

# AOS-W 8.9.0.0 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. (2021)

## **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.

---

<b>Contents</b> .....	<b>3</b>
<b>Revision History</b> .....	<b>5</b>
<b>Release Overview</b> .....	<b>6</b>
Related Documents .....	6
Supported Browsers .....	6
Guidelines Before Upgrading 7000 Series Controllers to AOS-W 8.9.0.0 .....	7
Terminology Change .....	7
<b>Contacting Support</b> .....	<b>7</b>
<b>New Features and Enhancements in AOS-W 8.9.0.0</b> .....	<b>9</b>
Configuring Default Gateway on OAW-4850 switches .....	9
Dashboard Monitoring .....	9
Displaying the Name for Assa Abloy Door Locks .....	9
Enhancement to Serial Data Transport Profiles .....	9
Exporting IDS Logs from WebUI .....	9
New IoT Generic Filtering options .....	9
Configuring Wireless Containment Deauth .....	9
Upgrade to Vendor QOSMOS Code .....	10
Mesh Support on Wi-Fi 6E Access Points .....	10
Support for Azure Southbound Action for BLE Devices .....	10
Support for UTB .....	10
Increase in Maximum Supported BLE and Zigbee TX Power Values .....	10
Support for 512 Clients on Wi-Fi 6E Access Points .....	10
Support for Air Slice on Wi-Fi 6E Access Points .....	10
Support for New Channel Representation on Wi-Fi 6E Access Points .....	10
Support for a New AP Platform .....	11
Support for Hotspot on Wi-Fi 6E Access Points .....	11
Support for Multiple BSSID on Wi-Fi 6E Access Points .....	11
Configuring 6 GHz Radio Band on AP-635 Access Points .....	11
Support for Wi-Fi 6E ARM .....	12
Support for Wi-Fi 6E AirMatch .....	12
Support for Wi-Fi 6E Air Management .....	12
Support for Wi-Fi 6E Air Management Activity Detection .....	12
Support for Wi-Fi 6E Air Management Information Element Parsing .....	12
Scanning Enhancements for Wi-Fi 6E Access Points .....	12
Support for 6 GHz Radio .....	12
Support Regulatory Domain Profile for 6 GHz Radio .....	12
Support for Client Match for 6 GHz Radio .....	12
Support for EN302502 and EN301893 in UNI3 Bands .....	13
Support for GCM Ciphers on OAW-AP555 Access Point .....	13
Support for Dropbear SSH .....	13
Client Match Support for 802.11v .....	13
Enhancements to Multicast Group Limit .....	13
Enabling TLS Method for an External Logging Server .....	13
Encrypt Private Key in the Flash .....	13
Enhancements to number of PVST+ instances .....	13

---

---

Increase in Number of Tunneled Networks in VIA .....	13
Upgrade Notification for a Cluster Upgrade .....	13
Additional Certificate for Meridian Beacon Management .....	14
Additional Certificate for Meridian Asset Tracking .....	14
<b>Supported Platforms in AOS-W 8.9.0.0 .....</b>	<b>15</b>
Mobility Conductor Platforms .....	15
OmniAccess Mobility Controller Platforms .....	15
AP Platforms .....	15
<b>Regulatory Updates in AOS-W 8.9.0.0 .....</b>	<b>17</b>
<b>Resolved Issues in AOS-W 8.9.0.0 .....</b>	<b>18</b>
<b>Known Issues in AOS-W 8.9.0.0 .....</b>	<b>31</b>
Limitation .....	31
Known Issues .....	31
<b>Upgrade Procedure .....</b>	<b>36</b>
Important Points to Remember .....	36
Memory Requirements .....	37
Low Free Flash Memory .....	37
Backing up Critical Data .....	41
Upgrading AOS-W .....	43
Verifying the AOS-W Upgrade .....	44
Downgrading AOS-W .....	46
Before Calling Technical Support .....	48

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 03	The AP-503H access points are added to the list of <b>Supported Platforms</b> .
Revision 02	This revision introduces the following changes: <ul style="list-style-type: none"><li>■ Added Additional Certificate for Meridian Beacon Management in New Features and Enhancements.</li><li>■ Added Additional Certificate for Meridian Asset Tracking in New Features and Enhancements.</li><li>■ Moved bug ID AOS-213507 from Known Issues to Resolved Issues.</li></ul>
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

### 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	<a href="https://www.al-enterprise.com">https://www.al-enterprise.com</a>
Support Site	<a href="https://myportal.al-enterprise.com">https://myportal.al-enterprise.com</a>
Email	<a href="mailto:ebg_global_supportcenter@al-enterprise.com">ebg_global_supportcenter@al-enterprise.com</a>
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



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

### Configuring Default Gateway on OAW-4850 switches

AOS-W supports configuring the default gateway for dedicated OOB management Ethernet port on OAW-4850 switches by using the **ip default-gateway mgmt <nexthop>** command.

### Dashboard Monitoring

A search option is introduced in the **Campus AP Allowlist** and **Remote AP Allowlist** tables of the **Configuration > Access Points > Allowlist** page in the WebUI.

### Displaying the Name for Assa Abloy Door Locks

The Assa Abloy door locks will now be displayed using a name in the output of the `show ap debug zigbee client-table` command. This enhancement is helpful in identifying and debugging issues related to a specific Assa Abloy door lock connected to the system.

### Enhancement to Serial Data Transport Profiles

A new CLI parameter **usbSerialDeviceTypeFilter <filter>** is added to the IoT transport profile configuration to allow users to filter serial data based on the USB dongle type.

### Exporting IDS Logs from WebUI

Starting from AOS-W8.9.0.0, a user has the option of exporting IDS logs as a CSV file from the WebUI.

### New IoT Generic Filtering options

The following generic filtering parameters are introduced in the IoT Transport Profile configuration:

- **usbSerialDeviceTypeFilter <filter>**
- **companyIdentifierFilter <filter>**
- **serviceUUIDFilter <filter>**
- **macOuiFilter <filter>**
- **localNameFilter <filter>**

### Configuring Wireless Containment Deauth

A new parameter **Wireless Containment Deauth** is introduced to enable users to set a unique reason code in the deauth frame. This unique reason code identifies if the deauths are originating from the WIPs solution.

## Upgrade to Vendor QOSMOS Code

The vendor QOSMOS code is upgraded to ProtoBundle-1.530.1-25 for AOS-W 8.9.0.0 release.

## Mesh Support on Wi-Fi 6E Access Points

AOS-W provides support for mesh deployment and WPA3-SAE-AES opmode on Wi-Fi 6E access points.

## Support for Azure Southbound Action for BLE Devices

The Asynchronous Cloud to Device (C2D) messages are added to support Azure southbound action on BLE devices.

## Support for UTB

A new parameter **utb\_filter\_block** is introduced to control the band on which the Ultra Tri-Band (UTB) limitation is applied in the regulatory-domain-profile. The UTB filter supports channel band on both 5 GHz and 6 GHz in AOS-W 8.9.0.0 release.

## Increase in Maximum Supported BLE and Zigbee TX Power Values

The maximum configurable transmission (Tx) power rate in an IoT radio profile is increased to 20 dBm.

## Support for 512 Clients on Wi-Fi 6E Access Points

AOS-W supports 512 clients for each radio band on Wi-Fi 6E access points.

## Support for Air Slice on Wi-Fi 6E Access Points

AOS-W supports Air Slice on Wi-Fi 6E access points for 5 GHz radio band only.

## Support for New Channel Representation on Wi-Fi 6E Access Points

AOS-W represents the channels on 6 GHz band as four separate fields for Wi-Fi 6E access points. The four separate fields are as follows:

- **Pri-Channel**
- **Sec-Channel**
- **Band**
- **Bandwidth**

AOS-W also modifies the following AMON messages to include the four separate fields for each 6 GHz radio channel:

- RADIO\_STATS
- RADIO\_INFO
- AMON\_TAG

- UCM\_SESSION\_UPDATE
- SPEC\_DEV\_DETAILS
- AG\_SVC\_SESSION\_UPDATE

## Support for a New AP Platform

The Alcatel-Lucent 630 Series access points (AP-635) are high performance, tri-radio, indoor access points that can be deployed in either switch-based (AOS-W) or switch-less (OAW-IAP) network environments. These APs deliver high performance concurrent 2.4 GHz, 5 GHz, and 6 GHz 802.11ax Wi-Fi (Wi-Fi 6E) functionality with MIMO radios (2x2 in 2.4 GHz, 5 GHz, and 6 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services. Containment does not work on the 6 GHz radio when WPA3 with Management Frame Protection (MFP) is enabled.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point.
- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor.
- Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Thermal management.
- Support for OFDMA.

*For complete technical details and installation instructions, see Alcatel-Lucent 630 Series Access Points Installation Guide.*

## Support for Hotspot on Wi-Fi 6E Access Points

AOS-W supports Hotspot 2.0 on the 2.4 GHz and 5 GHz radio bands of Wi-Fi 6E access points.

## Support for Multiple BSSID on Wi-Fi 6E Access Points

AOS-W supports Multiple BSSID feature on Wi-Fi 6E access points. Multiple BSSID feature supports multiple virtual APs of a radio and advertises information for multiple BSSIDs by using a single beacon or probe response frame instead of multiple beacon or probe response frames, each corresponding to a single BSSID.

## Configuring 6 GHz Radio Band on AP-635 Access Points

Following are the guidelines to ensure a successful deployment of AP-635 access points by configuring the 6 GHz radio band:

- The virtual APs for 6 GHz radio band are disabled by default and must be enabled manually in the WLAN SSID settings of the virtual APs. To configure the WLAN SSID settings in the WebUI, navigate to **Configuration > System > Profiles** and select **Wireless LAN > Virtual AP** under **All Profiles** list, and enable the **Allow 6GHz Band** parameter. You can also enable the **allowed-band-6ghz** parameter in the **wlan virtual-ap <profile>** command.
- To allow the 6 GHz clients to connect to the 6 GHz WLAN SSID, Alcatel-Lucent recommends the following steps:

- a. Navigate to **Configuration > System > Profiles** and select **Wireless LAN > Virtual AP** under **All Profiles** list, and select **none** from the **Allowed band** drop-down list and enable the **Allow 6GHz Band** check box. You can also set the **allowed-band** parameter to **none** and enable the **allowed-band-6ghz** parameter in the **wlan virtual-ap <profile>** command.
- b. Create an alternate WLAN SSID virtual AP on 2.4 GHz and 5 GHz radio bands. Navigate to **Configuration > System > Profiles** and select **Wireless LAN > Virtual AP** under **All Profiles** list, and select **all** from the **Allowed Band** drop-down list, and disable the **Allow 6GHz Band** check box. You can also set the **allowed-band** parameter to **all** and **allowed-band-6ghz** parameter to **none** in the **wlan virtual-ap <profile>** command. This allows 6 GHz clients to locate 6 GHz APs through Reduced Neighbor Report (RNR) in 2.4 GHz and 5 GHz beacons.

For more information, refer to the *AOS-W 8.9.0.0 User Guide*.

## Support for Wi-Fi 6E ARM

AOS-W supports ARM on Wi-Fi 6E access points.

## Support for Wi-Fi 6E AirMatch

AOS-W supports AirMatch on Wi-Fi 6E access points.

## Support for Wi-Fi 6E Air Management

AOS-W supports Air Management on Wi-Fi 6E access points.

## Support for Wi-Fi 6E Air Management Activity Detection

AOS-W supports Wi-Fi 6E Air Management activity detection on 6 GHz channels.

## Support for Wi-Fi 6E Air Management Information Element Parsing

AOS-W supports Wi-Fi 6E Air Management information element parsing on 6 GHz channels.

## Scanning Enhancements for Wi-Fi 6E Access Points

Air Monitoring is enhanced to support scanning in the new Wi-Fi 6E AP-635 access points.

## Support for 6 GHz Radio

AOS-W supports configuration of the 6 GHz radio in the applicable access points. The 6 GHz radio can be configured in the RF management profile.

## Support Regulatory Domain Profile for 6 GHz Radio

AOS-W supports configuration of the regulatory domain profile for the 6 GHz radio.

## Support for Client Match for 6 GHz Radio

AOS-W supports configuration of the client match for the 6 GHz radio.

## Support for EN302502 and EN301893 in UNI3 Bands

The OAW-AP374 outdoor access point supports EN302502 and EN301893 for DFS in UNI3 bands. Support for EN302502 allows the usage of higher power in the UNI3 band in ETSI and support for EN301893 allows radar detection.

## Support for GCM Ciphers on OAW-AP555 Access Point

OAW-AP555 access point supports GCM ciphers.

## Support for Dropbear SSH

AOS-W supports Dropbear SSH version 2019.78.

## Client Match Support for 802.11v

The Client Match process sends only the fields that are relevant to it in the protobuf format and the AP station management process populates the rest of the message.

## Enhancements to Multicast Group Limit

Starting from AOS-W 8.9.0.0, the multicast group limit per managed device is increased from 8 to 32.

## Enabling TLS Method for an External Logging Server

Starting from AOS-W 8.9.0.0, a new sub-parameter is introduced to enable TLS method defined in RFC-5425. It can be used to secure log messages sent to an external logging server.

## Encrypt Private Key in the Flash

Starting from AOS-W, private key and passphrase are encrypted using TPM keys.

## Enhancements to number of PVST+ instances

AOS-W supports 128 PVST+ instances.

## Increase in Number of Tunneled Networks in VIA

Starting from AOS-W 8.9.0.0, VIA split tunnel network limit is increased to 256.

## Upgrade Notification for a Cluster Upgrade

Starting from AOS-W 8.9.0.0, the **Maintenance > Software Management** page in the **Managed Network** node hierarchy displays **RAPs are present, upgrade may take longer time** message when a cluster with OAW-RAPs are upgraded.

## Additional Certificate for Meridian Beacon Management

Meridian Beacon Management uses the following two additional certificates in AOS-W 8.9.0.0:

- Root CA: GTS Root R1
- Intermediate/Subordinate CA: GTS CA 1D4

These certificates are available from <https://pki.goog/repository/>. Install these certificates on the managed device.

## Additional Certificate for Meridian Asset Tracking

Meridian Asset Tracking uses an additional DigiCert Global Root CA in AOS-W 8.9.0.0. This certificate is available from <https://www.digicert.com/kb/digicert-root-certificates.htm>. Install this certificate on the managed device. This certificate has the following parameters:

- Valid until: 10-Nov-2031
- Serial number: 08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A
- SHA1 Fingerprint: A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36
- SHA256 Fingerprint:  
43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01  
:6

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-AP318
OAW-AP320 Series	OAW-AP-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



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 [myportal.al-enterprise.com](http://myportal.al-enterprise.com).

The following DRT file version is part of this release:

- DRT-1.0\_80922

This chapter describes the resolved issues in this release.

**Table 6:** *Resolved Issues in AOS-W 8.9.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200515 AOS-219987	—	The <b>DDS</b> process crashed on managed devices running AOS-W 8.3.0.10 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.10
AOS-209352	—	Some managed devices terminating VIA connection displayed the error message, <b>httpd[30106]: Reached session limit: 64</b> . The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-211545 AOS-217654	—	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as, <b>Reboot caused by kernel panic: Fatal exception in interrupt</b> . The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-212386	—	The <b>Configuration &gt; Licensing</b> tab of the WebUI did not display any data. The fix ensures that the WebUI displays the licensing details. This issue occurred when high availability was configured. This issue was observed in Mobility Conductors running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-212755	—	Some users connecting to OAW-AP505 access points running AOS-W 8.7.0.0 were unable to pass traffic intermittently. The fix ensures that clients are able to pass traffic.	AOS-W 8.7.0.0
AOS-213337	—	A few AP-325 access points running AOS-W 8.5.0.10 or later versions crashed unexpectedly. The log files list the reason for the event as <b>Reboot caused by kernel panic: Fatal exception in interrupt</b> . The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-213507	—	A managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as, <b>Reboot Cause: Soft Watchdog reset</b> . The fix ensures that the managed device works as expected. This issue was observed in a managed device running AOS-W 8.5.0.10 or later version.	AOS-W 8.5.0.10

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-214391 AOS-217130 AOS-217832	—	The STM process crashed on OAW-4750XMswitches. The fix ensures that the switches work as expected. This issue was observed in OAW-4750XMswitches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-214416	—	Some stand-alone switches running AOS-W 8.6.0.6 or later versions displayed the error message, <b>An internal system error has occurred at file main.c function rx_handler line 1517 error sxd_r_read_str_safe szFunctionName failed</b> . The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.6
AOS-214510 AOS-219139	—	A few clients were disconnected from the network. The log files listed the reason for the event as <b>Wlan driver excessive tx fail quick knockout</b> . The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-214846	—	The status of the APs was incorrectly displayed as down. The fix ensures that the Mobility Conductors display the correct status of APs. This issue was observed in Mobility Conductors running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-215669	—	Some managed devices running AOS-W 8.6.0.7 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)</b> . The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.7
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-216777	—	The Mobility Conductor was unable to recover. This issue was observed when the flash memory was 100% used in the Mobility Conductor. Once the flash space is increased as per SKU requirements, the Mobility Conductor recovers. This issue is observed in AOS-W 8.9.0.0 version.	AOS-W 8.9.0.0
AOS-215852	—	Mobility Conductors running AOS-W 8.6.0.6 or later versions log the error message, <b>ofa: 07765 ofproto INFO Aruba-SDN: 1 flow_mods 28 s ago (1 modifications)</b> . This issue occurs when openflow is enabled and when 35 seconds is configured as UCC session idle timeout.	AOS-W 8.6.0.6

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216145	—	Mobility Conductors running AOS-W 8.5.0.8 or later versions sent continuous DNS requests to the managed devices. This issue occurred when a folder that was not available on the /mm node was trying to get synchronized on the managed devices. The fix ensures that the Mobility Conductors do not send continuous DNS requests to the Managed Devices.	AOS-W 8.5.0.8
AOS-216536 AOS-220630	—	Some managed devices running AOS-W 8.5.0.11 or later versions were unable to come up on the Mobility Conductor. This issue occurred when the managed devices received the branch IP address as the switch IP address in a VPNC deployment. The fix ensures that the managed devices are able to come up on the Mobility Conductor.	AOS-W 8.5.0.11
AOS-217104 AOS-219159	—	The ESI redirect failed and traffic was forwarded to the default gateway. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-151022 AOS-188417	185176	The output of the <b>show datapath uplink</b> command displayed incorrect session count. The fix ensures that the the <b>show datapath uplink</b> command displays correct session count. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-193231 AOS-200101 AOS-207456	—	The <b>Dashboard &gt; Infrastructure &gt; Access Devices</b> page of the WebUI displayed an error message, <b>Error retrieving information</b> . The fix ensures that the WebUI displays the list of access devices. This issue was observed in Mobility Conductors running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-209093 AOS-210452	—	Some managed devices running AOS-W 8.7.0.0 or later versions generated multiple AMON receiver errors. The fix ensures that the managed devices work as expected.	AOS-W 8.7.0.0
AOS-210198	—	The <b>Dashboard &gt; Security &gt; Detected Radio</b> page of the WebUI displayed incorrect number of <b>Clients</b> . The fix ensures that the WebUI displays correct number of <b>Clients</b> . This issue was observed in Mobility Conductors running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-213011 AOS-219946	—	Packet loss was observed for a few clients during a cluster failover. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-214977 AOS-220420	—	Memory leak was observed in <b>arci-cli-helper</b> process. This issue occurred while running an API script. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-215303	—	Users were unable to view file names in the <b>Diagnostic &gt; Technical Support &gt; Copy Files</b> page of the WebUI. This issue occurred when <b>Flash file system</b> was selected as the source file. The fix ensures that users are able to view the file names in the <b>Diagnostic &gt; Technical Support &gt; Copy Files</b> page of the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-215498	—	Some OAW-AP535 access points running AOS-W 8.5.0.11 or later versions detected false radar. The fix ensures that the APs work as expected.	AOS-W 8.5.0.11
AOS-215712	—	Mobility Conductors running AOS-W 8.7.0.0 or later versions forwarded all syslog messages with severity level marked as debug. This issue occurred when CEF format was enabled on the Mobility Conductor. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.7.0.0
AOS-216512	—	The DHCP client / station related AMON message sent the mask, server IP address, and client IP address in a reverse order to the AirWave server. The fix ensures that the Mobility Conductors work as expected. This issue was observed in Mobility Conductors running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-216622	—	A few APs running AOS-W 8.7.0.0 or later versions incorrectly displayed the restricted flag, <b>p = Restriction mode in POE-AF/AT</b> in the AP database even if the Ethernet port was disabled. The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-216764	—	Users were not redirected to the captive portal page. The fix ensures that the captive portal works as expected. This issue was observed in managed devices running AOS-W 8.7.1.0 or later versions in a cluster setup.	AOS-W 8.7.1.0
AOS-216766	—	Some APs generated sapd coredump. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216874 AOS-219841	—	Some users were unable to access the network and a network outage was also observed. This issue occurred when the VRRP IP was removed from the datapath bridge table. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-216972	—	Some managed devices running AOS-W 8.6.0.7 or later versions forwarded data frames that are larger than the configured IPsec tunnel MTU value. The fix ensures that the managed devices do not forward data frames that are larger than the configured IPsec tunnel MTU value.	AOS-W 8.6.0.7
AOS-217106	—	The <b>no valid</b> parameter of the <b>ap regulatory-domain-profile</b> command did not work while creating a new regulatory profile. The fix ensures that the <b>no valid</b> parameter of the <b>ap regulatory-domain-profile</b> command works as expected. This issue was observed in controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.7
AOS-217807	—	Some OAW-RAPs took a long time to come up on a managed device. This issue occurred due to a delay in allowlist-db synchronization between the Mobility Conductor and managed devices and when external authentication was enabled for OAW-RAPs. The fix ensures that the OAW-RAPs do not take a long time to come up on a managed device. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions in a cluster setup.	AOS-W 8.6.0.5
AOS-218012	—	The <b>Maintenance</b> tab of the WebUI displayed a list of clusters that were not configured for that particular node. The fix ensures that the WebUI does not display clusters that are not configured for a particular node. This issue was observed in Mobility Conductors running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-218231 AOS-216177	—	Wireless users were unable to find a few wired clients. The fix ensures that the wireless users are able to find the wired clients. This issue was observed in controllers running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-218622	—	Some APs running AOS-W 8.6.0.6 or later versions crashed unexpectedly. The log files listed the reason for the event as <b>PC:aruba_wlc_ratesel_getcurrate+0x24/0xd0 [wl_v6] Warm-reset</b> . The fix ensures that the APs work as expected.	AOS-W 8.7.1.1

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218795	—	Downloadable user roles were not downloaded and hence, user roles were not assigned to the tunnel-node users. The fix ensures that the user roles are assigned to the tunnel-node users. This issue was observed in managed devices running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-218822	—	High flash memory utilization was observed in Mobility Conductors running AOS-W 8.5.0.10 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.5.0.10
AOS-219098 AOS-219914	—	Some devices were unable to connect to the network. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219098 AOS-219914	—	Some devices were unable to connect to the network. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219178	—	Clients connected to the anchor controller were unable to receive IP addresses. The fix ensures that the clients are able to receive IP addresses. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-219214	—	The valid user ACL was reordered in stand-alone controllers running AOS-W 8.6.0.8 or later versions. The fix ensures that the ACL is not reordered.	AOS-W 8.6.0.8
AOS-219328	—	SNMP configurations failed and the error message, <b>Error: User (itam_net) should be created before adding to the trap host</b> was displayed. This issue occurred when the SNMP server v3 trap host which had the engine-id same as the engine-id of the switch was removed and added again. The fix ensures that the SNMP configurations do not fail. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-219365	—	Some APs running AOS-W 8.7.0.0 or later versions rebooted sporadically. This issue occurred when the smart antenna feature was enabled. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219376	—	Some users were unable to add VIA server details if the domain name exceeded 32 characters. The fix ensures that the users are able to add VIA server details. This issue was observed in Mobility Conductors running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219384	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as <b>PC is at wlc_nar_dotxstatus+0x450</b> . The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219390	—	The <b>datapath</b> process crashed on stand-alone controllers running AOS-W 8.7.1.1 or later versions. The log files listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b> . This issue occurred when the op mode of the SSID profile was changed from WPA3-AES-CCM-128 to WPA3-CNSA. The fix ensures that the stand-alone controllers work as expected.	AOS-W 8.7.1.1
AOS-219627 AOS-218851	—	Clients were unable to connect to 2.4 GHz SSID of some APs. This issue occurred when the MAC address of the Radio 1 was incorrect. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219725	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as <b>PC is at wlc_nar_detach+0x8c</b> . The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219936	—	The stand-alone controller displayed the error message, <b>Module Profile Manager is busy. Please try later</b> while configuring netdestination. The fix ensures that the stand-alone controllers work as expected. This issue was observed in stand-alone controllers running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-219978 AOS-220568	—	A few iPhone 12 Pro users experienced poor upstream network performance. This issue occurred when APs operated in tunnel mode. The fix ensures optimal network performance. This issue was observed in APs running AOS-W 8.6.0.9 or later versions in tunnel mode.	AOS-W 8.7.1.2
AOS-220053	—	Some OAW-RAPs went down on managed devices running AOS-W 8.6.0.5 or later versions. This issue occurred after a failover. The fix ensures that the OAW-RAPs work as expected.	AOS-W 8.6.0.5
AOS-220108	—	The <b>OFA</b> process crashed on Mobility Conductor Virtual Appliances running AOS-W 8.6.0.6 or later versions. This issue occurred when the <b>show openflow debug ports</b> command was executed. The fix ensures that the Mobility Conductor Virtual Appliances work as expected.	AOS-W 8.6.0.6



**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220552	—	The <b>Configuration &gt; Services &gt; Clusters</b> page of the WebUI did not display the status of live upgrade. This issue occurred when the cluster profile name had blank spaces. The fix ensures that the WebUI displays the status of live upgrade. This issue was observed in Mobility Conductors running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-221005	—	Some stand-alone switches running AOS-W 8.7.1.2 or later versions were stuck in reboot loop. The log files listed the reason for the event as <b>Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)</b> . The fix ensures that the stand-alone switches work as expected.	AOS-W 8.7.1.2
AOS-221429	—	Downloadable user role was not applied correctly to the first user connecting in the split tunnel mode. The fix ensures that the downloadable user role are applied correctly. 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-221666 AOS-222708	—	Some OAW-RAPs running AOS-W 8.6.0.9 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as, <b>Kernel panic - not syncing</b> . The fix ensures that the OAW-RAPs work as expected.	AOS-W 8.6.0.9
AOS-224186	—	The <b>show tech-support</b> command did not display any information about the kernel crash and an error message, <b>No kernel crash information available</b> was displayed. The fix ensures that the <b>show tech support</b> command displays crash related information. 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-223839	—	The output of the <b>show ap active</b> command did not display any value for <b>Outer IP</b> . The fix ensures that the command displays the <b>Outer IP</b> value. This issue was observed in Mobility Conductors running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-223797	—	The <b>show ap remote auth-trace-buf</b> command did not display any output. The fix ensures that the command displays the output. 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-222931	—	Some APs did not form active tunnels with the AAC. The fix ensures that the APs form tunnels with the AAC. This issue was observed in managed devices running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222904	—	A few USB clients connected to an OAW-IAP became inactive when the OAW-IAP was rebooted. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-222771	—	Some managed devices running AOS-W 8.5.0.12 or later versions did not send SNMPv3 information to the OmniVista 3600 Air Manager server. The fix ensures that the managed devices send SNMPv3 information to the OmniVista 3600 Air Manager server.	AOS-W 8.5.0.12
AOS-222754	—	The SNMP walk to managed devices failed when the SNMP requests had the IPv6 address of the switch. This issue occurred when the primary managed device had VRRP IPv6 address configured. The fix ensures that the SNMP walk to managed devices do not fail. This issue was observed in managed devices running AOS-W 8.4.0.1 or later versions.	AOS-W 8.4.0.1
AOS-222540 AOS-224221	—	Some APs dropped EAPOL packets from the bridge mode wired port. The fix ensures that the APs do not drop the EAPOL packets. This issue was observed in APs running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-221938	—	Some users were unable to download the VIA profile and were redirected to an incorrect link. This issue occurred when users accessed VIA from a public network. The fix ensures that the users are able to download the VIA profile. This issue was observed in Mobility Conductors running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-221726 AOS-223220	—	Some managed devices running AOS-W 8.7.1.1 or later versions were unable to form L2 clusters with its peers. The fix ensures that the managed devices are able to form L2 clusters.	AOS-W 8.7.1.1
AOS-221478 AOS-221569 AOS-221572	—	The <b>auth</b> process crashed on managed devices running AOS-W 8.5.0.9 or later versions. This issue occurred when the <b>show auth-tracebuf mac</b> command was executed. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.9
AOS-221352	—	Some mesh links reported incorrect RSSI values. The fix ensures that the mesh links report correct RSSI values. This issue was observed in APs running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-221225	—	Some OAW-AP387 access points running AOS-W 8.7.1.1 or later versions rebooted unexpectedly. The log files listed the reason for the event as <b>Reboot caused by kernel panic: Fatal exception</b> . The fix ensures that the APs work as expected.	AOS-W 8.7.1.1

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-221222	—	Some APs came up with the <b>IDe</b> flag and the <b>show ap database</b> command displayed the <b>e</b> flag even when EST was not configured. This issue occurred when an external allowlist authentication was configured on the managed devices and also when CPsec enabled APs were brought up on the managed devices. The fix ensures that the APs work as expected. This issue was observed in managed devices running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-221144	—	ARP packets were not forwarded to the uplink switch when bcmc-optimization was enabled on the switches. This issue was observed in Mobility Conductors and managed devices running AOS-W 8.5.0.9 or later versions. The fix ensures that the Mobility Conductors and managed devices work as expected.	AOS-W 8.5.0.9
AOS-221018 AOS-220919	—	Some users were unable to connect to SSIDs. This issue occurred in 802.11r and MultiZone enabled configurations. 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-220903	—	The <b>s</b> flag indicating LACP striping was not displayed in the output of the <b>show ap database long</b> command even when LLDP was enabled on two uplinks. The fix ensures that the <b>show ap database long</b> command displays the <b>s</b> flag when LLDP is enabled. This issue is observed in APs running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-220704	—	Some APs were incorrectly displayed under different clusters. The fix ensures that the APs are not displayed under different clusters. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-224336	—	The IoT transport profile authentication failed. This issue occurred when a remote server was used. The fix ensures successful authentication. This issue was observed in Mobility Conductors running AOS-W 8.8.0.1 or later versions.	AOS-W 8.8.0.1
AOS-223656	—	Some OAW-RAPs are unable to come up on managed devices after a reboot. The fix ensures that the OAW-RAPs are able to come up on the 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-221093 AOS-222773	—	Mobility Conductors running AOS-W 8.0.1.0 or later versions took a long time to process templates that were sent to the managed devices. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.0.1.0

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222776	—	Some managed devices running AOS-W 8.0.1.0 or later versions established IPsec tunnels with stale WAN IP addresses. The fix ensures that the managed devices work as expected.	AOS-W 8.0.1.0
AOS-220515	—	Some managed devices running AOS-W 8.5.0.12, or later versions displayed the error message, <b>[fpapps] filling up the default gateway configuration</b> . The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.12
AOS-220398	—	A few clients in bridge mode were unable to connect to wpa2-psk SSIDs. The fix ensures that the clients in bridge mode are able to connect to wpa2-psk SSIDs. This issue was observed in stand-alone controllers running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-220251	—	Some users experienced connectivity issues. This issue occurs when APs did not respond to the authentication frames in MultiZone networks that had non-cluster zones and dot11r enabled Virtual APs. The fix ensures that the APs work as expected. This issue was observed in stand-alone controllers running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-220179	—	A few clients were unable to complete the SAE handshake. This issue occurred when the password of an SSID profile was modified to a length greater than the existing password. The fix ensures that the SAE handshake is not interrupted. This issue was observed in APs running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-218328 AOS-220026 AOS-223535	—	VRRP flapping was observed on managed devices running AOS-W 8.6.0.4 or later versions and hence, clients faced connectivity issues. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.4
AOS-219803	—	XML query done on a non-existing user resulted in an invalid response. The fix ensures that the switch responds as expected. This issue was observed in Controllers running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-219769	—	The <b>rap-gre-mtu</b> parameter of the <b>ap system-profile</b> command did not work as expected. The fix ensures that the <b>rap-gre-mtu</b> parameter works as expected. This issue was observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-219385	—	Some APs took a long time to come up on the backup data center after primary data center failover. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219112	—	UBT clients hopped between VLANs. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-218661	—	The <b>AP</b> process crashed on managed devices running AOS-W 8.7.1.1 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.1
AOS-218646	—	Some users connected to OAW-AP515 access points running AOS-W 8.6.0.7 or later versions experienced degraded audio quality. The fix ensures that the clients do not experience degraded audio quality.	AOS-W 8.6.0.7
AOS-218642	—	Some users were unable to access the internet. This issue occurred when client entries were not removed by the managed devices even when CoA disconnect was triggered for the clients. The fix ensures that the clients are able to access the internet as expected. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-218488 AOS-219694	—	The management VLAN address of the Mobility Conductor was pointed to the Remote AP tunnel. The fix ensures that the management VLAN address is not available in the Remote AP tunnel. This issue was observed in Mobility Conductors running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-219806	—	Some APs running AOS-W 8.8.0.0 or later versions did not have the support for H2E advertisement. The fix ensures that the APs support H2E advertisement in beacon and probe responses.	AOS-W 8.8.0.0
AOS-218322	—	Some managed devices running AOS-W 8.5.0.5 or later versions did not send SSID related information during data collection. The fix ensures that the managed devices send SSID related information during data collection.	AOS-W 8.5.0.5
AOS-214428 AOS-218277	—	The <b>auth</b> process crashed on managed devices running AOS-W 8.5.0.11 or later versions. Hence, the Remote APs rebooted and VIA users faced connectivity issues. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.11
AOS-216152 AOS-218208 AOS-222478	—	Some clients were unable to connect to APs. The log file listed the reason for the event as, <b>AP is resource constrained</b> . The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8

**Table 6: Resolved Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218162	—	The wired Ethernet port did not form GRE tunnel with the managed device. The fix ensures that the wired Ethernet port forms GRE tunnel with the managed device. This issue was observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-218117 AOS-219179 AOS-224575	—	The <b>show ntp servers</b> and <b>show ntp status</b> commands displayed the error message, <b>Address family for hostname not supported</b> . However, the WebUI displayed the NTP servers. The fix ensures that the commands do not display the error message. This issue was observed in managed devices running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7
AOS-217890	—	A managed device running AOS-W 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b> . The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10
AOS-217741	—	Mobility Conductors experienced timeout and did not send SNMP response to the AirWave server. The fix ensures that the Mobility Conductors work as expected. This issue was observed in Mobility Conductors running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-217678 AOS-218131	—	Some APs running AOS-W 8.6.0.7 or later versions did not honor the user alias route src-nat ACL and tunnelled the traffic to managed devices. The issue occurred when a netdestination alias is configured in the ACL. The fix ensures that the APs work as expected.	AOS-W 8.6.0.7
AOS-217539 AOS-219010 AOS-219952 AOS-220918 AOS-221298	—	The <b>auth</b> process crashed in managed devices running AOS-W 8.7.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.7.0.0

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 8.9.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218844	—	Mobility Conductor picks only 43% of the APs for cluster CRU. This issue is observed in Mobility Conductor running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-219249	—	The VLAN configuration as part of <b>conductorip</b> or <b>conductoripv6</b> command is not pushed from the Mobility Conductor to a managed device after the zero touch provisioning process. This issue is observed on a managed device running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-222200	—	Mobility Conductors running AOS-W 8.7.0.0 or later versions are unable to classify webrtc traffic. This issue is observed during conference calls.	AOS-W 8.9.0.0

**Table 7: Known Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-223354	—	Some stand-alone switches running in AOS-W 8.9.0.0 display the error message, <b>Error upgrading image: Basic image verification failed on Ancillary Image</b> during the upgrade. <b>Workaround:</b> Issue the <b>show storage</b> command to ensure that the switch has enough flash storage.	AOS-W 8.9.0.0
AOS-223199	—	OpenFlow connection flaps between Mobility Conductor and managed devices. This issue occurs when the IPSec tunnel MTU is set to a value lesser than 1500. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-223012	—	Datapath categorization does not work as expected for Skype4B calls. This issue occurs in OAW-RAPs operating in split-tunnel mode. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-223807	—	The <b>inet_frag_secret_rebuild: hashfn (ffffffffc17679b8/ip6_hashfn)</b> kernel debug messages are observed on OAW-4850 controllers running AOS-W 8.8.0.2. This issue occurs during upgrade of the OAW-4850 controllers.	AOS-W 8.8.0.2
AOS-224042	—	A few APs experience packet drop when clients roam between the APs. This issue is observed in APs running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-224867	—	An rsync failure occurs on a managed device. This issue occurs during boot when the <b>DHCP</b> process wrongly derives the switch IP as IP address of the Mobility Conductor. The IP address of the Mobility Conductor is subsequently configured as a FQDN in configuration. This issue is observed in a managed device running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-222699 AOS-223281 AOS-223640	—	A few Intel AX210 clients face connectivity issue while connecting to AP-635 access points operating in 6 GHz band. This issue occurs when an existing non-Tx VAP is changed to Tx VAP. This issue is observed in AP-635 access points running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-222662	—	Both WebUI and CLI display incorrect logging severity. The output of the <b>show logging server</b> command displays <b>All</b> as logging severity and the <b>Syslog Servers</b> table in the <b>Configuration &gt; System &gt; Logging</b> page displays the severity as <b>Warning</b> . This issue occurs only when logging severity is not configured. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0.	AOS-W 8.9.0.0



**Table 7: Known Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222661	—	The <b>Syslog Servers</b> table in the <b>Configuration &gt; System &gt; Logging</b> page of the WebUI does not display the port number. This issue occurs when port numbers are not configured. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-222660	—	The <b>show logging server</b> command does not display the status of <b>BSD</b> as enabled even if the TLS option is enabled. This issue is observed in Mobility Conductors running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-221676	—	When Intel AX210 client is connected to TX VAP in 6GHz radio of [[[Undefined variable Variables.635AP Series]]], it shows 70% or more ping drops and keeps getting disconnected with reason "Wlan driver wireless client out of range (seq num 0)". This is an existing Intel driver side issue and known to occur in version 22.70.x.x or lower if used with AX210 chipsets.	AOS-W 8.9.0.0
AOS-220557	—	Some Intel AX clients face connectivity issues. This issue is observed in AOS-W version 8.7.1.3 or later versions in [[[Undefined variable Variables.635AP Series]]], OAW-AP555, OAW-AP535.	AOS-W 8.9.0.0
AOS-220125	—	The <b>Datapath</b> process crashes on Mobility Conductors running AOS-W 8.9.0.0. This issue occurs when the packet size is larger than the configured IPsec tunnel MTU value.	AOS-W 8.9.0.0
AOS-219048	—	When Service AP is configured with PSK SSID, AP brings up the switch and configures Provision AP as WIFI-Uplink profile. The Service AP becomes unstable in the switch. The AP's uplink is disconnected, resulting in loss of connection with the controller. This issue is observed in OAW-AP335.	AOS-W 8.9.0.0
AOS-218578	—	In a dual stack setup, when there is a scheduled upgrade in MM, the upgrade fails consistently. This issue is observed in switchesMM-MD and Controller Build is AOS-W70xx_8.8.0.0_79405.	AOS-W 8.9.0.0
AOS-218219	—	A Microsoft Teams call with an external client does not get classified and prioritized.. This MS-Teams call is not classified and prioritized by UCC. This issue is observed in AOS-W 8.8.0.0 or later versions.	AOS-W 8.9.0.0
AOS-215989	—	Some APs running AOS-W 8.8.0.0 or later versions experience low throughput. This issue occurs when the number of VAPs is increased. This issue occurs when HE MU-OFDMA parameters are enabled. This affects only HE MU-OFDMA capable client devices.	AOS-W 8.9.0.0

**Table 7: Known Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213428	—	The <b>Upgrademgr</b> process does not provide FQDN support for image servers. This issue is observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-213345	—	The output of the <b>show ap image-preload status &lt;summary/all/list&gt;</b> command does not display the list of APs. This issue is observed in managed devices in a cluster setup running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-212858	—	The <b>Maintenance &gt; Software Management &gt; Upload AOS image for controller</b> page of the WebUI does not allow users to delete multiple images simultaneously. This issue is observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-212847	—	The <b>Maintenance &gt; Software Management &gt; Upload AOS image for controller</b> page of the WebUI does not allow users to upload multiple images simultaneously. This issue is observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-212288	—	The status of the managed devices are displayed as <b>UKN</b> after an L2 fail over. This issue is observed in Mobility Conductors and managed devices running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-211655	—	Some clients are unable to roam between APs when co-ex is enabled. This issue is observed in OAW-AP514 access points running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-213157	—	A Mobility Conductor fails to perform version check of managed devices during the image upgrade process. This issue is observed in Mobility Conductors in a cluster setup running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-212941	—	The newly configured VLANs are not displayed when the <b>show vlan</b> command is executed. This issue occurs after a flash backup restore. This issue is observed in managed devices running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-211634	—	The <b>Controller</b> field is not updated in the <b>Dashboard&gt; Services</b> page of the WebUI. This issue occurs when a cluster-failover happens during an ongoing Microsoft Teams call. This issue is observed in managed device running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-211453	—	Microsoft Teams conference call is not supported. This issue is observed in managed devices running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0

**Table 7: Known Issues in AOS-W 8.9.0.0**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210383	—	The <b>Cluster Members</b> pop-up window in the <b>Dashboard &gt; Infrastructure &gt; Clusters</b> page of the WebUI does not display any value for <b>Hostname</b> , <b>Role</b> , and <b>Reachable</b> fields. This issue occurs when the user configures IPv6 cluster in the WebUI. This issue is observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.8.0.0
AOS-208640 AOS-215865 AOS-219181	—	A few high efficiency clients experience poor performance with OAW-AP505 access points running AOS-W 8.7.1.0 or later versions. This issue occurs when <b>HE MU-OFDMA</b> parameters are enabled.	AOS-W 8.7.1.0
AOS-202352 AOS-202531	—	After a live upgrade is initiated, users are unable to stop the upgrade as the <b>Cancel</b> button in the <b>Maintenance &gt; Software Management &gt; Controllers and Clusters</b> page of the WebUI does not work. This issue is observed managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-222554 AOS-222612	—	WPA3-AES-CCM-128 authentication fails for a few clients. This issue occurs in APs operating in 6 GHz channels. This issue is observed in APs running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-211070	—	Cluster live upgrade fails and the WebUI displays an error message, <b>Controller &lt;IP address &gt; is down</b> . This issue occurs when an IPv6 enabled managed device establishes an IPv4 connection with the Mobility Conductor. This issue is observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-223903	—	A Mobility Conductor does not accept applying a valid XML file that is generated in Python for IPv6 relay-option and IPv4 option 82. The Mobility Conductor displays the <b>Filename &lt;sample.xml&gt; has invalid keywords</b> error. This issue is observed in a Mobility Conductor running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-221963	—	When a policy has both WebCC and AppRF rules, the OmniAccess Mobility Controller classifies all traffic as ssl, https or http2. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-225201	—	The scheduled upgrade information of cluster and managed device is not displayed in the WebUI and CLI. This issue is observed in Mobility Conductor running AOS-W 8.9.0.0.	AOS-W 8.9.0.0

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 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 41](#) 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 41](#) 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 41](#) 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 to AOS-W 8.9.0.0:

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: [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 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: <tftp> <filename> flash: flashbackup.tar.gz
```

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

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

```
(host) #restore flash
```

Please wait while we restore the flash backup.....

Flash restored successfully.

Please reload (reboot) the controller for the new files to take effect.

# Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.



---

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see [Memory Requirements on page 37](#).

---



---

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message is displayed 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.



---

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 41](#) 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 41](#) 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 41](#).
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.