

AOS-W 8.10.0.4 Release Notes



Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

<https://www.al-enterprise.com/en/legal/trademarks-copyright>

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2022)

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	3
Revision History	4
Release Overview	5
Important	5
Related Documents	5
Supported Browsers	5
Terminology Change	6
Contacting Support	6
What's New in AOS-W 8.10.0.4	7
Supported Platforms in AOS-W 8.10.0.4	8
Mobility Conductor Platforms	8
OmniAccess Mobility Controller Platforms	8
AP Platforms	8
End-of-Support	11
Regulatory Updates in AOS-W 8.10.0.4	12
Resolved Issues in AOS-W 8.10.0.4	13
Known Issues in AOS-W 8.10.0.4	14
Limitations	14
Known Issues	15
Upgrade Procedure	23
Important Points to Remember	23
Memory Requirements	24
Low Free Flash Memory	24
Backing up Critical Data	27
Upgrading AOS-W	28
Verifying the AOS-W Upgrade	29
Downgrading AOS-W	30
Before Calling Technical Support	32

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.

This AOS-W release notes includes the following topics:

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

Important

- As mandated by the Wi-Fi Alliance, AOS-W 8.10.0.x requires Hash-to-Element (H2E) for 6 Ghz WPA3-SAE connections. H2E is supported only on Windows 11, Linux wpa_supplicant version 2.10 and later versions. Hence, users must upgrade their Windows and Linux software for successful 6 Ghz WPA3-SAE connections.
- To align with the Inclusive Terminology Initiative, the factory-default APs running AOS-W 8.9.0.0 or later versions use **aruba-conductor** as the host name instead of **aruba-master** to identify a target managed device or standalone switch during DNS discovery.

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

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

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

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 3: *Supported Mobility Conductor Platforms*

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

OmniAccess Mobility Controller Platforms

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

Table 4: *Supported OmniAccess Mobility Controller Platforms*

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

AP Platforms

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

Table 5: *Supported AP Platforms*

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

Table 5: Supported AP Platforms

AP Family	AP Model
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H, AP-303HR
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
370EX Series	AP-375EX, AP-377EX, AP-375ATEX
OAW-AP387	OAW-AP387
500 Series	OAW-AP504, OAW-AP505
500H Series	AP-503H, AP-503HR, AP-505H, AP-505HR
510 Series	OAW-AP514, OAW-AP515, AP-518
518 Series	AP-518
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555

Table 5: *Supported AP Platforms*

AP Family	AP Model
560 Series	AP-565, AP-567
570 Series	AP-574, AP-575, AP-577
580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX
630 Series	AP-635
650 Series	AP-655

This chapter provides information on the Alcatel-Lucent products that are not supported for a particular release. The following AP models will no longer be supported beginning with the next major release, AOS-W 8.11.0.0 and higher:

- 200 Series
- OAW-AP203H Series
- OAW-AP203R Series
- OAW-AP205H Series
- OAW-AP207 Series
- 210 Series
- 220 Series
- OAW-AP228 Series
- 270 Series
- 320 Series
- 330 Series
- OAW-AP340 Series
- OAW-AP387

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_84965

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.10.0.4*

New Bug ID	Description	Reported Version
AOS-231326	Some managed devices running AOS-W 8.6.0.18 or later versions crashed and rebooted unexpectedly. The log files listed the reason for this event as Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2) . This issue occurred due to socket buffer corruption. The fix ensures that the managed devices work as expected. Duplicates: AOS-231256, AOS-233583, AOS-233673, AOS-237753, AOS-237985, and AOS-231372	AOS-W 8.6.0.18

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

Limitations

Following are the limitations observed in this release.

IP Default-Gateway Management Address

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

650 Series and 630 Series Access Points

The 650 Series and 630 Series access points have the following limitations:

- No Wi-Fi uplink on the 6 GHz radio channel
- No spectrum analysis on any radio
- No Zero-Wait DFS
- No Hotspot and AirSlice support on the 6 GHz radio
- No 802.11mc responder and initiator functionality on any radio
- Only 4 VAPs on the 6 GHz radio instead of 16
- Maximum of 512 associated clients on any radio, instead of 1024

6 GHz Channel Information in Regulatory Domain Profile

AOS-W does not display the 6 GHz channel information in the existing regulatory domain profile of Wi-Fi 6E APs by default.

To include 6 GHz channel information, ensure that you change the country code to a different country code, apply the change, and then revert it to the original country code. Another option is to create a new regulatory domain profile that includes the 6 GHz channel information by default, or copy the existing regulatory domain profile into a new regulatory domain profile to save the configuration.

The following example configures a regulatory domain profile and specifies a valid 6 GHz band.

```
host) [mynode] (config) #ap regulatory-domain-profile reg-635
host) [mynode] (Regulatory Domain profile "reg-635") #country-code US
host) [mynode] (Regulatory Domain profile "reg-635") #valid-6ghz-channel 165
```

AirSlice

AirSlice is disabled for 500 Series and 510 Series access points and enabled for 530 Series, 550 Series, and 630 Series access points.

OAW-40xx Series and OAW-4x50 Series controllers

The `cpboot` command does not upgrade the AOS-W software version of OAW-40xx Series and OAW-4x50 Series controllers.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.10.0.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the <code>show datapath uplink</code> 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-156537	–	Multicast streaming fails when broadcast and multicast optimization is enabled on the user VLAN. This issue is observed in managed devices running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-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-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 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.5.0.2
AOS-205650 AOS-231536	–	DHCP traffic from relay agent is not forwarded through the next-hop list configured in Layer 3 GRE tunnel. This issue is observed in managed devices running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15

Table 7: Known Issues in AOS-W 8.10.0.4

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209580	–	The output of the show ap database command does not display the o or i flags, which indicate whether an AP is an outdoor AP or an indoor AP. This issue occurs when the AP installation type is not set to default. This issue is observed in Mobility Conductors running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-215090 AOS-232617 AOS-232618 AOS-234348	–	The Dashboard > Overview page of the WebUI incorrectly displays different colors for Clients graph. This issue is observed in Mobility Conductors running AOS-W 8.9.0.2 or later versions.	AOS-W 8.9.0.2
AOS-215495	–	Some APs display the error message, ARM Channel 40 Physical_Error_Rate 0 MAC_Error_Rate 84 Frame_Retry_Rate 0 arm_error_rate_threshold 70 arm_error_rate_wait_time 90 . This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
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 switch IP address in a VPNC deployment.	AOS-W 8.5.0.11
AOS-216874 AOS-230298	–	The virtual MAC address of a VLAN gets deleted from the bridge table and hence, results in a network outage. This issue is observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-217628	–	Some managed devices running AOS-W 8.5.0.11 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, Reboot Cause: Kernel Panic (Intent:cause:register 12:86:f0:2) fib6_clean_node . Duplicates: AOS-226513, AOS-226753, AOS-221178, AOS-226575, and AOS-227666	AOS-W 8.5.0.11
AOS-218844 AOS-227400 AOS-231009	–	Some APs fail to preload image during cluster live upgrade. This issue is observed in APs running AOS-W 8.6.0.9 or later versions in a cluster setup.	AOS-W 8.6.0.9
AOS-219150	–	The Mobility Conductor fails to push the SRC NAT pool configuration to the managed devices. This issue occurs when the ESI redirect ACL is configured using the WebUI. This issue is observed in Mobility Conductors running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-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

Table 7: Known Issues in AOS-W 8.10.0.4

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219791	–	The aggressive scanning mode under ARM profile settings is enabled by default. This issue is observed in APs running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-221308	–	The execute-cli command does not work as expected for a few show commands. This issue is observed in Mobility Conductors running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-225263 AOS-232589	–	L2 database synchronization fails on standby switches. This issue is observed in stand-alone switches running AOS-W 8.8.0.1 or later versions.	AOS-W 8.8.0.1
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-226017 AOS-231886 AOS-235947	–	The airmatch_recv process crashes on Mobility Conductors running AOS-W 8.6.0.9 or later versions. The log files list the reason for the event as Exceeded max number of packet limit .	AOS-W 8.6.0.9
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-226773	–	The MAC ACLs do not work as expected when OpenFlow is enabled. This issue is observed in managed devices running AOS-W 8.6.0.11 or later versions in a cluster setup.	AOS-W 8.6.0.11
AOS-226800 AOS-229670	–	The name of the cluster profile changes after a reboot. Hence, the managed devices are unable to form a cluster. This issue is observed in OAW-4450 switches running AOS-W 8.5.0.13 or later versions in a cluster setup.	AOS-W 8.5.0.13
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-228581	–	A VPNC crashes and reboots unexpectedly. The log files list the reason for the event as Reboot Cause: Datapath timeout (SOS Assert) (in ipsec_decrypt) . This issue occurs when the buffer memory is queued in the wrong processor. This issue is observed in VPNCs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-228996	–	The amon_sender process crashes on managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5

Table 7: Known Issues in AOS-W 8.10.0.4

New Bug ID	Old Bug ID	Description	Reported Version
AOS-229024	–	Some OAW-AP505 access points running AOS-W 8.7.1.5 or later versions crashes and reboots unexpectedly. The log files list the reason for the event as PC is at wlc_mbo_parse_ie+0x15c/0x2b0 [wl_v6] .	AOS-W 8.7.1.5
AOS-230900 AOS-231081 AOS-234940	–	Some 530 Series and 550 Series access points running AOS-W 8.6.0.0 or later versions crash and reboot unexpectedly. The log file list the reason for reboot as Reboot caused by kernel panic: Take care of the TARGET ASSERT first.	AOS-W 8.7.1.7
AOS-231178	–	The stm process crashes on managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.7
AOS-231225	–	A few clients are unable to connect to APs running AOS-W 8.7.1.4 or later versions. The log files in the output of the show ap remote debug mgmt-frames ap-name <ap-name> command list the reason for the event as Disassociated due to insufficient resources at AP.	AOS-W 8.7.1.4
AOS-231233	–	Users are unable to upgrade APs using the FTP server. Also, the TFTP server is selected automatically to upgrade the APs. This issue is observed in managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-231283	–	The log files of few Wi-Fi 6E APs (630 Series and 650 Series access points) running AOS-W 8.10.0.0 or later versions incorrectly display the 6G radio 2 disabled due to mfg configuration message during reboot of the APs, even though the 6 GHz radio is not disabled when the APs boot up.	AOS-W 8.10.0.0
AOS-231326	–	Some OAW-4750XM switches running AOS-W 8.7.1.6 or later versions crash and reboot unexpectedly. The log files list the reason for the reboot as Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2) . Duplicates: AOS-231256, AOS-233583, AOS-233673, and AOS-231372	AOS-W 8.7.1.6
AOS-231649	–	Users with read-only access are able to enable configurations and view passwords configured for WLANs. This issue is observed in Mobility Conductors running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-231990	–	The Dashboard > Infrastructure page displays an incorrect Last Reboot time. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.8

Table 7: Known Issues in AOS-W 8.10.0.4

New Bug ID	Old Bug ID	Description	Reported Version
AOS-232311	–	The user table does not list the entries of L3 connected clients and hence, clients are unable to pass traffic. Also, the netdestination configuration is not synchronized between authmgr and sapm processes. This issue is observed when ValidUser ACL is configured for bridge mode clients. This issue is observed in stand-alone switches running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-232348 AOS-235259 AOS-237006	–	The stm process crashes on OAW-AP325 access points running AOS-W 8.7.1.7 or later versions.	AOS-W 8.7.1.7
AOS-232378	–	The pim process crashes on managed devices running AOS-W 8.7.1.8 or later versions. This issue occurs due to invalid memory access.	AOS-W 8.7.1.8
AOS-232443	–	Server derivation rules are not assigned correctly and an error message, Missing server in attribute list is displayed. This issue occurs when there is a delay in response from the RADIUS server. This issue is observed in stand-alone switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-232493	–	The entries of denylisted clients are not synchronized between the managed devices. This issue is observed in managed devices running AOS-W 8.6.0.15 or later versions in a cluster setup.	AOS-W 8.6.0.15
AOS-232620	–	A discrepancy is observed between the total number of APs and the total number of AP BLE devices reported. This issue is observed in stand-alone switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.8.0.2
AOS-232775	–	The session timeout returned post captive portal authentication from a RADIUS server is not honored. This issue occurs when both IPv4 and IPv6 addresses are associated to a single user connected in split tunnel forwarding mode and when the idle timeout value is lesser than session timeout value. This issue is observed in managed devices running AOS-W 8.9.0.2 or later versions.	AOS-W 8.9.0.2
AOS-232928	–	Some stand-alone switches running AOS-W 8.7.1.9 or later versions display the error messages, KASan: use after free in wlc_pcb_fn_find+0xc8/0x160 [wl_v6] at addr fffffc034931b08 and KASan: out of bounds access in wlc_pcb_fn_find+0xc8/0x160 [wl_v6] at addr . Duplicates: AOS-233808, AOS-234781, and AOS-236854	AOS-W 8.7.1.9
AOS-232991	–	Users are unable to issue the lc-cluster exclude-vlan command and an error message, ERROR: Invalid character is displayed. This issue is observed in Mobility Conductors running AOS-W 8.7.1.7 or later versions.	AOS-W 8.7.1.7

Table 7: Known Issues in AOS-W 8.10.0.4

New Bug ID	Old Bug ID	Description	Reported Version
		Workaround: Issue the no lc-cluster exclude-list command and then add the list of VLANs to be excluded.	
AOS-232997	–	Some managed devices running AOS-W 8.7.1.9 or later versions are stuck after an upgrade and the aaa process crashes.	AOS-W 8.7.1.9
AOS-233768	–	A few APs do not update the channel, bandwidth, and EIRP when the configuration is modified in radio profiles in the absence of a virtual AP. This issue is observed in APs running AOS-W 8.2.0.0 or later versions.	AOS-W 8.9.0.3
AOS-234103	–	Some clients experience downstream packet disruption. This issue is observed in APs running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.17
AOS-234282	–	Syslog messages generated for bridge mode clients do not include the details of SSID profiles. However, syslog messages generated for tunnel mode clients include the details of SSID profiles. This issue is observed in managed devices running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-234315	–	A few APs sent PAPI messages to external IP addresses, and the log displayed a random IP address for the PAPI_Send failed error message. This issue is observed in APs running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-234523	–	SSL protocol configurations are automatically altered for random managed devices without user initiating the changes. This issue is observed in Mobility Conductors running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-234730	–	Some AP-635 access points running AOS-W 8.9.0.3 or later versions crashes and reboots unexpectedly. The log files list the reason for the event as kernel panic: Take care of the TARGET ASSERT first (wal_soc_dev_hw.c:711 Assertion !((panic_mask & WHAL_UMCMN_TQM1_ASSERT_INT_MASK).	AOS-W 8.9.0.3
AOS-234819 AOS-235085	–	Some OAW-RAPs running AOS-W 8.6.0.9 or later versions do not broadcast BSSIDs and are stuck in AM mode. Workaround: Reload the managed device or re-configure the DRT file using the ap regulatory activate <drt_file_name> command,	AOS-W 8.6.0.9
AOS -235002	–	WPA3-AES-CCM-128 encryption is incorrectly displayed as WPA2 AES in the WebUI. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1

Table 7: Known Issues in AOS-W 8.10.0.4

New Bug ID	Old Bug ID	Description	Reported Version
AOS-235063	–	An error message, Invalid data: Static FW CP ACL cannot be deleted is displayed when users try to delete the custom ACL. This issue is observed in managed devices running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-235220	–	The Maintenance > Software Management page of the WebUI does not display the entire list of clusters. This issue occurs when the cluster name or hostname is changed. This issue is observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-235401	–	Some managed devices running AOS-W 8.6.0.17 or later versions do not send the outer IP IPV6 address to OmniVista 3600 Air Manager.	AOS-W 8.6.0.17
AOS-235628	–	AP related RF neighbor and RAPIDS list information are not sent to OmniVista 3600 Air Manager. This issue is observed in stand-alone controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-235647	–	Some OAW-4750XM switches running AOS-W 8.7.1.9 or later versions crash unexpectedly. The log files list the reason for the event as Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:2) .	AOS-W 8.7.1.9
AOS-235681 AOS-235719 AOS-236481 AOS-237063	–	The Dashboard > Infrastructure > Access Devices page of the WebUI does not display the correct status of APs that are down. However, CLI displays the correct number of APs that are down. This issue is observed in Mobility Conductors running AOS-W 8.10.0.0 or later versions.	AOS-W 8.7.1.9
AOS-235810	–	Configuration changes to the SAP MTU value is not displayed correctly. This issue occurs when the storage format of the MTU configuration is changed and when the file is not read correctly. This issue is observed in managed devices running AOS-W 8.9.0.2 or later versions.	AOS-W 8.9.0.2
AOS-235891	–	Standalone switches running AOS-W 8.7.1.9 or later versions displayed continuous PAPI_Send errors. This issue occurred because IP address of the AP is not available for wired clients at UCC and the error message is seen when UCC attempts to send messages through PAPI to AP with zero IP.	AOS-W 8.7.1.9
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 8.10.0.4

New Bug ID	Old Bug ID	Description	Reported Version
AOS-236462	–	A few OAW-RAPs go down unexpectedly. This issue occurs when the IPv6 address of the AP is changed. This issue is observed in OAW-RAPs running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-236534 AOS-236773	–	Some switches running AOS-W 8.10.0.2 show an error undefined while selecting a AAA profile using the WebUI.	AOS-W 8.10.0.2
AOS-236621	–	Some OAW-4850 switches running AOS-W 8.10.0.2 or later versions crash unexpectedly. The log files list the reason for the crash as Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20)	AOS-W 8.10.0.2
AOS-236813	–	Mobility Conductors running AOS-W 8.10.0.2 or later versions generate multiple log messages, switch_daemon.0x204c03b68f82[8050]: <310322> <8050> [switch.10.143.242.6:58000] ofc-switch-manager Unknown message type 12.	AOS-W 8.10.0.2

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 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 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: [upgradelImageNew.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 flashback.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: flashback.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>  
<remote directory>
```

```
(host) #copy flash: flashback.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: flashback.tar.gz
```

```
(host) #copy usb: partition <partition-number> <filename> flash: flashback.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 occurs 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:



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.