VLAN pools. This issue occurs when the configured VLAN pool is exhausted. This issue is observed in switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-226361 AOS-226850 AOS-227154	–	Mobility Conductors running AOS-W 8.7.1.5 or later versions incorrectly route traffic to different ports.	AOS-W 8.7.1.5
AOS-226455	–	The **show datapath netdest-id** command does not display any output. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-226547	–	A few APs are stuck in the **pre-validating status** state. This issue occurs when the **ap convert pre-validate all-aps** command is executed. This issue is observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-226548	–	Some managed devices running AOS-W 8.5.0.11 or later versions select an incorrect next hop list after a reboot. This issue occurs when two uplinks are configured.	AOS-W 8.5.0.11
AOS-226858	–	Some managed devices running AOS-W 8.7.1.5 or later versions display incorrect timestamp for the NTP server. However, the Mobility Conductor displays the correct timestamp.	AOS-W 8.7.1.5
AOS-226880	–	The LLDP process returns incorrect value for **lldpLocSysName**. This issue occurs due to memory corruption. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227005 AOS-229010	–	A few APs running AOS-W 8.7.1.5 or later versions crash unexpectedly. The log file list the reason for the event as **PC is at ieee80211_parse_wnm_mbo_ subelem+0x54/0x238 [umac]**.	AOS-W 8.7.1.5
AOS-227016 AOS-229420	–	Some users experience a delay while downloading the VIA VPN profile. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227076 AOS-226143	–	AppRF fails to classify traffic for a few applications. This issue is observed in stand-alone switches running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-227094	–	Heartbeats were missed and ping latency is also observed on managed devices running AOS-W 8.7.1.4 or later versions. This issue occurs after a cluster split.	AOS-W 8.7.1.4

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-227258	–	The **Dashboard > Overview** page of the WebUI displays the status of 2.4 GHz radio even when 2.4 GHz radio was disabled in the rf dot11g-radio-profile. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227324	–	The **ofc_cli_agent** process crashes on Mobility Conductors running AOS-W 8.6.0.13 or later versions. This issue occurs when the **show openflow-controlller ports** command is executed.	AOS-W 8.6.0.13
AOS-227454	–	Users are unable to connect to IKEv1 authenticated VIA. This issue occurs when **isakmd** process is stuck is busy state. This issue is observed in OAW-4750XM switches running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7
AOS-227542	–	Some Mobility Conductors running AOS-W 8.7.1.4 or later versions display the error message, **topology [6772]: <310310> <6772> <ERRS> |topology| |ofc-topology| max port limit(current:8750, max:8750) reached, rejecting new.**	AOS-W 8.7.1.4
AOS-227557	–	Some managed devices running AOS-W 8.7.1.5 or later versions in a cluster setup incorrectly use the IP address of the Mobility Conductor as the NAS IP address. This issue occurs after a cluster live upgrade.	AOS-W 8.7.1.5
AOS-227719	–	The **Dashboard > Infrastructure** page of the WebUI displays an incorrect **UPTIME** of the Mobility Conductor. This issue occurs when the Mobility Conductor has been UP for more than a year. This issue is observed in Mobility Conductors running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-227916	–	Mobility Conductors running AOS-W 8.7.1.4 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Nanny rebooted machine - low on free memory due to OFC flow_manager leak**.	AOS-W 8.7.1.4
AOS-227966	–	A few 7010, 7024, OAW-4450, and OAW-4850 switches running AOS-W 8.0.0.0 or later versions respond with its own MAC address to ARP requests sent for the management interface.	AOS-W 8.7.1.6
AOS-227981	–	A few 7010, 7024, OAW-4450, and OAW-4850 switches running AOS-W 8.0.0.0 or later versions incorrectly route the incoming external subnet traffic on management port to data ports.	AOS-W 8.7.1.6
AOS-227986	–	A few 7010, 7024, OAW-4450, and OAW-4850 switches managed devices running AOS-W 8.7.1.6 or later versions incorrectly route traffic out of data ports.	AOS-W 8.7.1.6

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-228164	–	Some APs running AOS-W 8.7.1.5 or later versions are unable to resolve DNS IP address for Aeroscout server.	AOS-W 8.7.1.5
AOS-228187	–	The packet capture icon in the **Dashboard > Infrastructure > Access Devices** page of the WebUI does not change its color to green while enabling packet capture. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-228245	–	The packet capture option in the **Dashboard >Infrastructure > Access Devices** page of the WebUI does not allow users to select a channel for packet capture for 6 GHz radio band. However, CLI allows users to specify a channel for packet capture. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-228356	–	The **detect-wireless-hosted-network** and **protect-wireless-hosted-network** parameters of the **ids unauthorized-device-profile** command does not work as expected in stand-alone switches running AOS-W 8.6.0.13 or later versions.	AOS-W 8.6.0.13
AOS-228375	–	Some OAW-AP515 access points running AOS-W 8.6.0.15 or later versions crash unexpectedly. The log files list the reason for the event as **esp_ output+0x3e8/0x588/LR:tun_net_xmit+0x5e8/0xb60**.	AOS-W 8.6.0.15
AOS-228429	–	A few clients are unable to obtain the correct role from the ClearPass Policy Manager. This issue is observed in Mobility Conductors running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-228475	–	Users are unable to drag and re-order server rules. This issue is observed in Mobility Conductors running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-228571	–	High flash memory utilization is observed on Mobility Controller Virtual Appliances running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-228671	–	SNMP walk fails with an error message, **Error: OID not increasing** for sysExtNSwitchRole, sysExtNSwitchName, and sysExtNSwitchSerNo. This issue is observed in Mobility Conductors running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.1.4
AOS-228714	–	APs located in different geographical locations are incorrectly present in the same AirMatch partition. This issue occurs when interferers with same MAC address is present at different geographical locations. This issue is observed in APs running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-228757	–	The **show wms rogue-ap list** command does not display the list of all rogue APs, This issue is observed in Mobility Conductors running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-228785	–	Captive portal authentication in bridge mode does not work as expected for APs in mesh mode. This issue is observed in managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-228886	–	Users are unable create a backup of the running configuration through TFTP server. This issue is observed in stand-alone switches running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-228934	–	SNMP walk returns the internal temperature value as **INVALID** for 9012 switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-229049 AOS-230190	–	The **Maintenance > Software Management** page of the parent node hierarchy displays the list of all individual switches instead of clusters and hence, users are unable to upgrade multiple clusters. This issue is observed in Mobility Conductors running AOS-W 8.8.0.2 or later versions.	AOS-W 8.8.0.2
AOS-229097	–	The **auth** process crashes on managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-229114	–	Some OAW-4750XM switches running AOS-W 8.6.0.10 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2)**	AOS-W 8.6.0.10
AOS-229205	–	A few OAW-AP515 access points running AOS-W 8.6.0.15 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot reason: SomeCrash Warm-reset**.	AOS-W 8.6.0.15
AOS-229206	–	The output of the **show ap debug radio-stats ap-name** command incorrectly displays **0** for **Avail TX Buffers**. This issue is observed in Mobility Conductors running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-229319	–	Some clients in decrypt-tunnel mode were deautheticated and sapcp ageout is also observed in management frames. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-229894	–	A few APs in Air Monitor mode display an incorrect encryption mode. This issue is observed in APs running AOS-W 8.9.0.1 or later versions.	AOS-W 8.9.0.1

Table 7: *Known Issues in AOS-W 8.9.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-230242	–	The **Configuration > WLANs** page of the WebUI does not display the list of available WLANs. This issue is observed in Mobility Conductors running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-230538	–	A few OAW-AP555 access points running AOS-W 8.7.1.4 or later versions fail to generate coredump.	AOS-W 8.7.1.4
AOS-230730	–	The **BLE** process crashes and hence, Zigbee devices get disconnected from the network. This issue is observed in stand-alone switch running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-229690	–	The output of the **show ucc** command does not display a few column titles. This issue is observed in Mobility Conductors running AOS-W 8.7.0.0. or later versions.	AOS-W 8.7.0.0

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*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Conductor, or two versions lower. For example multiversion is supported if a Mobility Conductor is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.5.0.0, AOS-W 8.4.0.0, or AOS-W 8.3.0.0.

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 inis 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 the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 36 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 36 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 36 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Low Free Flash Memory

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

Prerequisites

Before you proceed with the freeing up the flash memory:

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

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

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

Freeing up Flash Memory

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

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

   Table 8: *Flash Memory Requirements*

Upgrading from	Upgrading to	Minimum Required Free Flash Memory Before Initiating an Upgrade
8.3.x	8.9.x	360 MB
8.5.x	8.9.x	360 MB
8.6.x	8.9.x	570 MB
8.7.x	8.9.x	570 MB
8.8.x	8.9.x	450 MB
8.9.x	8.9.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        : ArubaOS 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        : ArubaOS 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 32.

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.

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 36 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the AOS-W image version.

3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 36 for information on creating a backup.

Downgrading AOS-W

A Mobility Conductor or managed device has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the Mobility Conductor or managed device from the other partition.

Pre-requisites

Before you reboot the Mobility Conductor or managed device with the pre-upgrade AOS-W version, perform the following steps:

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 36.
2. Verify that the control plane security is disabled.
3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

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

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot Controller after upgrade**.

d. Click **Upgrade**.

3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, and click **Reboot**.

The Mobility Conductor or managed device reboots after the countdown period.

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

In the CLI

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

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

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

or

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

2. Set the Mobility Conductor or managed device to boot with your pre-upgrade configuration file.

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

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

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

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

4. Set the backup system partition as the new boot partition.

```
(host) # boot system partition 1
```

5. Reboot the Mobility Conductor or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Conductor or managed device is using the correct AOS-W version.

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with IP addresses and interface numbers.
- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information.