AOS-W 8.11.0.0 Release Notes

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

Contents

Chapter 1
Revision History

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

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 2
Release Overview

This AOS-W release notes includes the following topics:

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

Related Documents

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

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

Supported Browsers

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

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

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

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

New Features and Enhancements in AOS-W 8.11.0.0

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

Short Supported Release

AOS-W 8.11.0.0 is a Short Supported Release (SSR).

Support for OAW-AP610 Series OAW-AP Platforms

The Alcatel-Lucent OAW-AP610 Series access points (OAW-AP615) are high performance, dual-radio, tri-band indoor access points that can be deployed in either switch-based (AOS-W) or switch-less (Alcatel-Lucent AOS-W Instant) network environments. These APs deliver high performance 2.4 GHz, 5 GHz, and 6 GHz 802.11ax Wi-Fi (Wi-Fi 6E) functionality with dual radios (2x2 in 2.4 GHz, 5 GHz, and 6 GHz), with the ability to operate these radios on any two out of three bands simultaneously. Additionally, these APs deliver capacity with OFDMA (Orthogonal Frequency Division Multiple Access) technologies while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor.
- One Ethernet port, ENET0, capable of data rates up to 2.5 Gbps.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on the Ethernet port.
- High power BLE
- Mesh
- Thermal management

OAW-AP615 access points operate in 2.4 GHz and 5 GHz radio bands by default. To enable the AP to broadcast on 6 GHz radio band, set the flexible dual band radio mode to either **5 GHz and 6 GHz** or **2.4 GHz and 6 GHz** mode

For complete technical details and installation instructions, see *Alcatel-Lucent* OAW-AP610 Series *Access Points Installation Guide*.

AirMatch Support for OAW-AP610 Series Access Points

AirMatch provides support for dynamic selection of the opmode, in addition to assigning channel and EIRP to the current opmode in OAW-AP610 Series access points (OAW-AP615). AirMatch selects the opmode dynamically depending on the RF coverage for each radio band–2.4 GHz, 5 GHz and 6 GHz.

BLE Daemon Support for Per-AP Calibrated RSSI Tables

Starting from this release, APs with Gen-2 BLE/IoT radios will adjust the calibrated RSSI values for iBeacon advertisements when BLE transmit power levels are modified using the ble-txpower setting in the IoT Radio Profile configuration. The calibrated values can then be verified using the **show ap debug ble-advertisement-info** command.

Changes to the Default Setting for Max Clients in an SSID Profile

AOS-W now supports a maximum of 1024 wireless clients per radio. The maximum number of clients can be configured using the **max-client** parameter of the **wlan ssid-profile** command.

Cipher Suites in Web Server Configuration

The **cipher-suite** parameter is introduced to replace **ciphers** parameter. This feature allows users to select specific ciphers from the supported list of ciphers. Cipher suites are streamlined in such a way that only strong cipher suites are enabled by default. This is compatible with the FIPS mode as well. As a part of this enhancement, users are given the option to selectively enable and disable the remaining cipher suits while configuring the web server profile.

Concurrent VIA VPN Sessions Limit

The maximum number of concurrent VIA VPN session per user is restricted. The admin is enabled to configure a value between 1-32 to restrict the concurrent VIA VPN sessions per user.

Configuring the Default Gateway on the OOB Management Port

AOS-W 8.11.0.0 supports configuring the default gateway for dedicated OOB management Ethernet port on 7000 Series switches by using the **ip default-gateway mgmt <nexthop>** command.

Default ARP Rate Set for Global Firewall Parameter - ARP Attack

Starting from this release, the default value for global firewall parameter **Monitor/Police ARP Attack (non Gratuitous ARP) rate (per 30 seconds)** is set to 100.

Enable or Disable BLE Periodic Telemetry

The BLE Telemetry setting can now be enabled or disabled in the AOS-W webUI. A new parameter **blePeriodicTelemetryDisable** is introduced in the iot transportProfile command to disable periodic telemetry reporting.

Enabling Fast Initial Link Setup (FILS) for an AP in 6 GHz Only Mode

AOS-W 8.11.0.0 now supports an AP in a 6GHz only mode. If 2.4GHz and 5GHz VAPs are unavailable, then FILS will be automatically enabled for the 6GHz VAPs configured on the AP allowing the 6GHz clients to obtain the SSID information by FILS. When 2.4GHz and 5GHz VAPs are available again, FILS will be automatically disabled allowing the 6GHz clients to obtain the SSID information over the Reduced Neighbor Report (RNR) in the 5 GHz or 2.4 GHz beacons.

Enhancement to the wlsxWlanStationTable MIB

As an enhancement, a new wlanStaApName MIB object is added to the wlsxWlanStationTable MIB to simplify the correlation of APs and Stations.

Flex Dual Band Support for OAW-AP615 Access Points

AOS-W 8.11.0.0 now supports dual band support on Alcatel-Lucent OAW-AP615 that provides flexibility for the radios of OAW-AP615 to operate on different radio bands. The OAW-AP615 access points do not support tri-radio mode or split 5 GHz mode. For example, radio 0 can operate on 2.4 GHz or 5 GHz band and radio 1 can work on 2.4 GHz or 6 GHz band. OAW-AP615 access points operate in 2.4 GHz and 5 GHz radio bands by default. To enable the AP to broadcast on 6 GHz radio band, set the flexible dual band radio mode to either **5 GHz and 6 GHz** or **2.4 GHz and 6 GHz** mode.

The following command enables the flex dual band support for an AP on stand-alone switches.

```
(host) [mynode] (AP system profile "default") #flex-dual
```

The following command enables the flex dual band support for an AP in a Mobility Conductor-Managed Device topology.

```
(host) [mynode] (AP system profile "default") #flex-dual-mode
```

The following command provides the status of the flex dual band support for an AP.

```
(host) [mynode] #show ap active
```

Grouping AirGroup Servers based on the Username

AirGroup, with enforce registration enabled, allows the 802.1X authenticated users to view the list of all servers that share the same username. Users need not add any CPPM policy to view the list of servers that share the same username.

The following CLI command enables enforce registration in the AirGroup profile:

```
(host) [md] (config) #airgroupprofile <profile-name> enforce-registration
```

The output of the **show airgroup servers** and **show airgroup cppm entries** commands display the **D** flag to indicate that the servers share the same username.

Username-based policy entries are automatically added for servers with username and no CPPM policy. This policy is displayed in the output of the **show airgroup cppm entries** command along with the **D** flag.

The **show airgroup servers username <username>** command also displays the list of servers that have the same username.

Improvements to Health Messages Reported during IoT Transport

The health messages sent during IoT transport have been updated to include more information on the health statuses of the devices.

- Radio health message now includes information about the Up or Down status of the radio mode, BLE mode or Zigbee Mode etc.
- USB health message now reports as healthy, only if the dongle is up-and-running. The USB device includes USB Nordic APB and Serial-Data USB device such as Enocean device.
- AP health message will now include the AP layer's metrics status which are related to reporting data.

IoT Audit Trail

The **show ap debug iot-audit-trail** command is introduced to display all the action commands executed in the CLI and report the Southbound API messages received from the server.

IPM Radio Power Reduction Steps

Starting from AOS-W 8.11.0.0, the IPM radio power reduction steps use radio indices (0,1, and 2) to refer to the radios that are restricted. Prior to AOS-W 8.11.0.0, the IPM radio power reduction steps referred to the operating bands of the radio. This enhancement removes the association between the power reduction steps and the operating bands to simplify the IPM feature design. The association between the radio index and the operating band is displayed in the output of the **show ap active** command.

Mesh Support for OAW-AP615 Access Points

AOS-W 8.11.0.0 now extends mesh support for OAW-AP615 access points. In the mesh cluster profile, the a, g, 6GHz, and all mesh bands will allow the mesh nodes to operate on 5 GHz, 2.4GHz, 6GHz, and all radio bands. The mesh link and Wi-Fi uplink features continue to operate on the band configured in the AP system profile. When the radio modes are changed, the mesh and wifi uplink modules will restart and resume on the radio defined in the existing configuration. If the provisioned rf-mesh band is not available on the flex-dual band, it will let the AP use the **all** rf-mesh band all to instead of the rf band you configured. It means that if the rf band configuration is not in the flex-dual mode, it will let the AP open all the mesh radios to connect. For example, when the rf-mesh band is **g** and the flex-band is **5GHz-and-6GHz**, the rf-mesh band will automatically change to **all** and radio 0 will operate on 5 GHz and radio 1 will operate on 6 GHz radio bands.

Modifications to CLI Commands

The **write erase all, halt, and reload** commands can be issued only from the **/mm/mynode** and **/mm** nodes of the Mobility Conductor.

Modifications to CLI command Parameters

The **active-client-rebalance-threshold**, **standby-client-rebalance-threshold**, and **unbalance-threshold** parameters of the **lc-cluster group-profile** command are not supported from AOS-W 8.11.0.0.

No Support for WEP Configuration in Wi-Fi Uplink Profile

AOS-W no longer supports WEP parameters for configuring Wi-Fi uplink profile. The following parameters have been removed from Wi-Fi uplink profile:

- Static WEP
- WEP Key 1
- WEP Key 2
- WEP Key 3
- WEP Key 4
- WEP Transmit Key Index

OOB 6 GHz Scanning for OAW-AP615

AOS-W allows users to configure OOB 6 GHz scanning settings for OAW-AP615 access points. The **oob-switch** parameter is introduced in the regulatory domain profile to enable and disable OOB 6 GHz scanning for OAW-AP615 access points. Disabling **oob-switch**, disables 6 GHz scanning and it is applicable only when OAW-AP615 access points are in the 5GHz-and-2.4GHz operation mode.

Opmode-transition Support for WPA3

AOS-W allows users to disable the **opmode-transition** parameter for virtual APs to be deployed on 6 GHz bands using MFP.

Organizational Unit (OU) as an Optional Parameter

Organizational Unit (OU) is no longer a mandatory parameter for VIA Domain Name profiles. This is because the OU parameter is now deprecated by various certificate authorities. Hence, **OU** is an optional parameter under **Add New** window of **Configuration** > **Authentication** > **L3 Authentication** > **VIA Connection** > **default** > **VIA Domain Name Profiles** in the WebUI. In the CLI, the **OU** parameter is optional under the following command.

```
(host) [mynode] (config) #aaa authentication via connection-profile > dn-profile
```

RTS Frame Transmission to the Clients

AOS-W allows users to control RTS frame transmission to the clients. The **rf dot11a-radio-profile, rf dot11g-radio-profile, rf dot11a-secondary-radio-profile,** and **rf dot11-6GHz-radio-profile** commands allow users to enable or disable RTS mode based on their network requirement.

Support of 1024 clients on 2G and 5G Bands

AOS-W 8.11.0.0 now supports 1024 clients on the 2G and 5G bands of an OAW-AP655.

Support for Active Client Rebalance Threshold Feature

Starting with AOS-W 8.11.0.0, the Active client rebalance threshold feature is not supported and can no longer be configured using the AOS-W WebUI or CLI.

Support for All Flags in the AP Database

AOS-W now includes all available flags associated with an AP in the **show ap database flags <flags>** command.

Support for Bucket Based Client Load Balancing

AOS-W 8.11.0.0 now supports the bucket based client load balancing feature that distributes the buckets based on the platform capacity in a cluster. In bucket based client load balancing, the cluster manager intermittently checks for the proportionate distribution of the bucketmap among the cluster nodes, and if required, re-balances 8 buckets of one ESSID in one iteration. The periodicity of rebalancing of the buckets among the cluster nodes is at every 20 seconds.

The following CLI command displays the current bucket distribution for all the ESSIDs.

```
(host) [mynode] #show lc-cluster bucket distribution all
```

The following CLI command displays the current bucket distribution for a specific ESSID.

```
(host) [mynode] #show lc-cluster bucket distribution essid
```

The following CLI command displays the details of the bucketmap publish counters.

```
(host) [mynode] #show lc-cluster bucketmap publish counters
```

The following CLI command clears the details of the bucketmap publish counters.

```
(host) [mynode] #clear lc-cluster bucketmap publish counters
```

Support for CentOS 7.9 and Ubuntu 20.04

AOS-W 8.11.0.0 now supports deploying a Mobility Controller Virtual Appliance or a Mobility Conductor Virtual Appliance using CentOS 7.9 or Ubuntu 20.04 KVM Hypervisor.

Support for Ethernet 0 as Downlink Port

Starting from AOS-W 8.11.0.0, Ethernet Port 0 can be assigned as the downlink port if Ethernet Port 1 is configured or running as the primary uplink on OAW-AP318, OAW-AP374, OAW-AP375, OAW-AP375ATEX, OAW-AP377, OAW-AP584, OAW-AP585, OAW-AP585EX, OAW-AP587, and OAW-AP587EX.

Support for Hyper-V Version Windows Server 2019

AOS-W 8.11.0.0 now supports deploying a Mobility Controller Virtual Appliance or a Mobility Conductor Virtual Appliance using Hyper-V Version Windows Server 2019.

Support for Multiple Long-Lasting Connections with Nordic Chip Radio

Starting from this release, AOS-W Instant supports concurrent scanning and bleConnect connections to the IoT devices. A maximum of ten concurrent connections can be established. This function is currently supported only on OAW-IAPs with nordic radios –OAW-AP500 Series, OAW-AP510 Series, OAW-AP530 Series, OAW-AP550 Series, OAW-AP560 Series, OAW-AP570 Series, OAW-AP610 Series, and OAW-AP630 Series access points, along with an external USB dongle.

Support for New ABB Sensors

The following two new ABB sensors are supported by AOS-W APs. Listed below are details on how to identify the sensor type and and work out the sensor identifier from the advertisement packets:

- **DFU Target Device**–The DFU target is the device that runs the DFU having at least one active DFU transport. It can be the bootloader in DFU mode, or an application with DFU running in the background. To be able to perform an update using the AP the sensor must be discovered when it enters the bootloader mode.
  - **Sensor Identifier**–The DFU target device sensor is recognized by service class UUID : **0xFE59**. This service UUID needs to be configured under **Filters** in the IoT transport profile.

    The following procedure describes how to configure DFU Target Device on an AP:

    1. When configuring the IoT transport profile, ensure that the **Server Type** is either set to **Telemetry Https**, **Telemetry Websocket**, or **Azure IoT Hub**.
    2. Under **Filters**, click **Company Identifier**, and the click **+**.
    3. Enter the sensor identifier **FE59** in the text box and click **Ok**.

The following CLI command is used to configure DFU Target Device on an AP:

```
(AOS-W AP)[Mode]# iot transportProfile example
```

```
(AOS-W AP)(IoT Transport Profile "example")# companyIdentifierFilter FE59
```

- **SALT Star Vario**—The SALT Star Vario sensor is recognized by local name : **perma**. When the local name is parsed to the OAW-IAP, the identity of the sensor is assigned as SALT + MAC Address. For example, if device's MAC address is 00:80:25:FB:1A:73, then its identity is SALT008036FB1A73. This sensor identifier can be configured under **Filters** in the IoT transport profile.

  The following procedure desccribes how to configure SALT Star Vario on an AP:

  1. When configuring the IoT transport profile, ensure that the **Server Type** is either set to **Telemetry Https**, **Telemetry Websocket**, or **Azure IoT Hub**.
  2. Under **Filters**, click **Local Name**, and the click **+**.
  3. Enter the sensor identifier **Perma** in the text box and click **Ok**.

  The following CLI command is used to configure SALT Star Vario on an AP:

```
(AOS-W AP)(Config)# iot transportProfile example
(AOS-W AP)(IoT Transport Profile "example")# localNameFilter perma
```

  For more information, see *Configuring an IoT Transport Profile* in the *AOS-W 8.11.0.0 User Guide*.

Support for Packet Debugging Functionality on APs

AOS-W introduces the following two commands that support packet debugging functionality to troubleshoot the data packets through the AP datapath:

- **ap remote-debug-pkt**
- **show ap remote-debug-pkt**

Support for UNII-4 Channels

AOS-W supports UNII-4 (channels 169-177) on OAW-AP530 Series, OAW-AP550 Series, OAW-AP630 Series, and OAW-AP650 Series access points.

Support to Enable Frame Bursting

AOS-W allows users to control frame bursting even if there is only one active client associated to the AP. Users can enable or disable frame bursting using the **rf dot11a-radio-profile frame-bursting-mode** , **rf dot11-6Ghz-radio-profile frame-bursting-mode, rf dot11a-secondary-radio-profile frame-bursting-mode,** and **rf dot11g-radio-profile frame-bursting-mode** commands.

Vendor Specific IE based Containment

AOS-W allows to configure exclusions for IDS containment based on vendor specific IE information. This feature allows APs to be exempted from containment even when the devices use randomized MAC addresses. To exempt APs from containment, users should configure the vendor OUI and OUI type in the IDS unauthorized device profile. A maximum of five vendor OUI and OUI types can be defined for confinement exclusion.

VLAN Derivation Support to Clients using Split-Tunnel Forwarding Mode

VLAN derivation support is extended to wired and wireless clients using split-tunnel forwarding mode along with tunnel, bridge and decrypt-tunnel modes.

Wi-Fi Uplink Support for OAW-AP610 Series Access Points

AOS-W supports Wi-Fi uplink feature on OAW-AP610 Series access points for 2.4 GHz, 5 GHz, and 6 GHz radio bands.

Zero-Wait DFS Support for OAW-AP650 Series Access Points

AOS-W supports zero-wait DFS feature on the OAW-AP650 Series access points for 5 GHz radio band.

Behavioral Changes

This release does not introduce any changes in AOS-W behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.11.0.0.

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 3: *Supported Mobility Conductor Platforms*

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

OmniAccess Mobility Controller Platforms

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

Table 4: *Supported OmniAccess Mobility Controller Platforms*

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

AP Platforms

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

Table 5: *Supported AP Platforms*

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

Table 5: *Supported AP Platforms*

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

Deprecated APs

The following APs are no longer supported from AOS-W 8.11.0.0 onwards.

Table 6: *Deprecated AP Platforms*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP

Table 6: *Deprecated AP Platforms*

AP Family	AP Model
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-AP320 Series	OAW-AP324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP387	OAW-AP387

Chapter 5
Regulatory Updates in AOS-W 8.11.0.0

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_85075

Chapter 6
Resolved Issues in AOS-W 8.11.0.0

This chapter describes the resolved issues in this release.

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-156537	Multicast streaming failed when broadcast and multicast optimization was enabled on the user VLAN. The fix ensures that the multicast streaming works as expected. This issue was observed in managed devices running AOS-W 8.7.1.4 or later versions. **Old Bug ID:** 192751	AOS-W 8.7.1.4
AOS-205192	The channels configured using the **Configuration > System > Profiles > All Profiles > AP > Regulatory Domain** profile page of the WebUI did not take effect. The fix ensures that the channel configured using WebUI takes effect and works as expected. This issue was observed in Mobility Conductors running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-209580	The output of the **show ap database** command did not display the **o** or **i** flags, which indicate whether an AP is an outdoor AP or an indoor AP. This issue occurred when the AP installation type was not set to default. The fix ensures that the command display the **o** or **i** flags. This issue was observed in Mobility Conductors running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-215090	The **Dashboard > Overview** page of the WebUI incorrectly displayed different colors for **Clients** graph. The fix ensures that the WebUI displays correct details. This issue was observed in Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.2
AOS-216942 AOS-237622 AOS-237621	Some OAW-AP535 access points running AOS-W 8.7.1.10 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.10
AOS-218219	A Microsoft Teams call with an external client did not get classified and prioritized by UCC. The fix ensures that managed devices work as expected. This issue was observed in managed devices running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-218844 AOS-222351 AOS-227400 AOS-231009	A Mobility Conductor picked only 43% of the APs for cluster CRU. The fix ensures that the Mobility Conductor works as expected. This issue was observed in Mobility Conductors running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-219150	Mobility Conductor failed to push the SRC NAT pool configuration to the managed devices. This issue occurred when the ESI redirect ACL was configured using the WebUI. The fix ensures that the Mobility Conductor pushes the SRC NAT pool configuration to the managed devices. This issue was observed in Mobility Conductors running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-219791	The aggressive scanning mode under ARM profile settings was enabled by default. The fix ensures that the aggressive scanning mode is only enabled at the time of booting. As soon as aggressive scanning is complete, the preferred mode of scanning is moderate scanning mode. The moderate scanning mode triggers a scan every five seconds while the aggressive scanning mode triggers a scan every second, when clients are not connected to the radio. This prevents the scanning from interfering with roaming. This issue was observed in APs running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-220837	Some OAW-4850 switches running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic [panic (fmt=0xffffffffc190db38 "Aiee, killing interrupt handler!")]**. The fix ensures that the OAW-4850 switches work as expected.	AOS-W 8.3.0.0
AOS-221308	The **execute-cli** command did not work as expected for a few show commands. The fix ensures that the command works as expected. This issue was observed in Mobility Conductors running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-221643	Some stand-alone switches running AOS-W 8.4.0.0 or later versions failed to send the client login and logout details of captive portal authentication to the Palo Alto Firewall. The fix ensures that the switches send the client details to the Palo Alto Firewall.	AOS-W 8.7.1.3
AOS-224523 AOS-224762	The **logging source-interface** command did not work as expected. The fix ensures that the command works as expected. This issue was observed in stand-alone switches running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-225263	L2 database synchronization failed on standby switches. The fix ensures that L2 database synchronization does not fail. This issue was observed in stand-alone switches running AOS-W 8.8.0.1 or later versions.	AOS-W 8.8.0.1
AOS-226017 AOS-231886 AOS-235947	The **airmatch_recv** process crashed on Mobility Conductors running AOS-W 8.6.0.9 or later versions. The log files listed the reason for the event as **Exceeded max number of packet limit**. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.6.0.9
AOS-226548	Some managed devices running AOS-W 8.5.0.11 or later versions selected an incorrect next hop list after a reboot. This issue occurred when two uplinks were configured. The fix ensures that the managed devices select the correct nexthop list.	AOS-W 8.5.0.11
AOS-226773	The MAC ACLs did not work as expected when OpenFlow was enabled. The fix ensures that the MAC ACLs work as expected. This issue was 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-226851 AOS-227319 AOS-228483	The IPsec map in the route table of the managed device had an incorrect IP address of the Mobility Conductor. This issue occurred when the managed device had been up for more than 180 hours. The fix ensures that the correct IP address of the Mobility Conductor is available in the IPsec map. This issue was observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.7.1.5

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-227981	A few OAW-4010, OAW-4024, OAW-4450, and OAW-4850 controllers running AOS-W 8.7.1.6 or later versions incorrectly routed the incoming external subnet traffic on management port to data ports. The fix ensures that the controllers work as expected.	AOS-W 8.7.1.6
AOS-228056	Users were unable to delete the configured time range neither through the **no time-range** command nor through the **Configuration > Roles and Policies > <role> > Time Range** field of the WebUI. The fix ensures that the users are able to delete the configured time range. This issue was observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-228104	A few OAW-AP535 access points running AOS-W 8.6.0.16 or later versions crashed unexpectedly. The log files listed the reason for the event as **Firmware Assert - PC : 0x4b1ce6dc, whal_reset.c:943 Assertion (wait < wait_timeout) failedparam0**. This issue occurred when, ■ there was continuous bi-directional traffic flow in a mixed-client network. ■ channels were busy. The fix ensures that the APs work as expected.	AOS-W 8.6.0.16
AOS-228149	When the number of wired devices tagged to the managed device was more than 100, the wired devices were not flagged after activating the cluster. The fix ensures that the managed device works as expected. This issue was observed in a managed device running AOS-W 8.10.0.0 in a cluster setup.	AOS-W 8.10.0.0
AOS-228318	Some OAW-AP535 access points running AOS-W 8.6.0.10 or later versions crashed unexpectedly. The log files listed the reason for the event as **Firmware Assert - PC: 0x4b1ce6dc, ar_wal_tx_de.c:68 Assertion 0 failedparam0 :zero.** This issue occurred when, ■ there was continuous bi-directional traffic flow in a mixed-client network. ■ the channels were busy. The fix ensures that the APs work as expected, Duplicates: AOS-228322, AOS-228362, AOS-230888, AOS-234857, AOS-228848, and AOS-234635	AOS-W 8.6.0.10
AOS-228462	The **show airmatch debug schedule switch-info** command did not display any output. This issue occurred when there were more than 120 switches connected in the network. The fix ensures that the **show airmatch debug schedule switch-info** command displays the output. This issue was observed in Mobility Conductors running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-228714	APs located in different geographical locations were incorrectly present in the same AirMatch partition. This issue occurred when interferers with same MAC address was present at different geographical locations. The fix ensures that the APs in different geographical locations are not present in the same AirMatch partition. This issue was observed in APs running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-228771	A dump-server profile with SCP did not work with a Windows SCP server. This issue was observed when a dump-collection profile was configured to use SCP with a Windows SCP server and OpenSSH, but empty test and crash files were sent to the Windows SCP server. The fix ensures that the dump-server profile with SCP works with a Windows SCP server. This issue was observed in managed devices running AOS-W 8.8.0.2 or later versions.	AOS-W 8.8.0.2
AOS-228996	The **AMON-sender** process crashed on managed devices unexpectedly. This issue was observed in OAW-4750XM controllers running AOS-W 8.7.1.5 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.5
AOS-229024	Some OAW-AP505 access points running AOS-W 8.7.1.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **PC is at wlc_mbo_parse_ie+0x15c/0x2b0 [wl_v6]**. The fix ensures that the AP work as expected.	AOS-W 8.7.1.5
AOS-229059	The kernel logs of a switch contained the debug and kernel logs of the APs. The fix ensures that the kernel logs of a switch do not contain the logs of the APs. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.5
AOS-229190 AOS-229798 AOS-230295	The **Dashboard** > **Overview** > **Clients** page of the WebUI did not display active and standby switch information. This issue was observed in Mobility Conductors running AOS-W 8.10.0.0 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.10.0.0
AOS-229336	A lot of **Radio Frames Retry Percent** alerts were triggered for an OAW-AP635 access point running AOS-W 8.9.0.0 or later versions. The fix ensures that the APs do not trigger the **Radio Frames Retry Percent** alerts.	AOS-W 8.9.0.0
AOS-229474 AOS-229582 AOS-229990	The **show ap database flags** command did not filter the output based on the specified flags. This issue was observed in Mobility Conductors running AOS-W 8.6.0.15 or later versions. The fix ensures that the command filters the output based on the specific flags.	AOS-W 8.6.0.15
AOS-229496 AOS-232865 AOS-234432	Some APs were unable to synchronize configurations from the managed devices. This issue occurred when PMTU was set to a value less than 1500. The fix ensures that the APs can synchronize configurations from the managed device. This issue was observed in APs running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.7
AOS-229538	Clients in the management interface VLAN were able to access the controller data ports through the management port, although the client default gateway was set to management interface IP. This issue was observed in OAW-4010, OAW-4024, OAW-4450, and OAW-4850 switches running AOS-W 8.0.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-229758	Clients were unable to receive IP addresses. This issue occurred when WPA2-PSK-AES and WPA2-PSK-TKIP opmodes were used for APs operating in d-tunnel mode. The fix ensures that clients are able to receive IP addresses. This issue was observed in APs running AOS-W 8.9.0.0 or later versions.	AOS-W 8.10.0.0
AOS-229828	Some controllers were facing issues when supporting weak ciphers during SSL/TLS negotiations. This issue was observed in switches running AOS-W 8.7.1.6 or later versions. The fix ensures that the cipher suites can be enabled and disabled as a part of the web server configuration to ensure secure SSL/TLS negotiations.	AOS-W 8.7.1.6
AOS-229897	Users were unable to download logs from the **Diagnostics > Technical Support** page of the WebUI. The fix ensures that the users are able to download logs using the WebUI. This issue was observed in Mobility Conductors running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-230169	The **firewall cp deny** rule failed to deny traffic for cluster CoA VRRP addresses. The fix ensures that the **firewall cp deny** rule denies traffic as expected. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions in a cluster setup.	AOS-W 8.0.0.0
AOS-230232	Some OAW-AP535 access points running AOS-W 8.9.0.1 or later versions failed to effectively capture many High Efficiency data frames during packet capturing. The fix ensures that the APs can capture non-DFS channel High Efficiency data frames.	AOS-W 8.9.0.1
AOS-230386 AOS-236524	A few OAW-AP555 access points running AOS-W 8.9.0.0-FIPS or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.0
AOS-230598 AOS-236018	The **auth** process crashed on managed devices running AOS-W 8.0.0.0 or later versions. The log file listed the reason for the reboot as **Segmentation Fault: bridge_ip_user_free**. The fix ensures that the managed devices work as expected.	AOS-W 8.0.0.0
AOS-230690	The feature bits of Mobility Controller Virtual Appliance incorrectly changed to enabled after restoring flash backup. The fix ensures that the Mobility Controller Virtual Appliance work as expected. This issue was observed inMobility Controller Virtual Appliances running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-230732	A few clients did not receive any reply from the DNS server. Also, packets that were dropped were encapsulated in GRE and the outer IP header had a checksum value of 0xFFFF. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-230749	The output modifier **|** was not visible as an optional parameter in the **show ap active** and **show ap radio-summary** commands. The fix ensures that the output modifier **|** is visible in the **show ap active** and **show ap radio-summary** commands. This issue was observed in APs running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-230798 AOS-231576	The output of the **show global-user-table list** command displayed duplicate user entries for bridge-mode wired and wireless users. The fix ensures that the command does not display the duplicate entries. This issue was observed inMobility Conductors running AOS-W 8.7.1.8 or later versions.	AOS-W 8.7.1.8
AOS-230822	The error message, **Error decrementing DS refcountfor cert** was displayed when users uploaded a new server certificate. This issue occurred when users tried to change the current switch certificate to an expired certificate. The fix ensures that the referencing for handling switch certificates works as expected. This issue was observed in Mobility Conductors running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-230900 AOS-231081 AOS-234940	Some OAW-AP530 Series and OAW-AP530 Series access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for reboot as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-231083	Some OAW-AP555 access points running AOS-W 8.7.1.7 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the crash as **FW Crash dog_hb.c:209 DOG_HB detects starvation of task "WLAN RT2", triage**. The fix ensures that the access points work as expected.	AOS-W 8.7.1.7
AOS-231178	The **stm** process crashed frequently after upgrading to AOS-W 8.7.1.7 version. This issue was observed in OAW-4550 switches running AOS-W 8.7.1.7 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.7
AOS-231191	The output of the **show wms system** command displayed the WMS Offload State information. The fix ensures that the output of the command is modified to remove WMS Offload State information. This issue was observed in controllers running AOS-W 8.9.0.2 or later versions.	AOS-W 8.9.0.2
AOS-231206	The **wpa3_sae** process crashed or was stuck in the **PROCESS_ NOT_ RESPONDING_CRITICAL** state. This issue occurred due to timer corruption. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-231218 AOS-232924 AOS-235193	High CPU utilization was observed in the **pptpd** process of managed devices running AOS-W 8.5.0.0-FIPS or later versions. This issue occurred because the FIPS version did not support the **pptpd** process. The fix ensures support for the **pptpd** process.	AOS-W 8.5.0.0
AOS-231233	Users were unable to upgrade APs using the FTP server. Also, the TFTP server was selected automatically to upgrade the APs. The fix ensures that users are able to upgrade the APs using the FTP server. This issue was observed in managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-231283	The log files of some Wi-Fi 6E APs incorrectly displayed the **6G radio 2 disabled due to mfg configuration** message. This issue occurred even when the 6 GHz radio mode was not disabled when the APs booted up. The fix ensures that the error message is not displayed. This issue was observed in OAW-AP630 Series and OAW-AP650 Series access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-231399 AOS-234467	Users were unable to add MC-VA licenses to any pool and an error message, **Can't find GSM license available count** was displayed. The fix ensures that users are able to add MC-VA licenses to managed devices. This issue was observed in managed devices running AOS-W 8.9.0.1 or later versions.	AOS-W 8.9.0.1
AOS-231501	Wi-Fi uplink over 6GHz band did not work as expected for OAW-AP610 Series, OAW-AP630 Series, and OAW-AP650 Series access points running AOS-W 8.10.0.0 or later versions. The fix ensures that the Wi-Fi uplink feature works as expected.	AOS-W 8.10.0.0
AOS-231649	Users with read-only access were able to enable configurations and view passwords configured for WLANs. The fix ensures that users with read-only access are not able to enable configurations and view passwords. This issue was observed in Mobility Conductors running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-231849	Mesh Portal APs did not change channels even after AirMatch changed the channels. This issue was observed in APs that had only mesh VAPs configured. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-231856	A few APs running AOS-W 8.6.0.0 or later versions crashed unexpectedly. The log files listed the reason for the event as **An internal system error has occurred at file sapd_sysctl.c function sapd_sysctl_write_param line 184 error Error writing /proc/net/wifi0/max_eirp_per_chan : Invalid argument**. This issue occurred due to change of channel on one or both the radios when EIRP check was done for the new channel. The fix ensures that the EIRP request is processed and no error logs are generated.	AOS-W 8.7.1.8
AOS-231859	OmniVista 3600 Air Manager displayed an incorrect number of clients connected to the Mobility Conductor. This issue occurred when AMON stats messages were not sent for OAW-RAP wired users. The fix ensures that the AirWave displays the correct number of clients connected to the Mobility Conductor. This issue was observed in Mobility Conductors running AOS-W 8.6.0.19 or later versions.	AOS-W 8.7.1.6
AOS-231990	The **Dashboard** > **Infrastructure** page displayed an incorrect **Last Reboot** time. The fix ensures that the WebUI displays the correct **Last Reboot** time. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.8

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-232014	During the EST enrollment process, a dummy private key was generated and stored as plain text. The fix ensures that the dummy key file is removed from the flash. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.6
AOS-232079	ACLs were not applied correctly. This issue occurred when DPI was enabled. The fix ensures that the ACLs are applied correctly on managed devices. This issue was observed in managed devices running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-232096	Some S-AAC controllers leaked data traffic of wireless clients that were connected in split-tunnel forwarding mode. The fix ensures that the controllers do not leak traffic. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.6
AOS-232120	The timestamp value was not updated correctly in the RADIUS accounting packets. The fix ensures that the timestamp value is updated correctly. This issue was observed in OAW-4850 controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232121	The **wipeout flash** command did not work as expected. The fix ensures that the command removes all the data and flash backup files as expected. This issue was observed in Mobility Conductors running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232124	High CPU utilization was observed in the **stm** process when client devices were utilizing TSPEC signaling. This issue was observed in Mobility Conductors running AOS-W 8.8.0.3 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.8.0.2
AOS-232130	iOS native VPN with EAP authentication did not work on managed devices running AOS-W 8.6.0.0 or later versions. The fix ensures that the iOS native VPN with EAP authentication works as expected.	AOS-W 8.9.0.1
AOS-232171	The list of clients that were not L2-connected were still displayed in the user table even when CoA disconnect was triggered. The fix ensures that the user table is updated correctly. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.15
AOS-232311	The user table did not list the entries of L3-connected clients and hence, clients were unable to pass traffic. Also, the netdestination configuration was not synchronized between the **authmgr** and **sapm** processes. This issue was observed when ValidUser ACL was configured for bridge mode clients. The fix ensures that the users are able to pass traffic. This issue was observed in stand-alone controllers running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-232348 AOS-235259	The **stm** process crashed on OAW-AP325 access points running AOS-W 8.7.1.7 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-232377	PAN firewall integration did not work as expected on 7240XM controllers running AOS-W 8.7.1.5 or later versions. The fix ensures that the PAN firewall integration works as expected.	AOS-W 8.7.1.5

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-232378	The **pim** process crashed on managed devices running AOS-W 8.7.1.8 or later versions. This issue occurred due to invalid memory access. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.8
AOS-232430	The spanning tree and interface related configuration details were not displayed in the output of the **show running-config** command. The fix ensures that the command displays the spanning tree and interface related configuration details. This issue was observed in Mobility Conductors running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-232443	Server derivation rules were not assigned correctly and the error message, **Missing server in attribute list** was displayed. This issue occurred when there was a delay in response from the RADIUS server. The fix ensures that the server derivation rules are assigned correctly. This issue was observed in stand-alone controllers running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-232469	Some managed devices running AOS-W 8.7.1.4 or later versions did not failover to the secondary Mobility Conductor after a reboot of the primary Mobility Conductor. The fix ensures that the managed devices failover to the secondary Mobility Conductor during a reboot.	AOS-W 8.7.1.4
AOS-232475	Users were unable to delete the time range configuration using both **no time-range** command and from the **Configuration** > **Roles and Policies** > **<role>** > **Time Range** field of the WebUI. The fix ensures that the WebUI and CLI allow users to delete the time range configuration. This issue was observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-232493	The entries of denylisted clients were not synchronized between the managed devices running AOS-W 8.6.0.15 or later versions in a cluster setup. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.15
AOS-232614	The multicast aggregation message, **stm_send_split_tunnel_status_to_mdns** was not sent to the **OFA** process. This issue occurred due to incorrect endianness. The fix ensures that the message is sent properly to the **OFA** process. This issue was observed in Mobility Controller Virtual Appliances and OAW-41xx Series controllers running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-232620	A discrepancy was observed between the total number of APs and the total number of AP BLE devices reported. The fix ensures that there is no discrepancy between the total number of APs and the total number of AP BLE devices reported. This issue was observed in APs running AOS-W 8.8.0.2 or later versions.	AOS-W 8.8.0.2
AOS-232631	Some controllers, after a reboot, responded to DNS queries even after the command **ip cp-redirect** was set to be disabled. The fix ensures that the controllers work as expected. This issue was observed in controllers running AOS-W 8.7.1.7 or later versions.	AOS-W 8.7.1.7

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-232657	Some APs got disconnected from the managed devices. This issue occurred when incorrect band information was sent to the **sapd** process when WIFi uplink was enabled. This fix ensures that the APs stay connected to the managed devices.	AOS-W 8.10.0.0
AOS-232701	A few OAW-AP630 Series access points running AOS-W 8.8.0.0 or later versions in a Mobility Conductor-Managed Device topology crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt - PC is at ieee80211_add_or_retrieve_ie_from_app_opt_ies**. The fix ensures that the APs work as expe	AOS-W 8.9.0.3
AOS-232703	A few OAW-AP630 Series access points running AOS-W 8.9.0.3 or later versions in a Mobility Conductor-Managed Device topology crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (ar_wal_rx_uplink.c:538 Assertion 0 failed)**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-232704	Some OAW-AP635 access points running AOS-W 8.9.0.3 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the reboot as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (:Excep :0 Exception detected Thread name : WLAN BE)**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-232712	Some OAW-AP615 access points running AOS-W 8.7.1.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **PC is at wlc_cur_phy+0x140**. Enhancements to the wireless driver resolved the issue.	AOS-W 8.7.1.5
AOS-232757	A BLE southbound API connection was terminated when the characteristic discovery was interrupted. The fix ensures that the BLE southbound API connection is not interrupted. This issue was observed in managed devices running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.2
AOS-232775	The session timeout returned after captive portal authentication from a RADIUS server was not honored. This issue occurred when both IPv4 and IPv6 addresses were associated to a single user connected in split tunnel forwarding mode, and when the idle timeout value was lesser than session timeout value. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.9.0.2 or later versions.	AOS-W 8.9.0.2
AOS-232874	The WebUI did not work on standby Mobility Conductors running AOS-W 8.7.1.8 or later versions. The fix ensures that the WebUI works on standby Mobility Conductors.	AOS-W 8.7.1.8
AOS-232896	Some APs running AOS-W 8.9.0.3 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the reboot as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (ar_wal_tx_halphy_send.c:479 Assertion ptx_halphy->ppdu_posted == 0 failed)**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-232897	The **wlan ht-ssid-profile** CLI command overrode the radio frequencies from 80 MHz to 40 MHz, although the **show ap bss-table** CLI command displayed the radio frequencies as 80 MHz. The fix ensures that the **wlan ht-ssid-profile** CLI command does not override the radio frequencies. This issue was observed in OAW-AP515 and OAW-AP535 access points running AOS-W 8.7.1.9 and AOS-W 8.10.0.0 versions.	AOS-W 8.7.1.9
AOS-232928 AOS-233808 AOS-234781 AOS-236854	A few APs running AOS-W 8.7.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **KASan: use after free in wlc_pcb_fn_find+0xc8/0x160**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.7.1.9
AOS-232967	Some OAW-AP635 access points running AOS-W 8.9.0.3 or later versions crashed unexpectedly. The log files listed the reason for event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (ar_wal_tx_send.c:16601 Assertion 0 failed)**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-232991	Users were unable to issue the **lc-cluster exclude-vlan** command and an error message, **ERROR: Invalid character** was displayed. This issue was observed in Mobility Conductors running AOS-W 8.7.1.7 or later versions. The fix ensures that users are able to issue the **lc-cluster exclude-vlan** command .	AOS-W 8.7.1.7
AOS-233005	Memory leak was observed in the **stm** process of Mobility Conductor. This issue was observed in Mobility Conductors running AOS-W 8.7.1.7 or later versions. The fix ensures that the Mobility Conductor works as expected.	AOS-W 8.7.1.7
AOS-233006	The Branch Gateway (BGW) sent TACACS accounting request with incomplete user information to ClearPass Policy Manager. This issue was observed in OAW-4104 switches running AOS-W 8.7.0.0 or later versions. The fix ensures that TACACS sends complete user information to ClearPass Policy Manager.	AOS-W 8.7.0.0
AOS-233048	Mesh APs did not work as expected on 160 MHz channel. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-233098	ICMP incorrectly forwarded traffic through the management port instead of the data port. This issue occurred when the **ip default-gateway mgmt <gateway-ip>** address was configured. The fix ensures that the switches work as expected. This issue was observed in OAW-4450, OAW-4010, OAW-4024, and OAW-4850 switches running AOS-W 8.7.1.7 or later versions.	AOS-W 8.7.1.7
AOS-233108	A few clients faced performance issues when the Time to Wake feature was enabled in the AP for wireless clients. This issue was observed in OAW-AP515 access points running AOS-W 8.8.0.0 or later versions. The fix ensures that the TWT feature is disabled.	AOS-W 8.8.0.0

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-233115	A few clients dropped Wifi-calling IPsec traffic that came through GRE tunnels. This issue occurred when tunnel keepalive was enabled. This issue was observed in managed devices running AOS-W 8.6.0.15 or later versions. The fix ensures that the clients do not drop Wifi-calling IPsec traffic.	AOS-W 8.6.0.15
AOS-233186	A few managed devices running AOS-W 8.10.0.0 or later versions sent TACACS traffic with source IP address as the VLAN interface instead of the system IP address. This issue was resolved by selecting the system IP address as the source IP address when source IP address was not configured. This issue occurred because the VLAN interface configured on the managed devices was used when source interface IP address was not configured.	AOS-W 8.10.0.0
AOS-233188 AOS-233811 AOS-234844	Some managed devices were unable to come up using ZTP. This issue occurred when the Conductor IP configuration was not available. This issue was observed in managed devices running AOS-W 8.7.1.7 or later versions. The fix ensures that the managed devices are able to come up using ZTP.	AOS-W 8.7.1.7
AOS-233217	Some OAW-AP535 access points did not transmit beacons in 5 GHz radio mode and clients were unable to view the SSIDs. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.0 or later versions. The fix ensures that the APs transmit beacons and work as expected.	AOS-W 8.6.0.10
AOS-233235 AOS-237635	The **mDNS** process in a managed device crashed after executing the **show airgroup multi-controller-table** CLI command. This issue was observed in switches running AOS-W 8.10.0.0 or later versions. The fix ensures that the mDNS process works as expected.	AOS-W 8.10.0.0
AOS-233399	Poor network performance was observed, and captive portal page did not load as expected for non-HE devices. This issue occurred when open system was configured. This issue was observed in OAW-AP510 Series access points running AOS-W 8.7.1.9 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.7.1.9
AOS-233409 AOS-226801	All the client entries in the user table got deleted. This issue occurred when a license was added to the stand-alone switch. The fix ensures that the user table entries are not deleted whenever the license limit is updated on the stand-alone switch. This issue was observed in stand-alone switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-233411 AOS-234524 AOS-235363	Some APs running AOS-W 8.6.0.17 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.17
AOS-233518	Some OAW-AP635 access points running AOS-W 8.0.0.0 or later versions crashed unexpectedly. The log files listed the reason for event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (:Excep :0 Exception detected Thread name : WLAN_SCHED0)**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-233582	The licensing server failed to update the IP address of the secondary Mobility Conductor. This issue occurred when the secondary Mobility Conductor became the primary Mobility Conductor. The fix ensures that the licensing server correctly updates the IP address of the Mobility Conductor. This issue was observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-233686	Users were unable to add MC-VA licenses to any pool and an error message, **Can't find GSM license available count** was displayed. The fix ensures that users are able to add MC-VA licenses to managed devices. This issue was observed in managed devices running AOS-W 8.9.0.1 or later versions.	AOS-W 8.9.0.1
AOS-233750 AOS-236273	Clients connected to bridge mode SSIDs were unable to pass traffic. The fix ensures that clients are able to pass traffic. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-233766	IPsec flapping was observed between primary and secondary Mobility Conductors in a certificate-based Layer 3 redundancy deployment. The fix ensures and there is no IPsec flapping. This issue is observed in Mobility Conductors running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-233869	The **im_helper** process was stuck in **busy** state when users tried to export the iBeacon configurations from the Mobility Conductor. The fix ensures that the **im_helper** process is not stuck. This issue was observed in Mobility Conductors running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-234082	Some OAW-AP535 access points running AOS-W 8.7.1.9 or later versions crashed unexpectedly. The log files listed the reason of the event as **kernel panic: Take care of the TARGET ASSERT first (ar_wal_tx_seq.c:3041 Assertion)**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.9
AOS-234103	A few clients were unable to connect to APs running AOS-W 8.6.0.0 or later versions in a Mobility Conductor-Managed Device topology. Enhancements to the wireless driver resolved this issue. This issue occurred when the APs dropped packets due to low memory consumption.	AOS-W 8.6.0.17
AOS-234153	Mobility Conductors running AOS-W 8.7.1.9 or later versions displayed multiple OSCP error logs. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.7.1.9
AOS-234173	Some users experienced TCP communication failure. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-234208	Some APs running AOS-W 8.7.1.9 or later versions were unable to failover to a different cluster. This issue occurred when the cluster member IP address was configured as backup LACP in the AP system profile. The fix ensures that APs can failover to different clusters.	AOS-W 8.7.1.9
AOS-234282	A mismatch of syslog messages was observed for clients connecting to bridge mode and tunnel mode SSIDs. The fix ensures that the syslog messages for bridge mode contain the same information as that of the tunnel mode. This issue was observed in managed devices running AOS-W 8.10.0.0 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.10.0.0
AOS-234315	A few APs sent PAPI messages to external IP addresses, and the log files displayed the **PAPI_Send failed** error message. The fix ensures that the APs display the correct IP addresses in the logs. This issue was observed in APs running AOS-W 8.6.0.15 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.6.0.15
AOS-234442	Mobility Conductors running AOS-W 8.9.0.3 or later versions displayed a value of 0 for the list of APs and clients for the managed device in the **Dashboard**>**Overview** page of the WebUI. The fix ensures that the correct value is displayed in the WebUI.	AOS-W 8.9.0.3
AOS-234477	Instead of scanning at the scheduled intervals, radios were wrongly scanned for every 10 seconds. The fix ensures that the radios are scanned at the configured time intervals. This issue was observed in APs running AOS-W 8.4.0.0 or later versions	AOS-W 8.4.0.0
AOS-234523	The SSL protocol configurations were automatically altered for random managed devices without the user the initiating the changes. This issue was observed in Mobility Conductors running AOS-W 8.6.0.17 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.6.0.17
AOS-234577	Some OAW-AP635 access points running AOS-W 8.9.0.3 or later versions crashed unexpectedly. The log files listed the reason for event as **Reboot caused by kernel panic: Fatal exception in interrupt (PC is at tun_recv_esp+0x38/0x2f8)**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-234647	The **stm** process crashed on Mobility Conductors running AOS-W 8.10.0.2 or later versions. This issue occurred after a VRRP failover. The fix ensures that the Mobility Conductors work as expected,	AOS-W 8.10.0.2
AOS-234730	Some OAW-AP635 access points running AOS-W 8.9.0.3 or later versions crashed and rebooted unexpectedly. The log files listed 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)**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-234783	Some OAW-AP505H access points running AOS-W 8.10.0.0 or later versions were flooded with **wlc_offload PhyRxSts Circular Buffer Control** logs and crashed unexpectedly. The log files listed the reason for the event as **Kernel panic - not syncing: Ktrace core monitor: cpu0 hung for 45 seconds, hung cpu count: 1**. The fix ensures that the APs work as expected.	AOS-W 8.10.0.0
AOS-234923 AOS-236878	Some OAW-AP635 access points running AOS-W 8.9.0.3 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: Take care of the TARGET ASSERT first with ar_wal_tx_halphy_send.c:479 Assertion ptx_halphy->ppdu_posted == 0 failed**. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-235002	WPA3-AES-CCM-128 encryption was incorrectly displayed as WPA2 AES in the **Dashboard > Overview > Wireless Clients** page of the WebUI. This issue was observed in running AOS-W 8.10.0.1 or later versions. The fix ensures that the WebUI displays the correct encryption.	AOS-W 8.10.0.1
AOS-235063	A few users were unable to delete custom ACLs from firewall CP and the error message **Invalid data: FW CP ACL not found** was displayed. This issue occurred because the custom ACLs were part of the internal firewall CP rules. The fix ensures that users are able to delete custom ACLs from the firewall CP. This issue was observed in managed devices running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-235085 AOS-234819 AOS-237981 AOS-237986	Some OAW-RAPs running AOS-W 8.6.0.9 or later versions did not broadcast BSSIDs and were stuck in AM mode. The fix ensures that the OAW-RAPs broadcast BSSIDs properly after rebooting the switch.	AOS-W 8.6.0.9
AOS-235220	The **Maintenance > Software Management** page of the WebUI did not display the entire list of clusters. This issue occurred when the cluster name or hostname was changed. The fix ensures that the WebUI displays the entire list of clusters. This issue was observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-235234	A few VIA client connections were unexpectedly terminated due to an error in the **ISAKMP** process. This issue was observed in stand-alone switches running AOS-W 8.10.0.0 or later versions. The fix ensures that the switches work as expected.	AOS-W 8.10.0.0
AOS-235257	The **SAPD** process crashed on managed devices running AOS-W 8.7.1.7 or later versions. This issue occurred when a hotspotter attack was detected. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.7
AOS-235401	Some managed devices running AOS-W 8.6.0.17 did not reflect the IPv6 address configured for the OAW-RAP. The fix ensures that the managed devices display the Pv6 address configured for the OAW-RAP.	AOS-W 8.6.0.17

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-235526 AOS-237145	Airmatch optimizations did not consider all the APs when the Mobility Conductor was upgraded with a flash size greater than 128 GB. This issue occurred when the received messages from the APs were dropped. This issue was observed in Mobility Conductors running AOS-W 8.6.0.18 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.6.0.18
AOS-235628	The Airwave AP monitoring page did not display AP related information such as the RF Neighbors list and RAPIDS list. The fix ensures that AP related information is displayed in Airwave. This issue was observed in OAW-4008 and OAW-4550 switches in the standalone topology.	AOS-W 8.10.0.2
AOS-235647	Some OAW-4750XM switches crashed and rebooted unexpectedly. The log file listed the reason as **Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:2)**. The fix ensures that the switches works as expected.	AOS-W 8.7.1.9
AOS-235681	The WebUI displayed an incorrect number of APs that were **DOWN** . However, the CLI displayed the correct status of the APs. The fix ensures that the WebUI displays the correct status of APs. This issue was observed in stand-alone switches running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1
AOS-235786	A few OAW-4850 switches running AOS-W 8.6.0.17 sent system log messages without the hostname to the system log server. This issue occurred when the hostname was not set during the switch bootup. The fix ensures that a valid hostname is assigned to the switch.	AOS-W 8.6.0.17
AOS-235810	The changes to the configured SAP MTU value of the AP system profile were displayed incorrectly on the managed device. This issue occurred because the storage format of the MTU configuration file was changed and the file was not read correctly. The fix ensures that the managed device displays the corrcet MTU value.	AOS-W 8.9.0.2
AOS-235840 AOS-236318	The **Configuration** > **System** > **Profiles** page of the WebUI did not allow users to select any encryption other than xSec. The error message, **Invalid Opmode combination** was displayed when users unchecked the xSec checkbox. The fix ensures that the WebUI allows users to select any encryption. This issue was observed in Mobility Conductors running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-235891	Some stand-alone switches displayed continuous **PAPI_Send** errors. This issue occurred because, for wired clients, the IP address of the AP was not available at UCC. Hence, the error message was seen when UCC attempted to send messages through PAPI to AP with zero IP. The fix ensures that the PAPI message is not sent to the OAW-RAP when the APs IP address is zero.	AOS-W 8.7.1.9
AOS-235948	Some managed devices did not forward traffic to the captive portal page using redirect ACL. This issue occurred when the traffic was incorrectly forwarded to an inactive port. The fix ensures that the managed devices forward traffic as expected. This issue was observed in managed devices running AOS-W 6.5.4.19 or later versions.	AOS-W 6.5.4.19

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-235951	A few OAW-AP655 access points running AOS-W 8.11.0.0 crashed unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Bad mode in Synchronous Abort handler detected**. The fix ensures that the APs work as expected.	AOS-W 8.11.0.0
AOS-236200	Some OAW-AP374 access points configured as mesh APs crashed unexpectedly. The log file listed the reason for the crash as **kernel panic: Fatal exception**. The fix ensures that the APs work as expected. This issue was observed in OAW-AP374 access points running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-236235	Multiple APs crashed due to mismatch between **wmm_eap_ac** and **eapol_ac_override** in the configuration. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.2.	AOS-W 8.10.0.2
AOS-236255	A few APs failed to establish PPPoE connection. This issue occurred when the APs did not initiate PPPoE Active Discovery Initiation (PADI) after the upgrade.The fix ensures a successful PPPoE connection after an upgrade. This issue was observed in stand-alone switches running AOS-W 8.10.0.2.	AOS-W 8.10.0.2
AOS-236351 AOS-237780	A few users were unable to discover the wireless server in CPPM-based shared location. This issue occurred when CPPM shared location was not in AP neighborhood of the user-connected AP and CPPM shared role/username was also present. The fix ensures that the users are able to discover the server. This issue was observed in APs running AOS-W 8.10.0.0 or later versions in Mobility Conductor-Managed Device topology.	AOS-W 8.10.0.3
AOS-236462	A few OAW-RAPs running AOS-W 8.5.0.13 went down unexpectedly. This issue occurred because SAPD did not update the IPv6 IP address in the datapath user-table when the OAW-RAP renewed the IPv6 IP address. The fix ensures that the APs work as expected.	AOS-W 8.5.0.13
AOS-236621	Some OAW-4850 switches crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20)**. The fix ensures that the OAW-4850 switches work as expected.	AOS-W 8.10.0.2
AOS-236728	Some OAW-AP535 access points running AOS-W 8.9.0.3 crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: softlockup: hung tasks**. This issue occurred due to kernel softlockup in SMP during the **zero-wait-dfs** activities. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-236813	Mobility Conductor running AOS-W 8.10.0.2 generated error messages every 20 seconds for every managed device acting as an ofc-agent. The fix ensures that the Mobility Conductor handles the error messages related to the auxiliary OF channel correctly.	AOS-W 8.10.0.2

Table 7: *Resolved Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-236881	After upgrading Mobility Conductors to AOS-W 8.7.1.8 or later versions, the profile manager in the secondary Mobility Conductor stopped responding. This issue occurred when IPv6 mode was enabled in the secondary Mobility Conductor because of which it failed to download certificates from the primary Mobility Conductor. The fix ensures that the secondary Mobility Conductor works as expected when IPv6 mode is enabled.	AOS-W 8.7.1.8
AOS-236907	The hidden BSSIDs were visible to users connected to other hidden BSSIDs. This issue occurred when the 6 Ghz band was enabled. The fix ensures that the APs work as expected. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-236920	Users were unable to convert a few APs to OpenConfig. This issue occurred when the images on the SCP server were not provided the **Read** access. The fix ensures that the users are able to convert APs to OpenConfig. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.18
AOS-237081	Some OAW-AP345 access points were stuck in a reboot loop after upgrading to AOS-W 8.7.1.10-FIPS. Enhancements to the wireless driver resolved the issue.	AOS-W 8.7.1.10-FIPS
AOS-237174	Some 9240 switches using **SSHD** process recorded informational logs, even though the system log level was configured as **warning**. This issue occurred because the **SSHD** process used an incorrect syslog function. The fix ensures that the system logs are filtered correctly based on the configured log level.	AOS-W 8.10.0.2
AOS-237478	Some OAW-AP535 access points running AOS-W 8.9.0.3 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the crash as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue occurred when the client offloading session accelerated and decelerated in the same session. The fix ensures that the APs work as expected.	AOS-W 8.9.0.3
AOS-237869	Some OAW-AP635 access points running AOS-W 8.10.0.2 or later versions displayed the error message, **Unexpected stm (Station management) runtime error at stm_sysctl_read_param, 13937, Error opening /proc/sys/net/aruba103/max_clients : No such file or directory**. The fix ensures that the APs work as expected.	AOS-W 8.10.0.2
AOS-224968 AOS-226800 AOS-229670	The name of the cluster profile changed unexpectedly when the managed device was rebooted. Hence, the managed devices were unable to form a cluster. This issue was observed in OAW-4450 switches running AOS-W 8.5.0.13 or later versions. The fix ensures that the managed devices are able to form a cluster.	AOS-W 8.5.0.13

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

Limitations

Following are the limitations observed in this release.

Access Points

The Spectrum Analysis feature is not supported on OAW-AP615 access points.

UNII-4 Channel Support for OAW-AP615

OAW-AP615 access points do not support UNII-4 channel.

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 8: *Known Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-212624	The managed devices and APs fail to join the new primary switch in an L3 redundancy setup. This issue occurs when the role of the primary and secondary L3 conductors is interchanged in an L3 redundancy setup.	AOS-W 8.11.0.0
AOS-235314	The **ZMQbg!Reaper** process crashes on some Mobility Conductors randomly. This issue is observed in Mobility Conductors running AOS-W 8.11.0.0.	AOS-W 8.11.0.0
AOS-235829	Some OAW-AP615 access points are unable to pass TCP downstream traffic on the 6 GHz radio band. This issue occurs when the EDCA parameters are altered. This issue is observed in OAW-AP615 access points running AOS-W 8.11.0.0 version.	AOS-W 8.11.0.0
AOS-236478	Some OAW-AP655 access points experience severe packet drops when connected to an SSID. This issue is observed in OAW-AP655 access points running AOS-W 8.11.0.0 version.	AOS-W 8.11.0.0

Table 8: *Known Issues in AOS-W 8.11.0.0*

New Bug ID	Description	Reported Version
AOS-237372	A few OAW-AP610 Series access points running AOS-W 8.11.0.0 use the 6 GHz radio to connect to Wi-Fi uplink although the 6 GHz radio is disabled using the **apoot** command.	AOS-W 8.11.0.0
AOS-237903	The mobility-manager's **SNMP_TRAP iptable** rules are getting deleted on Mobility Conductor and managed devices. This issue occurs when the management interface or the default route on management interface is modified after configuring mobility-manager. This issue is observed in controllers running AOS-W 8.11.0.0. **Workaround:** It is recommended not to edit the management interface or modify the default route on management interface after configuring the mobility-manager. If you edit the previously mentioned management interface configurations after configuring mobilty-manager and you want those deleted iptable rules back, then reboot the device.	AOS-W 8.11.0.0
AOS-235479	The commands, **copy ftp** and **copy tftp** do not work via the interface management as expected. This issue is observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17

Chapter 8
Upgrade Procedure

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

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

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Conductor Licensing Guide*.
- With the introduction of the Long Supported Release (LSR) and Short Supported Release (SSR) terminology in AOS-W 8.10.0.0, a Mobility Conductor running an LSR release supports managed devices running the same release and the three preceding releases. This is considered as N-3 support. This allows a customer to run the latest LSR, the previous SSRs and the previous LSR simultaneously. A Mobility Conductor running an SSR release supports managed devices running the same release and the two preceding releases. This would be considered N-2 support and is the same behavior as the pre-AOS-W 8.10.0.0 MultiVersion support.
- Only for the AOS-W 8.10.0.0 LSR release, AOS-W 8.6.0.0 is treated as an LSR despite being beyond N-3. As such a Mobility Conductor running AOS-W 8.10.0.0 supports managed devices running AOS-W 8.10.0.0, AOS-W 8.9.0.0, AOS-W 8.8.0.0, AOS-W 8.7.0.0 and AOS-W 8.6.0.0.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your 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 43 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 43 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 43 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 9 for all supported switch models:

   Table 9: *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 9, 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 9

4. **If you are unable to free up sufficient flash memory, contact Technical Support. Do not reboot the switch.**
5. If sufficient flash memory is available, proceed with the standard AOS-W upgrade. See Upgrading AOS-W.
6. If a reboot was performed, you may see some of the following errors. Follow the directions below:
   - Upgrade using standard procedure. You may see some of the following errors:

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

     Please clean up the /flash and try upgrade again.

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

     Please clean up the /flash and try upgrade again.

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

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

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

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

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

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

```
*****************************************************************
* WARNING:  An additional image upgrade is required to complete the *
* installation of the AP and WebUI files. Please upgrade the boot   *
* partition again and reload the controller.                        *
*****************************************************************
```

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

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

- Issue the **delete filename <filename>** command to delete large files to free more flash memory.
- Check if sufficient flash memory is free as listed in Table 9.
- Proceed with the standard AOS-W upgrade procedure in the same partition. See Upgrading AOS-W.

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

```
(host) #backup flash
Please wait while we take the flash backup.......
```

```
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```

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

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

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

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

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

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

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

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

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 40.

NOTE

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

In the WebUI

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

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

NOTE

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

4. Log in to the AOS-W WebUI from the Mobility Conductor.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.

6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

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

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

In the CLI

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

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

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

or

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

or

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

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

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Conductor.

```
(host)#reload
```

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

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

Verifying the AOS-W Upgrade

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

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 43 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 43 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 43.
2. Verify that the control plane security is disabled.
3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

- If any new certificates were added in the upgraded AOS-W version, reinstall these certificates in the downgraded AOS-W version.

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

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

CAUTION

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

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

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

In the CLI

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

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

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

   or

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

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

   (host) # boot config-file `<backup configuration filename>`
3. Execute the **show image version** command to view the partition on which your pre-upgrade AOS-W version is stored.

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

CAUTION

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.