AOS-W 8.12.0.0 Release Notes

Alcatel·Lucent
Enterprise

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

Important

The factory-default image of APs introduced in AOS-W 8.9.0.0 or later versions use **aruba-conductor** as the host name instead of **aruba-master** to identify a target managed device or standalone switch during DNS discovery. However, the factory-default image of APs that were introduced prior to AOS-W 8.9.0.0 still use **aruba-master** during DNS discovery. The usage of **aruba-conductor** is to align with the Inclusive Language Initiative.

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 ConductorLicensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent AP Software Quick Start Guide*

Supported Browsers

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

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	▪ Windows 10 or later ▪ macOS
Firefox 107.0.1 or later	▪ Windows 10 or later ▪ macOS

Web Browser	Operating System
Apple Safari 15.4 (17613.17.1.13) or later	▪ macOS
Google Chrome 108.0.5359.71 or later	▪ Windows 10 or later ▪ macOS

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our ALE culture and moving forward, ALE will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

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

Chapter 3
What's New in AOS-W 8.12.0.0

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

New Features and Enhancements

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

Enabling SIM PIN for USB LTE Modems

Starting with AOS-W 8.12.0.0, SIM PIN configurations can be set on OAW-RAPs using CLI commands instead of AT commands.

Enhancements to the OFA Core Size

By excluding a section of process memory, OFA core size is reduced. This reduction helps in capturing and debugging OFA cores in scale scenarios.

Enhancement to VAPs

The processing time for manually created VAPs to transition from **interfering** to **valid** has been enhanced.

Added Support for Telematrix IP Phones with OAW-AP505H Access Points

Improved OAW-AP505H PSE port compatibility with early generation Telematrix IP phones.

Crypto IPSec Configuration

Starting with AOS-W 8.12.0.0, the **no** parameter is added to the **crypto ipsec mtu** command to set the IPSec MTU value to default. Also, the configured global MTU is added to the output of the **show tech-support** command.

No Support for Air Slice in AOS Campus Deployments

Starting with AOS-W 8.12.0.0, Air Slice support will not be available. If Air Slice is enabled prior to the upgrade, it will be displayed as enabled in the configuration, but it will not take effect internally. The following commands have been impacted:

- **show profile-list airslice-profile**
- **show ap bss-table**
- **show airslice**
- **ap-group**
- **ap-name**
- **airslice**

Implementation of Cryptographic Hashing within SNMPv3

AOS-W 8.12.0.0 implements the utilization of HMAC based SHA-224, SHA-256, SHA-384 and SHA-512 cryptographic hashing within SNMPv3. The **show snmp user-table** command was updated for AOS-W 8.12.0.0.

Upgrade in Maximum AP Count in 9012 Controllers

In AOS-W 8.12.0.0, the maximum AP count for 9012 switches is upgraded from 32 to 64.

New Syslog Error Alert in OmniAccess Mobility Controllers for Misconfigured or Failed AirMatch States

In AOS-W 8.12.0.0, a syslog error alert appears in OmniAccess Mobility Controllers for misconfigured or failed AirMatch States, which can be checked with the **show log errorlog all | include AirMatch** and **show log errorlog all | include mcell_recv** commands.

Improvement of Random Channel Selection in Mobility Conductors

In AOS-W 8.12.0.0, the speed and quality of the random channel selection has been improved in Mobility Conductors when the configuration is changed for the APs.

Improvement in AP Statistics

Several statistics have been improved for APs running AOS-W 8.12.0.0.

Addition of Symmetric Cipher AES-256

AOS-W 8.12.0.0 adds the symmetric cipher Advanced Encryption Standard 256 (AES-256) as an SSH server functionality.

Introduction of the coverage-level-2-4GHz Command to Configure the Aggressiveness Threshold

In AOS-W 8.12.0.0, a new parameter called **coverage-level-2-4GHz** under the **airmatch profile** command is introduced to configure the aggressiveness threshold. It is required to enable the **airmatch-mode-aware** parameter under the **rf profile** command.

Optimization in Tx Retransmissions

AOS-W 8.12.0.0 optimizes Tx rate adaptation to reduce retransmissions during idle background traffic when using 5 GHz and 6 GHz connections.

Zigbee Radio Profile Supports Multiple Channels

AOS-W 8.12.0.0 incorporates an option to add multiple channels in the Zigbee's radio profile. This new feature is available in the **Managed Network > Configuration > IoT > IoT Radios** page of the WebUI.

Implementation of an Option to Configure Enforce DHCP for UBT Clients

AOS-W 8.12.0.0 implements an option to configure enforce DCHP for UBT clients in the CLI. When using various roles or VLANs with User-based tunneling, the **enforce-dhcp** functionality is available at the role level.

Implementation of SCP for Secure Image Download

AOS-W 8.12.0.0 implements the SCP protocol for secure image download. The **scp-img-upgrade-preference** command is available to enable SCP for secure image download and it uses port 22 as default.

For more details on how to handle AP image download, see *Possible Scenarios during AP Image Download*.

Tap Functionality to Control LED Behavior on AP-605H Access Points

Starting with AOS-W 8.12.0.0, AP-605H access points support tactile control to toggle the operating LED mode between **normal** and **off**. This flip occurs only when the AP is active and configured in **normal** mode just by tapping the front of the AP.

6 GHz Enablement for AP-654 and AP-634 Access Points

Starting with AOS-W 8.12.0.0, the AP-654 and AP-634 platforms will support 6 GHz band operation, with support from Alcatel-Lucent's Frequency Coordination Orchestrator (FCO) solution, which will enable the Automated Frequency Coordination (AFC) feature for standard power operation.

Support for 670 Series Outdoor Access Points

The 670 Series access points (AP-675, AP-675EX, AP-677, AP-677EX,AP-679, and AP-679EX) are Alcatel-Lucent's first outdoor APs that support 6 GHz operation. These 802.11ax Wi-Fi 6E Outdoor Access Points offer 2x2 MIMO radios that allow for simultaneous tri-band operation. These APs also feature a wired 2.5 Gbps Smart Rate network interface and one SFP port for fiber support. The 670 Series access points require deployments managed by a Mobility Conductor when running AOS-W 8.12.0.0. The APs also support 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax wireless services.

Additional features include:

- Data rates up to 2.4 Gbps
- Support for Automatic Frequency Coordination (AFC)
- Maximum Ratio Combining (MRC)
- Orthogonal Frequency Division Multiple Access (OFDMA)
- IoT-ready (integrated Bluetooth 5 and 802.15.4 radio for Zigbee support)
- Target Wake Time (TWT) for improved client power savings
- Advanced Cellular Coexistence (ACC)
- WiFi uplink support

Support for AP-605H Access Points

The AP-605H access point is a high-end dual-radio tri-band 2x2 MIMO 802.11ax WiFi 6E hospitality AP platform supporting concurrent operation in any two of the three supported bands (2.4 GHz, 5 GHz and 6 GHz). The mode of operation is configurable either manually or through AirMatch. Ideal for hospitality, branch, and teleworker use-cases, the AP-605H access points can be deployed in either controller-based or controller-less network environments.

Additional features include:

- Flexible coverage across any two bands (2.4 GHz, 5 GHz, and 6 GHz) for up to 3.6 Gbps combined peak data rate.
- Up to seven 160 MHz channels in 6 GHz support low-latency, bandwidth-hungry applications like high-definition video and AR/VR applications.

- Combines wireless and wired access in compact desktop or wall mount model that can be PoE powered.
- Convenient wired connectivity and support for PoE with fast 2.5 GbE uplink port, two 1 GbE ports, and two 1 GbE PSE ports capable of supplying up to a total of 30W PoE.
- IoT-ready with integrated Bluetooth 5 and Zigbee.

Support for Higher Bit Sizes in Signature Generation

AOS-W 8.12.0.0 introduces support for higher key sizes in certificate signature generation to comply with United States Government security guidelines. Specifically, RSA keys will be 3072 bits or greater, while ECDSA keys will be 384 bits or higher.

Authentication Survivability Allows Automatic MPSK Passphrase Caching

Authentication survivability has been enhanced to include MPSK authentication. This enables cached data from a prior MPSK authentication to be available for gateways to authenticate and authorize users in case of RADIUS server inaccessibility.

Enhanced Debugging Experience in the Radio Profile

The **scheduler-mode** parameter is added to the radio profile in order to provide a better debugging experience. The parameter accepts two possible configurations, **fairness** and **latency**. The default parameter is set to **fairness**, which enables Traffic Allocation Framework (TAF) on the radio profile. The **latency** parameter disables TAF.

Support for OAW-AP584 Access Points Outdoor Operation in France and Israel

The DRT information for OAW-AP584 access points now complies with the regulatory guidelines that allow for outdoor operation in France and Israel.

Enhanced Support for AP IPv6 Address Generation

In the updated IPv6 address generation process, users can now seamlessly switch between address generation methods. While the default method remains the AP MAC address (EUI-64) format, an option to change to the stable privacy method is now available. This update introduces a new parameter, **ip6-addr-gen-mode**, within the **provision-ap** command for easy switching between these methods. The new parameter offers the following set of configuration options:

- **ip6-addr-gen-mode eui64**
- **ip6-addr-gen-mode stable-privacy**
- **no ip6-addr-gen-mode**

Accessibility Improvements

This release includes significant enhancements in accessibility features.

- **Luminosity Contrast Fixes**: Improved contrast ratios throughout the user interface to ensure better visibility and readability for users with visual impairments.
- **Redesigned Form Elements**: Checkboxes, ratio buttons, and toggle buttons have been redesigned for higher visibility. These elements now stand out more clearly against various backgrounds, aiding

users with visual challenges.

- **Enhanced Support for Screen Readers**: Significant improvements have been added in the software's compatibility with leading screen readers.
- **Improved Keyboard Navigation:** Enhanced keyboard navigation capabilities, ensuring a smoother and more intuitive experience for users who navigate without a mouse.

Enhanced SNMP Server Configuration for Individual Controller Identification

In this release, we introduce a significant enhancement to the SNMP (Simple Network Management Protocol) server configuration. The **new vrrp-id** parameter has been added to the **snmp-server** command, allowing users to assign a unique IP address as an identifier for each controller. This feature is designed to address the challenges faced in environments where multiple controllers are configured with the same IP address under the Virtual Router Redundancy Protocol (VRRP). This enhancement ensures SNMP traps and informs are correctly attributed to individual controllers, particularly after VRRP state changes.

Generic RADIUS Location Delivery Service

This release introduces generic location Information support in RADIUS, which facilitate advanced location-aware network functionalities. These enhancements enable precise location-based policy enforcement and improve billing and accounting practices. For the purpose of this release, only civic location attributes are supported. This enhancement introduces the following changes:

- The **ap location-profile** command is added to configure a profile that specifies the location information for access points.

  A new parameter **ap location profile** has been added to the **ap-group** command, and a new **ap location profile** parameter has been added to the **ap-name** command.
- Two new parameters, **radius-loc-obj-in-access** and **radius-loc-obj-in-accting** have been added to the **aaa-profile** command.
- The **show ap debug ap-location** command has been added to display effective AP location information as well as metadata for debugging purposes.
- The output of the existing **show dot1x ap-hash-table** command has been enhanced to display the effective AP location information.

Hardening Logical Port Security

This release introduces updates to the management of logical ports on the controller. The update includes hardening enhancements designed to optimize port usage by removing references to unused ports. Previously, certain legacy application integrations required specific ports for communication. Since these applications are no longer in use, the interfaces and ports dedicated to them have become unnecessary. Such ports and interfaces have been dereferenced.

Default control plane firewall rules have been applied. This change is applicable across all controller platforms.

Introduction of New 11ax (Wi-Fi 6) Statistics

This release provides advanced statistical data on network performance, leveraging the latest Wi-Fi 6 capabilities for improved network management and optimization. This data is key for enhanced

troubleshooting, allowing for quick identification and resolution of network issues and more precise network tuning.

Tracking of Randomized MAC Addresses

This feature enables the tracking of probe requests from clients using randomized MAC addresses, offering deeper insights into client presence within the network infrastructure. This update is pivotal for businesses seeking advanced analytics in environments where understanding visitor behavior and network usage patterns is essential. With this enhancement, the new parameters **laa-counter-msg** and **laa-counter-msg-interval** are introduced on existing **ids general-profile default**. Counter information is sent to ALE using **profile default-ale** command.

Updated USB Dongle Firmware Upgrade for SES-Imagotag SCD

This release introduces updates for the SES-Imagotag SCD firmware. This enhancement enables the capability for USB dongles to generate a Claim-ID, a critical component for establishing a secure connection to V:Cloud. This feature addresses the need for enhanced security in data communication between retail management systems and V:Cloud.

BLE Beacon Monitoring in Mobility Conductor- Managed Device Topology

This release introduces significant enhancements in the management of BLE (Bluetooth Low Energy) beacons within Mobility Conductor- Managed Device topology. This update introduces changes in the WebUI and CSV export functionality for BLE beacon information, streamlining the management process for large-scale deployments.

Support for 2 MBSSID Groups with 8 SSIDs on the 6GHz Band

This release broadens the capabilities of access points (APs) with enhanced support for multiple BSSID (MBSSID) groups, particularly targeting the 6 GHz band for Wi-Fi 6E compliance. APs are now equipped to manage up to 2 MBSSID groups. Each group can accommodate up to four 6 GHz VAPs (Virtual Access Points) to broadcast 8 unique SSIDs across the 6 GHz spectrum. This upgrade is complemented by the addition of new Command Line Interface (CLI) options and multizone configurations, providing granular control and customization for network users.

Enforce-DHCP is Configurable at the Role Level

When using various roles or VLANs with User-based tunneling, the **enforce-Dhcp** functionality is available at the role level. Previously this option was only configurable at profile(AAA) level, but now, this feature this provides better control and efficiency to handle clients. Use the **user-role authenticated** command to enable or disable this option:

- Enable: enforce-dhcp
- Disable: no enforce-dhcp

When enabled, the **show rights authenticated** command displays Enforce Dhcp: Enabled as part of the output.

Enable or Disable deauth-based steers for 802.11v and non-802.11v Clients

AOS-W 8.12.0.0 introduces a the **cm-deauth-steer-mode** knob in arm profile, which enables or disables **deauth-based** steers for both 802.11v and non 802.11v clients. The default for this new knob is

enabled. If this knob is disabled, no steers will be triggered for non 802.11v clients. This will also affect fallback to deauth steers for 802.11v capable clients after repeated failures of 802.11v requests. If both **cm-dot11v** and **cm-deauth-steer-mode** knobs are set to disabled, there will be no steers triggered by ClientMatch. Use **cm-deauth-steer-mode** knob in **rf arm-profile** to enable and disable this feature. Please note this has to be done in each of the arm profiles (for 2.4 GHz, 5 GHz and 6 GHz) independently.

Enhancement to the show ap tech-support ap-name Command

Starting with AOS-W 8.12.0.0, the output of the **show ap arm split-scan-history <ap-name>** command is added in the **show ap tech-support ap-name <ap-name>** command. This reduces the turn around time during data collection, improving customer service experience.

AirGroup Version 2 Support

Starting with AOS-W 8.12.0.0, Mobility Conductor and Managed Devices will run AirGroup Version 2. This enhancement is true for both Standalone and Distributed modes of the managed devices.

Support for Enabling and Disabling 6 GHz Radio

Starting with AOS-W 8.12.0.0, access points will support AFC on the 6GHz in Standard Power operation. The Wi-Fi 6E supported APs are AP-634,

AP-654, AP-675, AP-677 and AP-679 access points. Based on the AFC response, the following actions will take place:

- Disable the radio when there is no AFC response when AP comes up.
- Enable the radio when AFC response is received.
- Disable the radio when AFC timer has expired.

Wi-Fi 6E Standard-Power Support for Frequency Coordination Orchestrator

Frequency Coordination Orchestrator (FCO) is a new feature that introduces automatic 6 GHz radio enablement for supported campus access points, also known as Automatic Frequency Coordination (AFC). The work flow is as follows:

- Set up an account in HPE GreenLake to obtain API credentials.
- Configure the Mobility Conductor with these credentials.
- The APs will send the information to the Mobility Conductor, specifically, to the FCO Agent. This information includes AP location, AP FCCID and serial number.
- FCO service will retrieve an AFC response and send it back to SAPM on the MD where the AP is located.
- The managed device SAPM receives the AFC response message from Mobility Conductor SAPM and sends it to SAPD on the AP.
- After the AP receives the AFC response, it will apply it as a DRT update to the driver. The 6 GHz radio will be enabled or disabled based on the AFC response.

Note: This feature is not intended to work with standalone deployments or any other deployment in campus mode that does not involve Mobility Conductors.

For complete technical details and installation instructions, see the AOS-W 8.12.0.0 User Guide.

AirGroup Server Based Policy Support

8.12.0.0 relaunches support for Server Based Policy in v2. This feature has the following conditions:

- AirGroup is used with no CPPM.
- There are less than 512 wired servers.
- Customers want to configure specific devices to add location details for visibility.
- CLI policy profile is set at the /md level only.
- Applicable only to centralized mode.
- Not applicable for MDs running in distributed mode in 8.10 (i.e. Managed devices with v1).

Web socket Connection Support with Meridian Server

Starting with AOS-W 8.12.0.0, web-socket connection can be securely established with Meridian Asset Tracking and Telemetry web socket via a new handshake retry mechanism that alleviates the effects of incorrect token from Meridian server.

New Hypervisor Support for Virtual OmniAccess Mobility Controller and Virtual Mobility Conductor

Starting with AOS-W 8.12.0.0, all VMCs and VMCRs support:

- Windows Server 2022
- VMware ESXi 8.0

RADIUS Authentication Server Profile Configurations Added to AirGroup Version 2

The AirGroup version 2 module now accepts RADIUS authentication profile changes such as **nas-IP** and **source-interface** through the **aaa authentication-server radius** command. Rather than depending on the Mobility Conductor's settings, this feature allows for specific authentication-related configurations to be applied to managed devices.

The configuration varies depending on the AirGroup mode used:

- **Centralized mode** requires configurations to be applied on both the Mobility Conductor and managed device. In the case of having different profiles configured, the managed device's profile will take priority.
- **Distributed mode** requires node-specific configuration. In the case of having governing managed devices, the configuration will apply to all member nodes. However, node-specific configuration can still be applied to member nodes if needed.

Enhanced ASSERT Logging on OAW-AP500 Series and 600 Series Access Points

AOS-W introduces the **show ap debug wlan-firmware-alert-logs** command to record TARGET ASSERT logs from OAW-AP500 Series and 600 Series access points.

Separation of Cluster and Datapath Commands from 'tar log tech-support'

Cluster and datapath commands have been separated from **tar log tech-support**. For cluster logs, users should use: **tar logs tech-support cluster**.

New Enhancments Added to the show stm perf-history Commnad

Starting with AOS-W 8.12.0.0, the **show stm perf-history** command is modified as follows:

- Default output is 5 minute intervals, covering 24 hours
- New interval and duration CLI options are added to control the output row interval in minutes and the number of hours the total output covers.
- A new A2C column displays the counts of received Up, Down and Deny List events, and the number of STA retries received.

Enhanced ASSERT Logging on OAW-AP500 Series and 600 Series Access Points

AOS-W 8.12.0.0 introduces the **show ap debug wlan-firmware-alert-logs** command to record TARGET ASSERT logs on OAW-AP500 Series and 600 Series access points.

Enhancement to BMAP Handling During VLAN Configuration

By no longer updating cluster bucketmaps at the time of VLAN configuration, this enhancement eliminates the need for Virtual AP reconfiguration whenever a VLAN is added or removed. Additionally, with this change, cluster L2 vs. L3 connectedness has been eliminated. In turn, all clusters are now assumed to be L2 connected. This brings about three key changes:

- **Hitless failover:** Station failovers are now always hitless failovers. Cluster APs switch station traffic over to their standby UAC, but leave their 802.1x authentication association intact, resulting in a no-deauthentication failover.
- **VLAN retention:** No new VLAN derivation occurs on standby UACs during a hitless failover, meaning that stations will keep their originally assigned VLAN. It is important to note that this means that if their assigned VLAN is not present on the standby UAC, the station's traffic will be blackholed until the station reconnects and a new VLAN is derived.
- **Cluster CLI commands:** To check for VLAN mismatches, the **show lc-cluster vlan-probe status** command is recommended. Per the change above, the **show lc-cluster group-membership** command will always display devices as L2-connected.

Note: It is expected that all user VLANs within a cluster are configured on all managed devices within the cluster to ensure seamless client failovers.

Standard Power operations for Wi-Fi 6E APs will be disabled until all FCC certifications are accomplished. Once FCC certifications are in place, Frequency Coordination Orchestrator (FCO) service will be available for implementation in 6 GHz Standard Power GPS enabled APs running AOS-W 8.12.0.0.

Behavioral Changes

Removal of ssh-rsa Signature Scheme from SSH Cryptographic Settings

The **ssh-rsa** parameter has been removed to eliminate any security concerns with the SHA-1 hash algorithm and RSA public key algorithm.

Chapter 4
Supported Platforms in AOS-W 8.12.0.0

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

Table 5: *Supported AP Platforms*

AP Family	AP Model
OAW-AP303 Series	OAW-AP303, OAW-AP303P
OAW-AP303H Series	OAW-AP303H, OAW-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP318
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP370EX Series	OAW-AP375EX, OAW-AP377EX, OAW-AP375ATEX
OAW-AP500 Series	OAW-AP504, OAW-AP505
OAW-AP503 Series	OAW-AP503
OAW-AP500H Series	OAW-AP503H, OAW-AP503HR, OAW-AP505H, OAW-AP505HR
OAW-AP510 Series	OAW-AP514, OAW-AP515, OAW-AP518
OAW-AP518 Series	OAW-AP518
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577
OAW-AP580 Series	OAW-AP584, OAW-AP585, OAW-AP585EX, OAW-AP587, OAW-AP587EX
600 Series	AP-605H
OAW-AP610 Series	OAW-AP615
OAW-AP630 Series	AP-634, OAW-AP635
OAW-AP650 Series	AP-654, OAW-AP655
670 Series	AP-675, AP-675EX, AP-677, AP-677EX,AP-679, AP-679EX

Chapter 5
Regulatory Updates in AOS-W 8.12.0.0

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_89073

Chapter 6
Resolved Issues in AOS-W 8.12.0.0

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-147091	Some switches operating within the same VLAN experienced issues after a server was quarantined. The issue occurred due to the addition of a denylist flag on one of the switches, while the others continued to transmit packets from the auto-denylisted server. As a result, packets from the auto-denylisted server were dropped by the Mobility Conductor. The fix ensures the switches work as expected. This issue was observed in switches connected to an AirGroup server running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-156661 AOS-224890	The authentication survivability feature did not work as expected when the uplink was down. The fix ensures that the feature works as expected. This issue was observed in managed devices running AOS-W 8.2.2.2 or later versions.	AOS-W 8.2.2.2
AOS-208640	In some OAW-AP505 access points running AOS-W 8.7.1.0 or later versions, client devices experienced slow performance. This issue occurred when **HE MU-OFDMA** parameters were enabled. The fix ensures client devices perform as expected.	AOS-W 8.7.1.0
AOS-215875	The **show ap arm state** command displayed deprecated information such as Edge, Relevant Neighbors, Valid Neighbors, Neighbor Density, and Client Density. The fix ensures the **show ap arm state** command displays updated information. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-216536 AOS-220630	Some managed devices running AOS-W 8.5.0.11 or later versions were unable to come up on the Mobility Conductor. This issue occurred when the managed devices received the branch IP address as the switch IP address in a VPNC deployment. The fix ensures that the managed devices are able to come up on the Mobility Conductor.	AOS-W 8.5.0.11
AOS-218404	Some APs were unable to ping a few clients. The fix ensures that the APs are able to ping the clients. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-220903	The **s** flag indicating LACP striping was not displayed in the output of the **show ap database long** command even if LLDP was enabled on two uplinks. The fix ensures that the **show ap database long** command displays the s flag if LLDP was enabled on two uplinks. This issue was observed in APs running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-221982	Some VIA users experienced connectivity issues due to timeout. The issue was observed on IKEv2 EAP-GTC terminated VIA clients using external ClearPass Policy Manager along with an external proxy server configured for authentication. The fix increases the timeout for IKEv2 EAP-GTC connection formation. This issue was observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.10.0.0
AOS-227306	Some managed devices responded to the ARP probe frames with the SRC MAC address of the clients that were not connected to the network. The fix ensures that only intended managed device responds to the ARP probe frames with the SRC MAC address of the clients. This issue was observed in managed devices running AOS-W 8.7.1.5 or later versions.	AOS-W 8.7.1.5
AOS-227809	The process monitor options could not be disabled on the switches running AOS-W 8.6.0.14 or later versions. The fix ensures that the process monitor options can be disabled on the switches.	AOS-W 8.6.0.14
AOS-228357	Some standalone switches encountered a PSM WD with signature **psmdebug 0x01ff000d phydebug 0x21 macctl 0x4160403 maccmd 0x4**. The fix ensures the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-229190 AOS-248916	The **Dashboard > Overview > Clients** page of the WebUI did not display active and standby switch information. The fix ensures the data is displayed as expected. This issue was observed in Mobility Conductors running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-230427	Gateway backup on OmniVista 3600 Air Manager did not work for gateways running AOS-W 8.6.0.23. This issue occurred because OmniVista 3600 Air Manager did not support **ssh-rsa** host key algorithm, but the gateways supported only **ssh-rsa** as a client. The fix ensures that the gateway backup works as expected and support for **rsa-sha2-256** and **rsa-sha2-512** was reintroduced in OmniVista 3600 Air Manager.	AOS-W 8.6.0.23
AOS-231952 AOS-239896	Some access points crashed and rebooted unexpectedly. The log files listed the event as: **Firmware Assert - PC : 0x4b1ce6dc, whal_xmit.c:5664 Assertion 0 failedparam0**. The fix ensures the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-232527	Some users experienced issues when the deletion of an aged-out IPv4 address for a client inadvertently led to the deletion of all associated IPv6 addresses for the same client. This issue was observed when the **aaa user fast-age** command was enabled. The fix ensures that IPv6 addresses are not idled out when fast-age is enabled. This issue was observed on Mobility Conductors running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-232832 AOS-232962 AOS-233456 AOS-236010 AOS-236698 AOS-237445 AOS-240627 AOS-240765 AOS-241680 AOS-242454 AOS-242648 AOS-242649 AOS-242725 AOS-244622 AOS-245722	Some managed devices crashed and rebooted unexpectedly. The log files listed the reason of the event as, **Reboot Cause: soft Watchdog reset (Intent:cause:register de:86:70:4)**. The fix extracts additional data from the system at the time of the crash for further analysis. This issue was observed in managed devices running AOS-W 8.6.0.1 or later versions.	AOS-W 8.9.0.3
AOS-232875 AOS-239469	The **mon_serv** process crashed in specific high-load situations, especially when there were numerous APs and users with high roaming rates. The fix ensures switches work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-232970	The AP MAC address was not present in the calling station ID of the RADIUS accounting packets and hence, the RADIUS accounting requests were discarded. The fix ensures that the MAC address is present in the calling station ID. This issue was observed in managed devices running AOS-W 8.7.1.6 or later versions in a cluster setup.	AOS-W 8.7.1.6
AOS-233740	switches did not allow the deletion of system IPv6 address using the **no controller-ipv6** command. As a result, an error message was displayed stating **Controller-IPv6 cannot be removed. Please configure controller-ipv6 on some other valid vlan or the loopback**. The fix ensures switches work as expected. This issue was observed in switches running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0
AOS-233809	Users were unable to add GRE tunnels to a tunnel group when the tunnel is being referenced in Route ACL configuration. As a result, a misleading error message **Error: Tunnel is already part of a different tunnel-group** was displayed. The tunnel settings were not allowed to be modified when the tunnel was referred to in Route ACL configuration, and it displayed the above misleading error message. The fix ensures that the correct error message is displayed when GRE tunnels are added or modified, whether they are part of the tunnel-group or Route ACL configuration. This issue was observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-233941 AOS-239833	Some OAW-AP535, OAW-AP555, OAW-AP635 and OAW-AP655 access points were unable to send beacon packets using the Airgroup feature when multicast aggregation was enabled on the APs. The fix ensures APs can select one AP to forward MDNS packets to multiple VLANs. The issue was observed on APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-234480 AOS-238970	The **apflash ap31x-ap32x backup partition** command did not upgrade the backup partition of OAW-AP315 access points running AOS-W 8.7.1.9 or later versions in a cluster setup. The fix ensures that the command upgrades the backup partition of the APs.	AOS-W 8.7.1.9
AOS-234782	A few OAW-AP505H access points running AOS-W 8.10.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **skb double free detected!" at ("file-name/line-number/function-name") net/core/skbuff.c:1849/consume_skb()**. The fix ensures that the APs work as expected.	AOS-W 8.10.0.0
AOS-234823	A few Alcatel-Lucent OAW-4104 gateways failed to boot up during upgrade. The fix ensures that the gateways work as expected. This issue was observed in gateways running AOS-W 8.7.0.0.0 or later versions.	AOS-W 8.10.0.3
AOS-235242 AOS-235777	The **auth** process crashed and an error message, **auth module busy** was displayed. This issue occurred when the **show run** command was issued. The fix ensures that the users are able to issue the **show run** command. This issue was observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-235420	The numbers shown in **Rx Good Frames** and **Rx Frames Received** in the radio stats were the same in OAW-AP555. The fix ensures that the two stats work as expected. This issue was observed inOAW-AP555 running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1
AOS-235479	The commands **copy ftp** and **copy tftp** did not work as expected for the management interface. The fix ensures the commands 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-235744 AOS-235752	Some managed devices were unable to receive any configuration from the Mobility Conductor. This issue occurred when changes to a few group names were not synchronized on the standby Mobility Conductor before a reboot. The fix ensures that the managed devices receive configurations from the Mobility Conductor. This issue was observed in Mobility Conductors running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-235820	The **wms** process crashed on Mobility Conductors running AOS-W 8.10.0.2 or later versions. This issue occurred when the **wms** process exceeded the virtual memory limit of 2 GB. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.10.0.2
AOS-235893	Apple iPhone and Samsung phones were unable to associate to the wpa2-psk-aes and wpa2-psk-tkip mixed security mode. This issue occurred when the SSIDs were configured with WPA2-psk mixed mode. The fix ensures that Apple iPhone and Samsung phones are able to associate to the wpa2-psk-aes and wpa2-psk-tkip mixed security mode. This issue was observed in Mobility Conductors running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-236026 AOS-233809	Users were allowed to add GRE tunnels to an ACL, when the tunnel was part of a tunnel group. This could lead to unnecessary drop of traffic. The fix ensures GRE tunnels cannot be added to an ACL if they are already part of a tunnel group. This occurred since a tunnel in a tunnel-group can change its state from active to standby and if this tunnel is in a PBR ACL, then the traffic hitting the ACL will be dropped. This issue was observed in switches running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-236164	The **Dashboard** > **Infrastructure** page of the Mobility Conductor WebUI displayed an incorrect number of APs, as such duplicate APs were observed on the Mobility Conductor WebUI. The same issue was observed in the MON_SERV CLI. The fix ensures that the correct number of As is displayed in the WebUI and the MON_ SERV CLI. This issue was observed on Mobility Conductors running AOS-W 8.7.1.6 or later versions.	AOS-W 8.7.1.6
AOS-236174 AOS-236270	The SKBs in clients' AMPDU queue leaked when multi-clients roamed, and the heartbeats were missed due to lack of SKB. The fix ensures managed devices work as expected. This issue was observed in APs running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-236225 AOS-234379	Some OAW-AP630 Series and OAW-AP650 Series access points running AOS-W 8.9.0.1 or later versions experienced issues with the Draeger medical devices. The fix ensures that the APs work as expected.	AOS-W 8.9.0.1
AOS-236242	The **apmove** command did not work when the APs were connected to backup LMS controllers. The fix ensures that the users can use the **apmove** command as expected. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-236427	The license feature bits of a stand-alone switch were changed to enabled after restoring the flash backup. The fix ensures that the status of the license feature bits does not change after restoring the flash backup. This issue was observed in stand-alone switches / OAW-4010switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-236445 AOS-238079	Some users were unable to add or allocate licenses using the WebUI. The fix ensures that users are able to add or allocate licenses using the WebUI. This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-236471	Some standalone OAW-4740 Alcatel switches running AOS-W 8.0.0.0 or later versions did not show the configured banner information in the GUI login page. The fix ensures the banner is displayed in the GUI login page.	AOS-W 8.10.0.1
AOS-236503	The Cisco Firepower IPS dropped traffic between the dynamic IAP-VPN tunnels because of the detection of nonzero reserved bits in GRE header. The fix ensures the traffic is not dropped. This issue was observed in controllers running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-236721	The **Configuration > Roles & Policies > Roles** page of the WebUI did not display ACLs configured for the role. However, the CLI displayed the list of ACLs. The fix ensures the WebUI displays the expected information. This issue was observed in Mobility Conductors running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-236841 AOS-238400	The **Configuration > Services > Clusters >Add Controller** page of the WebUI did not display the list of **VRRP VLANs**. The fix ensures that the WebUI displays the list of VRRP VLANs. This issue was observed in managed devices running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-236852	The error log: **ofa: |ofa| ofa_gsm_ event_user_process: port not found:19, tnm50c4ddb3b194 end point is not configured or is down** was displayed when clients connected to an IAP-VPN tunnel. The fix ensures such error logs is not displayed. This issue was observed on Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-236880 AOS-236172	In some switches running AOS-W 8.6.0.18 or later versions, client devices were unable to connect to the 5 GHz band when scanning was enabled. After an AP reboot, some clients connected to the 5 GHz band for some hours, but later the issue recurred. This occurred because the AP tried to scan an unsupported channel. The fix ensures the AP does not scan unsupported channels so that client devices can connect to the 5 GHz band as expected.	AOS-W 8.6.0.18
AOS-236889 AOS-243540	Some managed devices running AOS-W 8.5.0.13 or later versions were unable to fetch user information through switch API calls. The **show user command** output often stated: **This operation can take a while depending on number of users. Please be patient** with no following response. The fix ensures the command works as expected.	AOS-W 8.5.0.13
AOS-237050	A few users experienced poor upstream network performance. Enhancements to the wireless driver resolved the issue. This issue was observed in APs running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-237052 AOS-208508 AOS-242671	The HTTP traffic of some users was incorrectly redirected by the captive portal. This issue occurred when the ACL changes were not updated on the APs. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.2 or later versions.	AOS-W 8.7.1.9
AOS-237113	High latency and jitter were observed on standalone switches running AOS-W 8.7.1.9 or later versions. The fix ensures that the standalone switches work as expected.	AOS-W 8.7.1.9
AOS-237203	Some stand-alone controllers with IAP-VPN tunnels generated multiple error logs. The fix ensures that the switches do not generate error logs. This issue was observed in stand-alone switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-237348	Some OAW-AP535 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 at whal_recv.c:1656 Assertion**. The fix ensures the APs work as expected.	AOS-W 8.9.0.3
AOS-237372	A few OAW-AP610 Series access points running AOS-W 8.11.0.0 or later versions used the 6 GHz radio to connect to Wi-Fi uplink although the 6 GHz radio was disabled using the **apboot** command. The fix ensures that the APs do not use the 6 GHz radio to connect to WiFi uplink when the 6 GHz radio is disabled.	AOS-W 8.11.0.0
AOS-237373 AOS-248873	The OAW-AP655 remote access point crashed unexpectedly when the PMTU value was set to 1200 or 1300 bytes. The log files listed the reason for the event as **PC is at skb_copy_and_csum_bits+0x24/0x274**. The fix ensures the AP works as expected. This issue was observed in OAW-AP655 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-237386	The **packetin_dispatcher** process crashed unexpectedly on Mobility Conductors running AOS-W 8.10.0.2 or later versions. The fix ensures that the Mobility Conductors work as expected.	AOS-W 8.10.0.2
AOS-237473 AOS-238104	The core files of the **nanny** process were not collected by the Mobility Conductor. The fix ensures that the Mobility Conductor collects the core files of the **nanny** process. This issue was observed in Mobility Conductor running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-237479	Some APs were unable to form standby tunnels with the cluster nodes. This issue occurred due to a race condition. The fix ensures the APs work as expected. This issue was observed in access points running AOS-W 8.7.1.7 or later versions.	AOS-W 8.7.1.7
AOS-237549	Some controllers were blocking EAPOL frames from passing to a wired RAP interface. The fix ensures the controllers work as expected. This issue was observed in mobility controllers running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-237710	During ARP discovery, devices with the same IP as the AP's default gateway caused the MAC address of the IP to be overwritten in the ARP cache, leading to unexpected rebootstrap processes. The fix ensures the ARP process is executed successfully and APs work as expected. This issue was observed in APs running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-237851	Some OAW-AP535 access points running AOS-W 8.10.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (phyrf_ani.c:718).** The fix ensures that the APs work as expected.	AOS-W 8.10.0.2
AOS-237931 AOS-242118 AOS-245405	A datapath crash was observed on Ubuntu 20_04 servers if the OS type was set to RHEL 7.2 or above. The fix ensures the servers work as expected. This issue was observed in virtual machines running on AOS-W 8.7.1.11 or later versions.	AOS-W 8.7.1.11

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-238103	Some OAW-AP635 access points were reporting high path loss values when compared to earlier models. The fix ensures the access points work as expected. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
AOS-238147 AOS-239823	Some APs powered up using PoE-AT incorrectly came up with **r** flag and were unable to broadcast SSIDs. The fix ensures that the APs work as expected and broadcast SSIDs. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.10
AOS-238150	Users connected through IAP-VPN were not listed in the SNMP table. The fix ensures users are listed in SNMP table as expected. This issue was observed in switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-238157	Some OAW-4750XM switches randomly rebooted with **Reboot Cause: Kernel Panic (Intent:cause:register)**. This issue occurred after upgrading to AOS-W 8.10.0.3 due to a memory corruption issue. The fix ensures controllers work as expected. This issue was observed on switches running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
AOS-238160 AOS-246310	Some access points running AOS-W 8.10.0.7 or later versions crashed and rebooted unexpectedly. The log files listed the reason of the event as **AP Reboot reason: BadPtr: 00000000 PC: anul_probe_req_find_by_mac+0x88/0x1d4 [anul] Warm-reset**. The fix ensures APs work as expected.	AOS-W 8.10.0.7
AOS-238205	Some 9240 switches running AOS-W 8.10.0.3 or later versions did not respond to the SNMP GET request to OID **WLSXSYSTEMEXT MIB::sysExtFanStatus**. The fix ensures that the controllers respond to the SNMP GET request.	AOS-W 8.10.0.3
AOS-238218 AOS-239882 AOS-241230 AOS-241971 AOS-242548	The mongo database took up a lot of flash space. The fix ensures that the Mobility Conductors work as expected. This issue was observed in Mobility Conductors running AOS-W 8.9.0.3 or later versions.	AOS-W 8.9.0.3
AOS-238298	Configuration changes that were made to the BLE UUID and the advertising interval parameters of the BLE service profile were not updated on the Mobility Conductor. The fix ensures that the changes are updated correctly on the Mobility Conductor. This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-238387	The authentication survivability feature did not work for EAP-TLS when the RADIUS server returned a username that was different from the Certificate Common Name (CN) during the normal authentication. The fix ensures that the authentication survivability feature works as expected. This issue was observed in managed devices running AOS-W 8.6.0.17.	AOS-W 8.6.0.17

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-238395 AOS-240213	The **profmgr** process was stuck in the **NOT_RESPONDING** state, and the standby Mobility Conductor was also stuck in the **CONFIG PROPAGATION** state. The fix ensures that the Mobility Conductor works as expected. This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.6.0.17
AOS-238407 AOS-236630 AOS-240428 AOS-241047 AOS-243539 AOS-249468	AppRF application or application category ACL did not block YouTube on devices connected to APs running AOS-W 8.6.0.16 or later versions. The fix ensures YouTube sessions are successfully terminated when needed.	AOS-W 8.6.0.16
AOS-238410 AOS-238939 AOS-238564 AOS-238487	The **httpd** process crashed on Mobility Conductors and managed devices running AOS-W 8.6.0.0 or later versions. This issue occurred when a specific type of cURL request was sent to the switches. The fix ensures that the managed devices and Mobility Conductors work as expected.	AOS-W 8.10.0.3
AOS-238424 AOS-247791	Some access points displayed the error, **file amon.c function amon_get_ant_gain line 4223 error invalid band 2**. The issue occurred when the 6 GHz radio band was disabled. The fix ensures the error is not displayed in such cases. This issue was observed in OAW-AP635 and OAW-AP655 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-238500	Some clients were unable to connect to a few APs. This issue occurred when the tunnel between the AP and the managed device in a cluster was down. This issue was observed in APs running AOS-W 8.7.1.9 or later versions. The fix ensures that clients are able to connect to access points as expected.	AOS-W 8.7.1.9
AOS-238519 AOS-240280	The BSS table of the OAW-RAP was reset unexpectedly. This issue occurred after a reboot of the Mobility Conductor. The fix ensures that the AP BSS table does not reset after a reboot of the Mobility Conductor. This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-238557	The SNMP MIB trap **wlsxUser6Table** returned incorrect values and did not increase the OID. The fix ensures the correct value is shown in the table. This issue was observed on OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-238578 AOS-238575 AOS-238576	The **halt** command did not save the audit-trail logs of the standalone switches. As a result, the **show audit-trail history** command did not display the configuration changes done before a reboot. The fix ensures the **halt** command saves the audit-trail logs of the switches. This issue was observed in standalone switches running AOS-W 8.10.0.3 or later versions.	AOS-W 8.10.0.3
AOS-238589 AOS-239319	The **impystart** process crashed on Mobility Conductor Virtual Appliances running AOS-W 8.10.0.2 or later versions. The fix ensures that the Mobility Conductor Virtual Appliances work as expected.	AOS-W 8.10.0.2

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-238600 AOS-239753	In some switches running AOS-W 8.11.0.0 or later versions, the logs were not displayed on the LCD during reload or halt. Information came up on the LCD after BIOS loaded. The fix ensures the logs are visible on the LCD as expected.	AOS-W 8.11.0.0
AOS-238604	The AP regulatory domain profile displayed different information in the WebUI and CLI. The fix ensures the WebUI and CLI display the same information. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.7
AOS-238648 AOS-250171 AOS-247454	The WebUI displayed incorrect Tx station throughput statistics for the client. The fix ensures statistics are accurately shown in the WebUI. This issue was observed in APs running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-238656	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Kernel panic - not syncing: Take care of the TARGET ASSERT first (ratectrl.c:999).** The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-238681	The RADIUS request access packets contained the IP address of the Mobility Conductor as the NAS IP address instead of the CoA VRRP IP address of the managed device. Hence, clients experienced connectivity issues. The fix ensures that the RADIUS request access packets contain the correct NAS IP address. This issue was observed in managed devices running AOS-W 8.9.0.1 or later versions in a cluster setup.	AOS-W 8.9.0.1
AOS-238708	Some AP-535 access points running AOS-W8.6.0.17 or later versions were showing very high interference. This may be causing the performance degradation of AP traffic with the client. The fix ensures that the AP performs as expected without showing very high interference.	AOS-W 8.6.0.17
AOS-238733	The network stack discarded Coordinator Realignment frames upon failed delivery attempts. A new protection mechanism has been implemented to ensure that Zigbee End Devices (ZEDs) are not removed from the network during orphaning. This issue was observed in access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-238768	The WebUI of Mobility Conductor running AOS-W 8.6.0.0 or later versions, displayed an incorrect count for the number of AP's and clients connected to it. This issue occurred after the Mobility Conductor was upgraded to AOS-W 8.10.0.2. The fix ensures that the WebUI of the Mobility Conductor displays the correct number of AP's and clients connected to it.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-238788	Meridian-configured BLE AP beacons were classified as unheard in the Meridian Editor UI when the software version was downgraded to 8.9.0.3. This issue occurred when the UUID was not added to the configured beacon's payload because of the BLE configuration of the AP. The fix ensures that the UUID is added to the payload of the configured beacon. This issue was observed in APs running AOS-W 8.9.0.3 or later versions.	AOS-W 8.9.0.3
AOS-238815	The modules of some APs appeared as **busy** when collecting system event logs making them unavailable. The fix ensures the system event logs are displayed as expected. This issue was observed on OAW-AP515 running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-238836	Clients that use machine and user authentication were unable to connect to SSID's. This issue was observed when WPA3 encryption was used. This issue was observed in APs running AOS-W 8.6.0.18 or later versions. This fix makes sure client authenticates successfully.	AOS-W 8.6.0.18
AOS-238846	The error message **Exceeds the max supported vlans 128** displayed when creating layer 2 VLANs at folder level. The issue was caused by matching strings in other paths being incorrectly included in the device bitmap. The fix ensures only the correct number of VLANs is taken into consideration for the VLAN count. This issue was observed in Mobility Conductors running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-238853	The health report sent to the Azure IoT Hub did not contain all the required information about the AP. The fix ensures that the health report contains the necessary information. This issue was observed in APs running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.2
AOS-238918	The **Configuration > IoT > Zigbee Services** page of the WebUI did not allow users to delete the Zigbee service profile. The fix ensures that users can delete the Zigbee service profile using the WebUI. This issue was observed in Mobility Conductors running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-238968	Some APs failed to send the IDS deauthentication frames even when the protect valid station parameter was enabled. This issue occurred when APs were connected in AM mode on 5 GHz channel. The fix ensures that the APs send the deauthentication frames when the valid station parameter is enabled. This issue was observed in OAW-AP515 and OAW-AP505 access points running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-239010	Some users experienced poor upstream network performance. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.2 or later versions. The fix ensures that the OAW-AP635 access points work as expected.	AOS-W 8.10.0.2

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-239130	The **TOTAL HIT** and **NEW HIT** information in the **Configuration > Authentication > User Rules > Rules-set** page of the WebUI displayed as **--**. However, the **show aaa derivation-rules user** command in the CLI displayed the information accurately. The fix ensures that the WebUI information matches with the CLI. This issue was observed in Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17
AOS-239183	In some switches running AOS-W 8.6.0.10 or later versions, the WebUI incorrectly displayed the daylight saving when configured for certain time zones, even after daylight saving was over. This fix ensures the correct time is displayed in the WebUI.	AOS-W 8.6.0.10
AOS-239202 AOS-240267 AOS-244650 AOS-245536	The **ble_daemon** process used high memory causing data packets to drop. This issue occurred when the BLE operation mode was enabled on the APs. The fix ensures the **ble_daemon** process works as expected. This issue was observed in APs running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-239238	The AP-provisioning process failed for some of the APs, preventing them from being configured properly. The fix ensures the process work as expected. This issue was observed in APs running AOS-W 8.10.0.1 or later versions.	AOS-W 8.10.0.1
AOS-239240	In some switches running AOS-W 8.10.0.6 or later versions, the **Telemetry Manager for Controllers** module was found to be busy after running the **show mgmt-server message-counters process tm** command. This behavior was observed at the time of running roam tests, during which, the management aspects stopped working. The fix ensures the switches perform as expected in this scenario.	AOS-W 8.10.0.6
AOS-239260	Some OAW-AP505 access points running AOS-W 8.6.0.18 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **BadPtr:00000294 PC:tun_recv_esp2_prep+0x10c/0x15c Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.18
AOS-239282	Clients were unable to connect to OAW-AP505H mesh access points. The log files listed the reason for this event as **UAC Down**. The fix ensures seamless connectivity. This issue was observed in OAW-AP505H mesh access points running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-239289	The output of the **show datapath cluster details** command displayed an incorrect time stamp. This issue occurred when the managed devices were up for more than 49 days. The fix ensures that the command displays the correct timestamp. This issue was observed in managed devices running AOS-W 8.10.0.2 or later versions in a cluster setup.	AOS-W 8.10.0.2

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-239324	In some OAW-AP535 access points running AOS-W 8.10.0.2 or later versions, users were unable to associate to neighboring APs, with deauthentication message **Reason Class 2 frames from non authenticated STA**. This issue was occurred in the 5GHz SSIDs. The fix ensures the APs perform as expected.	AOS-W 8.10.0.2
AOS-239341	Some OAW-AP345 access points running AOS-W 8.6.0.10 or later versions were detecting high channel utilization while there was none. This issue was due to the misinterpretation of the header information of ID duration frames. The fix ensures that the interpretation of duration frames is correct and APs work as expected.	AOS-W 8.6.0.10
AOS-239378	Some cluster nodes missed the cluster heartbeat from a different node. This caused both nodes to disconnect and isolate in a subcluster, creating an expected cluster split. The fix ensures that heartbeat misses do not derive in a cluster split. This issue was observed in managed devices running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239382	Some OAW-4750XM Mobility Conductors running AOS-W 8.7.1.9 or later versions configured in a cluster setup crashed and rebooted unexpectedly. The log files list the reason for the event as **Datapath timeout (SOS Assert)**. The fix ensures the Mobility Conductors work as expected.	AOS-W 8.7.1.9
AOS-239417	Some OAW-AP535 access points rebooted due a low memory condition. The log files listed the reason for the reboot as **kernel panic: softlockup: hung tasks**. The fix ensures memory is handled properly. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239452	Some OmniAccess Mobility Controllers reported the wrong AP BSSID when sending the **wlsxNAuthServerAcctTimedOut** SNMP trap. The fix ensures that OmniAccess Mobility Controllers report the correct BSSID when sending a server request timed out event. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-239459 AOS-248389	Mobility Conductors running AOS-W 8.10.0.7 or later versions continuously logged multiple unnecessary errors related to the **mon_serv_fwv process**. The logs pre-fixed the errors as **|mon_serv_fwv| mon_serv_gsm_handle_device_config_add**. The fix ensures these unnecessary logs are not displayed in the CLI.	AOS-W 8.10.0.7
AOS-239472 AOS-242785	The **show loginsessions** command displayed multiple entries with empty **User Name** and **User Role**. This issue also caused the SSH process to fail. This issue occurred because the CLI processes from previous sessions were still active in the background. The fix ensures such sessions are timed out accordingly, discarding empty entries in the **show loginsessions** command and resolving issues with the SSH process. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-239487	The PCAP files of some APs were incorrectly sent to the default folder of the dump server and not to the user-defined folder. This issue was caused due to the defined dump-server settings not being honoured. The fix ensures that the PCAP files are sent following all the user-defined dump-server settings and will use SCP if that is what has been configured. This issue was observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239492	APs were rebooting randomly. The log file listed the reason for the event as **Reboot Time and Cause: AP rebooted Tue Oct 11 21:49:53 CEST 2022; Critical process /aruba/bin/sapd [pid 32165] DIED, process marked as RESTART**. The fix ensures that the APs work as expected. This issue was observed in access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-239521	Users were unable to add a tunnel to a tunnel group and an error message **Error: All tunnels must have same vlan membership** was displayed. This issue occurred when the VLANs were configured in a different order when compared to the order configured for other tunnels in the same group. The fix tunnel additions to tunnel groups work as expected. This issue was observed in managed devices running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-239623	The output of the **show ap ble-ibeacon-info** command displayed an incorrect **APB Radio BLE Operational TxPower**. The fix ensures that the command displays the correct operational Tx power. This issue was observed in APs running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.4
AOS-239643 AOS-237332	The **show running-config** command displayed zero IPv6 interfaces for layer 3 VLANS instead of 128. An increase in the amapi buffer size ensures the command displays the expected number of IPv6 interfaces, which is 128 for L3 VLANS. The issue was observed in stand-alone controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-239653	After disconnecting from a wireless AP using 802.1x secured SSID, some clients were not logged out of the Palo Alto firewall. If the same client tried to connect again with a different username, it caused the controller to not logout the previous username and did not ask for a login for the new username. This caused the firewall not to update host information nor associate with correct firewall policy. The fix ensures the switches work as expected. This issue was observed in switches running AOS-W 8.9.0.3 or later versions.	AOS-W 8.9.0.3
AOS-239662	Some clients experienced issues with audio transmission during Skype and Microsoft Teams calls. The fix ensures that the clients do not experience issues with audio transmission. This issue was observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-239810	The **Dashboard** > **Overview** > **Clients**, **Channel Health Status** page of the WebUI was displayed intermittently as **Unknown**. The fix ensures WebUI displays the correct health status. This issue was observed in Mobility Conductor running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-239821 AOS-243932	The output of the **show running-config** command displayed with no left indentations. The fix ensures that the command output is displayed as expected. This issue was observed in switches running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-239850 AOS-249756	Some Mobility Conductors crashed unexpectedly due to a memory leak in the **vmsvc** process. The log files listed the reason as **[vmsvc] HostinfoOSData: Error: no distro file found**. The fix ensures the Mobility Conductors work 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-239872	WebUI did not allow users to live upgrade a cluster. However, the CLI allowed users to upgrade to a cluster. This issue occurred when the name of the cluster contained spaces. The fix ensures that users are allowed to live upgrade a cluster through the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-240014	In some switches running AOS-W 8.7.1.4 or later versions, an invalid AP console password was displayed in the AP System profile. This issue was caused by an incorrect password string length. This fix ensures only valid passwords can be set.	AOS-W 8.7.1.4
AOS-240026 AOS-236177 AOS-239232 AOS-240068 AOS-240633	Some customers were unable to access switches through the CLI or WebUI. This issue was related to third-party monitoring tools such as Armis, which caused the CLI sessions to be kept open for a long time accumulating memory leaks, affecting the functioning of the controller. The fix ensures customers are able to access controllers as expected. This issue was observed in controllers running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-240032	In some OAW-4850 switches, the Auth process crashed when RadSec functionality was disabled for a sever. The fix ensures the switches perform as expected in this scenario. This issue was observed in controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-240057	The uplink VLAN did not work as expected. This issue occurred when an OAW-IAP was converted to a OAW-RAP. The fix ensures that the uplink VLAN works as expected. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240185	Clients were unable to obtain user roles from ClearPass Policy Manager and fell into their initial role. This issue occurred due to radius accounting. This issue was observed in managed devices running AOS-W 8.7.1.10 or later versions. The fix ensures that clients can obtain their accurate user roles from CPPM.	AOS-W 8.7.1.10

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-240199	Users were unable to establish connection with managed devices using the **mdconnect** and **logon** commands. The fix ensures that the commands work as expected. This issue was observed in managed devices running AOS-W 8.7.1.11 or later versions.	AOS-W 8.7.1.11
AOS-240211	After a Radar detection in a particular channel, the ARM feature caused access points to return to the original channel, ignoring the 30-minute backoff period that is required after a radar detection which led beacons not being transmitted. The fix ensures the APs works as expected and does not return to Radar affected channel until 30 min. This issue was observed in OAW-AP535 running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-240240 AOS-245463 AOS-243291	The output of the **show ap radio-database** command did not display the correct information in the topology of Mobility Conductors and managed devices. The fix ensures the command displays the expected information. This issue was observed in Mobility Conductors and managed devices running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240279	Mobility Conductors running AOS-W 8.10.0.4 or later versions pushed additional IGMP and OSPF configurations to managed devices. This issue occurred when a VLAN configuration was edited. The fix ensures that additional configurations are not sent and Mobility Conductors work as expected.	AOS-W 8.10.0.4
AOS-240300	AirMatch assigned incorrect power levels to OAW-AP277 access points running AOS-W 8.10.0.4 or later versions. The fix ensures that AirMatch assigns correct power levels for APs.	AOS-W 8.10.0.4
AOS-240312	The **arci-cli-helper** process crashed on OAW-4750XM switches running AOS-W 8.7.1.10 or later versions. This generated crash files, but the switch did not reboot. The fix ensures that this process works as expected.	AOS-W 8.7.1.10
AOS-240347	Users were unable to collect the tech support logs of the Mobility Conductor. The fix ensures that the tech support logs of the Mobility Conductor are available for the users. This issue was observed in Mobility Conductors running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240371	The 802.1X authentication failed for a few clients. This issue occurred when OAW-AP635 access points were configured as OAW-RAPs. The fix ensures successful authentication. This issue was observed in OAW-AP635 access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240419	Packet loss was observed when sending traffic over a network secured using WPA3 and CNSA. This issue occurred when downloading files from a SMB server in a PC running Windows 10. This issue was observed in OAW-AP505 access points running AOS-W 8.10.0.5 or later versions. The fix ensures the APs work as expected.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-240425	The HTTPS connection was interrupted and the ICMP communication was blocked for some VIA clients. This issue occurred when, ■ the default size of 1452 bytes was used for MTU ■ the DF bit was set for IP packets This issue was observed in controllers running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-240433	The **ISAKMPD process** crashed with VIA clients terminated using DHCP servers for internal IP allocation. The fix ensures that the ISAKMPD process work as expected. The issue was observed in standalone OAW-4030 controllers running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240435	Some APs sent random false alerts to the OmniVista 3600 Air Manager monitor to display their status as **Down** while remaining **Active** on the controller. The fix ensures the APs send only correct alerts to OmniVista 3600 Air Manager. This issue was observed in OAW-AP303H access points running AOS-W 8.7.1.10 or later versions.	AOS-W 8.10.0.6
AOS-240561	Some APs unexpectedly showed an error: **MDIO Error: MDIO got failure status on phy 30**. A regulation of the clock frequency solved the issue. The fix ensures the APs work as expected. This issue was observed in OAW-AP505H and OAW-AP503H running AOS-W 8.7.1.10 or later versions.	AOS-W 8.7.1.10
AOS-240568 AOS-244716	In some switches, saving the tunnel configuration took longer than expected. The fix ensures the switches perform as expected. This issue was observed in standby switches running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-240601	In some OAW-AP500 Series access points running AOS-W 8.10.0.2 or later versions, the Scheduler Algorithm caused a delay, which introduced latency in the MU schedule for multiple clients. This fix ensures the algorithm works as expected.	AOS-W 8.10.0.2
AOS-240646	The output of the **show ap ble_ibeacon_info** command did not display the name of the AP. This issue was observed in Mobility Conductors running AOS-W 8.10.0.2 or later versions. The fix ensures the command displays the AP name.	AOS-W 8.10.0.2
AOS-240653	The size of **/mswitch/logs/fpapps.log** file increased indefinitely by 40 MB per month, consuming unnecessary memory resources. The fix ensures the log files are handled as expected. This issue was observed in standalone controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-240740	Some OAW-AP635 access points running AOS-W 8.10.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures the APs work as expected.	AOS-W 8.10.0.4

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-240772 AOS-240775 AOS-242483	The STM component failed on switches causing them to crash. The fix ensures the STM component works as expected. This issue was observed on controllers running AOS-W 8.10.02 or later versions.	AOS-W 8.10.0.2
AOS-240858	In some OAW-AP303H Series remote access points, cellular IP was not obtained, since it could not create an IPSEC tunnel with the controller. This made the RAP not to come up. This issue was observed in devices running AOS-W 8.10.0.5 or later versions. This fix ensures the OAW-RAP3 Series comes up as expected in this environment.	AOS-W 8.10.0.5
AOS-240920 AOS-242753	The **fpapps** process crashed randomly when querying an ifMIB OID with unknown index value using SNMP. The fix ensures **fpapps** does not crash when an invalid index value is used. This issue was observed on Mobility Conductors running AOS-W 8.9.0.3 or later versions.	AOS-W 8.9.0.3
AOS-240931	Ascom i62/i63 VoIP phones experienced connectivity issues in the form of low-quality audio output when connected to OAW-AP515 access points running AOS-W 8.10.0.4 or later versions. The issue was related to compatibility with a Broadcom patch. The fix ensures Ascom devices output the expected quality audio.	AOS-W 8.10.0.4
AOS-240953	Some OAW-AP635 access points failed to send data frames when configured in tunnel mode using opmode wpa3-sae-aes encryption. The clients were also unable to get an IP address. This issue was caused by PMF drop when the **Prohibit IP Spoofing** policy was enabled. The fix ensures APs on opmode wpa3-sae-aes or tunnel mode work as expected. This issue was observed on APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-240954	Some OAW-AP555 access points running AOS-W 8.10.0.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.10.0.5
AOS-240991	In some switches running AOS-W 8.11.0.0 or later versions, it was not possible to deploy MC-VA-50 using an OAW .iso image. The fix ensures the installation of AOS-W successfully completes in this scenario.	AOS-W 8.11.0.0
AOS-240995	Few switches processed the routes in the routing table incorrectly. This issue occurred when the **Allow-via-subnet-routes** feature was enabled using the **crypto-local isakmp** command. This issue was observed in switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-241083 AOS-242823	Some access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **ar_wal_tx_de.c:331 Assertion failed**. The issue was related to the AP image version found in previous versions of AOS-W. The fix contains a patch for the AP image that resolves the error. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-241086	Some clients were unable to connect to the controller due to crashes of the auth_mgr process after upgrading from AOS-W 8.6.0.7 to AOS-W 8.10.0.5 or later versions. The fix ensures the clients can connect as expected.	AOS-W 8.10.0.5
AOS-241088	In the WebUI **Dashboard > Infrastructure > Access Points**, the status of the APs appeared to be in an incorrect state when checked from the Mobility Controller. The fix ensures the status is accurate in the WebUI. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241120	Personal registered device was visible to all users even when no username was specified in the CPPM configured policy. The fix ensures the personal registered device is visible to only the owner and the specified intended users. This issue was observed in managed devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241158	The running configuration did not match the previous configuration after upgrading from 6.5.x to 8.x versions. The fix ensures that previous configurations are retained when upgrading to 8.x versions. This issue was observed in standalone OAW-4010 controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.19
AOS-241160	Some OAW-AP535 access points running AOS-W 8.10.0.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Kernel panic: "Fatal exception in interrupt" and "Take care of the TARGET ASSERT first"**. The fix ensures the APs work as expected.	AOS-W 8.10.0.5
AOS-241212 AOS-241537	Some OAW-4650 switches running AOS-W 8.10.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Nanny rebooted machine - low on free memory**. The fix ensures the switches perform as expected.	AOS-W 8.10.0.4
AOS-241228	In some standby controllers the **disable allowlist-sync** command was executed, causing the controllers to enter a CONFIG_FAILURE state. This command is intended for primary controllers only. This issue was observed in controllers running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-241256	The **Global User-Table** record displayed the MAC addresses of some clients to be associated with multiple APs. The fix ensures the correct information is displayed. The issue was observed in Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.5
AOS-241313	Zebra TC21 barcode scanners were unable to maintain a connection and send traffic when connected to OAW-AP505 devices running AOS-W 8.10.0.5 or later versions. The fix ensures TC21 barcode scanners can successfully connect to APs and pass traffic as intended.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-241325	In some switches running AOS-W 8.6.0.0 or later versions, the **Beacon Period** in the **Configuration > System > Profiles > RF Management** section in the WebUI, and the **show rf dot11a-radio-profile** command in the CLI was displayed as 100 msec. Instead, the **Beacon Period** should be expressed as 100 time units or 102.4 msec. The fix ensures that the **Beacon Period** value and units are displayed correctly.	AOS-W 8.6.0.0
AOS-241364	The output of the show **audit-trail | include admin** command displayed, **COMMAND: – command execution failed** repeatedly. The fix ensures the output of the command does not display the error for "show switches" anymore. This issue was observed in s running AOS-W 8.10.0.2 or later versions.	AOS-W 8.10.0.2
AOS-241434	The **show running-config** command could not be executed and displayed an **error Module DHCP Daemon is busy. Please try later**. The fix ensures the **show running-config** command works as expected. This issue was observed on mobility controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-241438	A case sensitive check was performed when the following commands were executed in the CLI: ▪ **show global-user-table list name <username>** ▪ **show global-user-table list role <role name>** ▪ **show global-user-table count ap-name <name>** This prevented users from getting accurate search results for usernames or APs. The fix ensures the command works for case sensitive inputs as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.5
AOS-241464 AOS-242568	Some OAW-AP535, OAW-AP555, OAW-AP585, OAW-AP635, and OAW-AP655 access points crashed and rebooted unexpectedly. The log files listed the event as, **kernel panic: Fatal exception, PC is at nss_ipsecmgr_sa_add_sync+0x4c/0x400 [qca_nss_ipsecmgr]**. The fix ensures the APs work as expected. The issue was observed in APs running AOS-W 8.10.0.4 or later versions in a cluster setup.	AOS-W 8.10.0.4
AOS-241497	Some OAW-AP275 access points running AOS-W 8.10.0.5 or later versions interconnected in a mesh topology crashed and rebooted unexpectedly. The log files recorded the event as, **Process /aruba/bin/sapd has too many open files**. The issue occurred when the AP sockets remained in open state even if they were already allocated. The fix ensures the APs work as intended.	AOS-W 8.10.0.5
AOS-241498 AOS-245217	A corrupt bridge ACL issue was observed in APs running AOS-W 8.10.0.5 or later versions, where some user roles were either missing or contained a duplicate of the **logon** role. This issue occurred when the AP failed over to a controller with a different ACL configuration, preventing the AP from passing traffic. The fix ensures APs work as expected.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-241532 AOS-245370	Some Mobility Conductors repeatedly displayed the error message, **WMS PGRES_FATAL_ERROR**, which filled the logs. The fix ensures that the devices operate as expected. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241550	Multiple AP-535 access points crashed unexpectedly with Kernel panic error. The log files listed the reason for the event as: **Kernel panic - not syncing: Take care of the TARGET ASSERT at ru_allocator.c:3166 Assertion (((rt_tbl))->info[((rix))].phy == WHAL_MOD_IEEE80211_T_HE_20**. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0
AOS-241560	Accessing switches through the WebUI lead to excessive logs regarding the **show uplink cellular details** command, including errors stating **Command not applicable for this platform (pos: 0)**, which can be safely ignored. The fix ensures that only the desirable logs are generated. This issue was observed in standalone OAW-4650Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241669	A session established with a guest SSID did not disconnect even after the session timeout. The fix ensures no connections are allowed to users when their session times out. This issue was observed in some controllers running AOS-W 8.6.0.9 connected through split-tunnel.	AOS-W 8.6.0.9
AOS-241709	The **auth** process crashed unexpectedly when ACLs and downloadable-user roles assigned to a VIA client were configured from CPPM. The fix ensures the controller works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.5
AOS-241737	The **RADIUS User-Name** attribute contained an empty value in the RADIUS Accounting-Stop packet when an authenticated Captive-Portal client clicked the logout button. The fix ensures the User-Name attribute contains user-name value in the RADIUS Accounting-Stop packet. This issue was observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-241801	Some 802.11r client devices running AOS-W 8.10.0.4 or later versions were unable to FT-roam. This issue was related to the PTKSA/GTKSA ReplayCounters in RSNE mismatching with the same in Probe-Response/Beacon packets. The fix ensures that 802.11r client devices are able to roam as expected.	AOS-W 8.10.0.4
AOS-241833	OAW-RAPs operating in a dual-stack environment with an IPv4 IPSEC experienced heartbeat loss after IPSEC re-key when IPv6 was inadvertently used. The fix ensures no heartbeat misses are seen on RAPs when IPSEC re-keying happens. The issue was seen on Remote OAW-AP505H access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-241841	Some OmniAccess Mobility Controllers were unable to ping their default gateway and display neighbor entries when using IPv6. The fix ensures the process works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241863	The ACL was incomplete in the SAPD and data path modules, and it caused connectivity issues. The fix ensures that the process works as expected. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241870	The **Dashboard > Infrastructure** page displayed APs as **Down** even after being cleared by executing the **clear gap-db ap-name** command. The fix ensures the WebUI displays the expected information. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-241898	The **Configuration > WLANs > VLANs** section of the WebUI did not reflect changes made to the VLAN. This issue was observed in controllers running AOS-W 8.10.0.5 or later versions. The fix ensures that the WebUI reflects the VLAN changes correctly.	AOS-W 8.10.0.5
AOS-241937	A few user-based tunnelled users failed to come up on managed devices due to certain race condition in the sequence of events during the user bootstrap process. This issue was observed in managed devices running AOS-W 8.10.0.2 or later versions. The fix ensures user-based tunneling works as expected.	AOS-W 8.10.0.2
AOS-241957	The WebUI required specifying a category when adding a logging server in **Configuration > System > Logging**. This should not be mandatory for logging server configuration. Thus, the fix excludes this requirement from the WebUI and allows users to add a logging server without a category. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242003	Moving files from OmniAccess Mobility Controllers to FTP using API POST caused the error: **/mm/mynode" COMMAND: --command execution failed**. The issue was fixed by adding a missing parameter in the UI mapping table. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-242013	Some VIA clients were not able to establish tunnels with controllers as the datapath tunnel table reached maximum capacity. The fix ensures that the tunnel entries are created and deleted properly in datapath tunnel table. This issue was observed on running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-242139	In some switches, there was a mismatch with the **g-basic-rates** and **g-tx-rates** values after users made changes to the SSID profile. The output of the **show configuration effective** command showed the expected values, but the output of the **show wlan ssid-profile** and **show running-config** commands did not. The fix ensures that the values are populated as expected. This issue was observed in controllers running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-242243 AOS-234945	After upgrading to AOS-W 8.12.0.0-FIPS, the virtual OmniAccess Mobility Controller crashed unexpectedly. The log files listed the reason for the crash as **rte_eth_tx_burst**. This occurred because the NIC driver received packets with a port number that was out of range. The fix ensures that valid port numbers are used. This issue was observed in virtual OmniAccess Mobility Controllers running AOS-W 8.12.0.0-FIPS.	AOS-W 8.7.1.8
AOS-242404	The reason and timestamp of APs in a **DOWN** status was not displayed in the Mobility Conductor dashboard under **Infrastructure > Access Devices**. The information displayed was **AP is down since - because of the following reason: None**, or similar. The fix ensures the correct data is displayed in the WebUI. This issue was observed in AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-242429 AOS-248682	Some switches failed after a system upgrade from AOS-W 6.5.x to 8.7.1.4 or later versions. Upon reboot, the error **Failed to set port as trusted, err=Module Process handling LAG and LACP functionality is busy. Please try later** was displayed. The fix ensures this error is no longer displayed. This issue was observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.10.0.7
AOS-242477 AOS-247390	**Rx Total Control frames Recvd** statistics were incorrectly displayed in the CLI. The fix ensures the statistics are displayed correctly. This issue was observed in OAW-AP300 Series, OAW-AP500 Series and 600 Series APs running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-242532	Some OAW-AP535 access points were not available on OAW-4550switches post power outage. This issue occurred when a USB converter and console cable were used, which interrupts the boot up process and results in the AP not showing up on the switch. The fix the ensures access are available in this scenario. The issue was observed in switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-242651	In some APs running AOS-W 8.10.0.6 or later versions, an issue was observed where all ZigBee ZED were off the APs client-table when pairing more than 12 ZEDs. The fix ensures the right number of ZED devices can be paired without issues.	AOS-W 8.10.0.6
AOS-242759	In some devices using curl, the **endpointURL** parameter was not configured in the IoT radio profile for ASSA ABLOY. This caused memory leaks in the Bluetooth Low Energy (BLE) relay process. The fix ensures that the connection using curl works as expected. This issue was observed in AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-242852	In some switches running AOS-W 8.10.0.4 or later versions, tunneled_user creation failed upon a bridge miss. This fix ensures tunneled_user is created, even if bridge miss happens.	AOS-W 8.10.0.4
AOS-242962 AOS-244935 AOS-245697 AOS-246559 AOS-248871 AOS-248913	Some APs randomly went offline and did not come up on the switch. The logs displayed the error **MMC init failed**. The issue was related to the eMMC flash memory of the AP entering an abnormal state. The fix improves the internal timing of the flash memory to ensure that the AP does not crash. This issue was observed on OAW-AP635 and OAW-AP655 access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-242970	When running the **clear gap-db ap-name** and **clear gap-db wired-mac** commands from a Mobility Conductor, the state AP records were not cleared down on Managed Devices. As a result, stale AP records were still observed in Managed Devices. The fix ensures the stale AP records are deleted as expected after running these commands. However, if needed, run the **clear gap-db stale-ap ap-name <ap-name> lms lms-ip <lms-ip>** command to clear the a stale entry on a particular Managed device. This issue was observed in Mobility Conductors running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-243033	In some switches, the associated access points randomly disconnected. This issue occurred in a cluster setup with the **Bypass** function enabled where the AP would not try to re-authenticate. The tunnel to **Active AP Anchor Controller** was maintained, but the tunnel to the **Standby Active AP Anchor Controller** was dropped. This caused that the client devices were unable to pass traffic. The fix ensures **dot1x** authentication is restored in this scenario. This issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-243064	Some OAW-AP535 access points crashed unexpectedly. The log files listed the reason as: **Reboot caused by kernel panic: Take care of the TARGET ASSERT first:Excep :0 Exception detectedparam0 :zero, param1 :zero, param2 :zero**. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.6 or later versions. The fix ensures that APs work as expected.	AOS-W 8.10.0.6
AOS-243162	Controllers restricted to Egypt did not display the country code in the output of the **show version** command. The fix ensures the correct information is displayed. This issue was observed in controllers running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-243222	The **Auth** module crashed on managed devices. The issue occurred due to insufficient memory allocated to the devices in a 6 node cluster and AP/client scale. The fix ensures the **Auth** module works as expected. This issue was observed in 9240 Series devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-243265	Some OAW-AP515 access points running AOS-W 8.10.0.5 or later versions unexpectedly generated AP panic dump files. The log files listed the reason for the event as: **Unable to handle kernel NULL pointer dereference at virtual address 00000014**. The fix ensures that NULL values are handled correctly, and the AP performs as expected.	AOS-W 8.10.0.5
AOS-243266	In some OAW-4650 switches, APs upgraded through TFTP were stuck in **Upgrading** status due to an incorrect automatic change of UDP ports. The fix ensures the APs perform as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.17
AOS-243338	Some APs were randomly shutting down due to IKEv2 exchange timeout. The fix ensures the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-243338	Some APs were randomly shutting down due to IKEv2 exchange timeout. The fix ensures the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-243442	Some managed devices unexpectedly displayed an error message for WLAN users. The log files listed the reason as: **INVAL_HDR_ HDR_TYPE: arp [25316] Found incorrect hardware type in ARP header: 256**. A correction of the endian sequence solved the issue. This issue was observed in x86 based platforms (OAW-41xx Series Controllers, 9200 Series Controllers, and VMCs) running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.5
AOS-243536	Some OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions displayed incorrect values in **Discovery State** and **Transport State** for AirGroup services, after running the **show airgroup switches** command. This occurred due to a race condition. Therefore, users connected to the affected APs were unable to use AirGroup services. The fix ensures the correct values are displayed.	AOS-W 8.10.0.6
AOS-243720	The WebUI did not display the correct output for the **show wms ap list** and **show wms rogue-ap list** commands. The fix ensures that the correct information is displayed in the WebUI. This issue was observed in Mobility Conductors running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-243787	Some switches running AOS-W 8.0.0.0 or later versions randomly became unstable during high peak hours. This issue was caused due to CPU high utilization. The fix ensures the controllers perform as expected.	AOS-W 8.12.0.0
AOS-244165	OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions included spurious messages stating **TOKEN WAS ABSENT** as error logs. These messages were intended to appear as debug logs, not error logs. The fix ensures these messages do not come up in error logs anymore, but instead are included in debugging logs.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-244167	OmniAccess Mobility Controllers incorrectly sent ACK messages in response to RFC-5176 Disconnect-Message Requests when in Bridge Mode, which is not supported. The fix ensures that no ACK messages for RFC-5176 are sent. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244210	Users were unable to configure a negative value for the transmit power setting in the **Overview > Profiles > IoT Profile > BLE Transmit Power** page of the WebUI. The fix ensures negative values can be configured through the WebUI. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244218 AOS-245833 AOS-247849 AOS-249157 AOS-249570	Some APs crashed and rebooted due to a memory allocation failure for the trigger frame, which dropped the connection. The fix ensures APs work as expected. This issue was observed in APs running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0
AOS-244231	Option 82 information was missing for the first DHCP discover packet in some switches running AOS-W 8.11.0.0 or later versions. The fix ensures the option 82 information is tagged correctly in the first DHCP discover packet.	AOS-W 8.11.0.1
AOS-244247	The value for **attack-rate tcp-syn <#>** could not be set over 255, and the clients could not be blacklisted. The fix ensures the value can be set over 255. This issue is observed in controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-244264	Some access points crashed unexpectedly. The issue occurred due to high memory utilization causing users to be unable to obtain IP addresses or associate the APs with SSIDs. The fix ensures no memory leaks occur while BLE transport profile is trying to connect to external servers. This issue was observed in OAW-AP345 access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244284	Some controllers running AOS-W 8.10.0.0 or later versions were dropping incoming encrypted AESCCM data packets from client devices due to the following reason – **Invalid Replay Counter**. The fix ensures that the packets are not dropped even if the Replay Counter is found to be invalid. The controller will keep a count of the number of packets where this error is seen.	AOS-W 8.10.0.0
AOS-244321	Some RADIUS server users were unable to connect to Passpoint due to an **Exhausted reqids** error. The fix ensures switches work as expected. This issue was observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244358	Under **Dashboard** > **Overview** > **Clients** > **Name**, the SSID of the clients incorrectly displayed the IP or the MAC address. The fix ensures the SSID displays correctly. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-244373	Some OAW-AP377 access points provisioned as a mesh point with **opmode open-system** intermittently lost connectivity to the controller within an hour. The fix ensures the access points work as expected. This issue was observed in access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244384	The Windows 10 Filesharing (SMBv2) download speed was slower when connected to OAW-AP515 access points or 9240 controllers compared to other devices. The fix ensures an improvement in download speeds. This issue was observed in OAW-AP515 access points and 9240 controllers running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-244398 AOS-244429 AOS-244743 AOS-244767 AOS-246357 AOS-247460	The **amon udp** command was used to enable OmniVista 3600 Air Manager to allow traffic on UDP port 8211. Due to a security change, PAPI drops some AMON feeds between the Mobility Conductor and managed devices. This issue is resolved after deprecating the **amon udp** command. This issue was observed in switches running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-244436	Some APs running AOS-W 8.9.0.3 and configured with a valid BSSID were incorrectly identified as rogue APs. After upgrading to AOS-W 8.10.0.6, IDS incorrectly reported AP impersonation events for valid BSSIDs. The fix ensures no false positives are reported by IDS. This issue was observed in APs running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244467 AOS-245304	A high volume of AMON messages was detected in a few days. This issue occurred after BLE service profile deployment. The fix ensures a reduced amount of AMON messages. This issue was observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244576	The datapath route-cache information for L3 GRE tunnels was lost unexpectedly. This was caused as the IPSec tunnel pointed to the wrong IP address whenever it went down and re-established itself, causing uplink issues on the network. The fix ensures uplink works as expected. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-244628	Some access points were unable to upgrade using the **apflash ap31x-ap32x backup partition** command. The fix ensures the command works as expected. This issue was observed in OAW-AP315 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-244659	Some clients experienced unexpected issues while roaming when using the OpenFlow protocol. The fix ensures OpenFlow works as expected and causes no issues. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-244664	Dual-stack managed devices with IPv6 cluster and IPv4 APs did not pass traffic after cluster failover when the AAC uplink was shut down on two-node clusters. The fix ensures devices pass traffic as expected under this scenario. This issue was observed on APs running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-244736	Some OmniAccess Mobility Controllers using UBT feature were incorrectly forwarding unicast traffic to other UBT tunnels. The fix ensures the feature works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.6
AOS-244800 AOS-244803 AOS-245378	Some OmniAccess Mobility Controllers crashed unexpectedly. The log files listed the reason as: **Reboot Cause: Kernel Panic (Intent:cause:register12:86:b0:4)**. The fix ensures the controllers work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21
AOS-244855	The output of the **show airmatch optimization** command returned no information when there are more than 200 optimization records in database. The fix ensures the command works as expected. This issue was observed in Mobility Conductors running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.6
AOS-244869	In some access points the 4-way handshake failed when WPA2 key-2 frames were re-transmitted by wireless client. The fix ensures the 4-way handshake process works as expected. This issue was observed in access points running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-244949 AOS-246630	Some APs crashed and rebooted due to mismatch in **Pending twt sessions** count and **current twt session** issues. This fix will count the number of **pending twt sessions** properly so that mismatch does not occur during WMI event send instance. This fix ensures the APs perform as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.6 and 8.11.1 or later versions.	AOS-W 8.10.0.6
AOS-244949 AOS-249560	Some APs crashed and rebooted due to a mismatch in **Pending twt sessions** count and **current twt session** issues. This fix will count the number of **pending twt sessions** properly so that mismatch does not occur during WMI event-send instance. This fix ensures that the APs perform as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-244965	An unnecessary debugging log appeared as **Received ICMP (DEST_UNREACH, PROT_UNREACH) from X.X.X.X for heartbeat tunnel**. The fix deletes this unnecessary log. This issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-245001	The **wired aaa-profile** configuration disappeared after the managed device restarted due to incorrect case sensitive checks. The fix ensures that the **wired aaa-profile** configuration is retained when the device restarts. This issue was observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245011	After upgrading to AOS-W 8.10.0.6, systems experienced periodic WebSocket disconnections every 5 minutes when transmitting BLE telemetry data to third-party servers. The issue was especially prevalent at a data reporting interval of 3 seconds, where certain telemetry updates were missing due to packet drops. The fix ensures WebSocket stability, reducing disconnections during high packet loss scenarios. This issue was observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245033	Clients experienced low download and upload speeds when connected to OAW-AP615 access points running AOS-W 8.11.0.0-FIPS or later versions. This issue was related to the AP image in FIPS versions of AOS-W. The fix updates the AP image and ensures APs work as expected.	AOS-W 8.11.0.0-FIPS
AOS-245034	Some switches running AOS-W 8.10.0.5 or later versions crashed unexpectedly due to a memory leak issue of the **FPAPPS** process. The fix ensures controllers work as expected.	AOS-W 8.10.0.5
AOS-245050	In the WebUI, **Dashboard** > **Infrastructure** > **Model**, some managed devices displayed their name without the prefix **AP**. The fix ensures the names are displayed correctly. This issue was observed in Access Points running AOS-W 8.6.0.20 or later versions in a cluster configuration.	AOS-W 8.6.0.20
AOS-245123 AOS-245396 AOS-245831	In the WebUI, under **Managed Network > Configuration > Roles & Policies > Roles > role-name**, the **Show Advanced View** option did not load any information. The information is expected to load after selecting a role from the list. The fix ensures that the advanced role policies are loaded. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245142	switches were unable to establish a HTTPS connection with the Meridian server. This issue occurred when the software was upgraded to AOS-W 8.11.0.0 or later versions. The fix ensures that the switches establish a connection with the Meridian server as expected. This issue was observed in switches running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0
AOS-245145	In the WebUI, under **Configuration > Roles & Policies > Role > role-name > Show Advanced View > Captive Portal**, the preview button for custom HTML captive portal page was not available. The fix ensures the preview button is present. This issue was observed in some OAW-4550switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-245153	Some users were unable to send the AirGroup service configurations to Mobility Conductors. The fix ensures AirGroup configurations are sent to Mobility Conductors. This issue was observed in Mobility Conductors running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-245191	In some controllers running AOS-W 8.6.0.18 or later versions, OmniVista 3600 Air Manager sessions were not timing out. Also, it was not possible to connect to the controllers using direct SSH. The fix ensures the sessions are timed out as expected.	AOS-W 8.6.0.18
AOS-245260	Some OAW-AP325 access points were detecting radar signals only in 40 MHz DFS channels. No radar hits were detected when changed to 20 MHz channel. This issue occurred due to wireless interference in the environment. The fix ensures false radar signals are rejected. This issue was observed in APs running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-245329	The **resolvwrap** process continuously crashed whenever a VLAN that was set to **dhcp-client** failed to get an IP. The fix ensures the **resolvwrap** process does not crash in this scenario. This issue was observed in gateways running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-245334	Some OAW-RAPs were intermittently bootstrapping after a conflict with IP types received. The fix ensures IP types are checked and OAW-RAPs perform as expected. This issue was observed in OAW-AP503H and AP-OAW-AP303H Series access points running AOS-W 8.10.0.4 or later versions.	AOS-W 8.10.0.4
AOS-245367	In standalone switches, it was not possible to configure application speed limit under the **Dashboard > Traffic Analysis > Applications** tab. The fix ensures the speed limit configuration can be applied through the WebUI. This issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-245379	Some access points crashed and rebooted unexpectedly. The log files listed the reason as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. **It's WLAN firmware crash at "wlan fw crash at sched_algo_qos.c:1530 sched_algo_choose_qos_tid_type".** The fix ensures the access points work as expected. This issue was observed in OAW-AP534, OAW-AP535, OAW-AP555, AP-634, OAW-AP635, and OAW-AP655 access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245401	**HE** capabilities were configured on the beacon and probe response for **2.4GHz** radio even though the **HE** setting was disabled. The fix ensures that HE capabilities are not configured on the beacon and probe response when the **HE** setting is disabled. This issue was observed in OAW-AP500 Series access points running AOS-W 8.9.0.0 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-245409	Some users were unable to pass traffic to the captive portal after a rebootstrap. This issue occurred when APs could not source NAT the traffic due to Back-up LMS having more DNS entries than LMS. When the AP changed LMS to Back-up LMS, the DNS ID table was not downloaded correctly. A correction of the DNS ID table resolved the issue. This issue was observed in access points in split-tunnel mode running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-245414	In some OAW-4750XM switches, GRE tunnel interface stats over SNMP were not populated. The fix ensures the counters are present in GRE tunnel interfaces. This issue was observed in switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17
AOS-245443	High channel utilization was observed in OAW-AP635 access points running AOS-W 8.11.0.0 or later versions. This issue was observed on 2.4 GHz radios. The fix ensures APs work as expected.	AOS-W 8.11.1.1
AOS-245458	The ports 0/0/6 to 0/0/11 of the OAW-41xx Series controllers did not transmit traffic as expected. The fix ensures the ports work as expected. This issue was observed in controllers running AOS-W 8.10.0.7.	AOS-W 8.10.0.7
AOS-245499	switches returned the wrong number of associated clients per SSID. This issue was related to an error in the SNMP table population process. The fix ensures the correct number of associated clients is returned by the switch. This issue was observed in switches running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21
AOS-245519	In some switches running AOS-W 8.10.0.0 or later versions, the system automatically restarted when the system was halted using the LCD menu. The fix ensures switch works as expected without restarting.	AOS-W 8.11.1.1
AOS-245539	The **Configuration > Roles & Policies > Aliases > Network Aliases** section of the WebUI did not accept the complete set of host names provided when added simultaneously. Instead, only the last input host name was successfully configured. The fix ensures the WebUI works as expected. This issue was observed on devices running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-245656	In the **Configuration > Interfaces > Ports** page of the WebUI, selecting a port channel displayed the details, but after navigating to physical port, the configuration was not displayed. As a result, the page had to be reloaded. The fix ensures the information is displayed as expected. This issue was observed in switches running AOS-W 8.10.0.7 or later versions	AOS-W 8.10.0.7
AOS-245657	The **show airmatch optimization** command incorrectly displayed a sequence of numbers, showing 4 digits instead of 5. The fix ensures that the command's output displays the correct sequence of numbers. This issue was observed in controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-245689	In some switches running AOS-W 8.10.0.7 or later versions, the **HA-flags** value was not shown in the output of the **show ha ap table** command. This fix ensures that this value is populated.	AOS-W 8.10.0.7
AOS-245777	The **Dashboard > Overview > Clients** page of the WebUI did not organize client data or display the graphics based on signal quality when applying the **Grouped by signal quality** filter. This issue was observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-245784	The **ap convert pre-validate** function did not work correctly when applied to OAW-RAPs running AOS-W 8.10.0.0 or later versions. The fix ensures the function works as expected on OAW-RAPs.	AOS-W 8.10.0.0
AOS-245788 AOS-246892 AOS-246962	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the crash as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The crash-info shows **TARGET ASSERT** occurred at **PC:0x00000000**. The fix ensures APs work as expected. The issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245853	Managed devices were ignoring Radius VSA for **Aruba-Admin-Role**. This issue occurred when authentication management was enabled and performing certificate authentication using the WebUI. The switch was getting updated with wrong role, even though **cppm** sent the correct one. The fix ensures the role is obtained from VSA and is updated accordingly. This issue was observed in devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245931	In the **Configuration > System > Logging** page of the WebUI, the **Duplicate combination of IP address and Category** error was displayed when adding an **arm-user-debug** entry, if **arm** entry already existed. The fix ensures the error message is not displayed in this scenario. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-245939 AOS-245445	In some switches, the **ap_crash_transfer_check error** log was generated when core file transfers failed using TFTP. As a result, unnecessary log files were accumulating. The fix ensures the log file is not generated in this scenario. This issue was observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-245976	In some switches running AOS-W 8.10.0.4 or later versions, the admin management user entry could not be deleted on Mobility Conductors and standalone switches. The issue occurred because the deletion of the admin management user was not allowed nor supported by default. The fix ensures that the admin user can be deleted from Mobility Conductors or standalone switches, if there is at least one root user already configured.	AOS-W 8.10.0.4

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-245980	Some clients connected to OAW-AP535 access points on the 5 GHz band experienced significant packet loss to the gateway and increased latency during calls when LACP was enabled on the controller. The issue was observed when both the GRE-Stripping IP was configured and the AP-LACP was activated on the AP. The fix ensures APs work as expected. This issue was observed in access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-246003 AOS-248886	Some OAW-AP505 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as: **BadAddr:fecf3ca8 PC:dev_get_iflink+0x0/0x28 Warm-reset**. This issue occurred in an IPsec environment, where a tunneled device was deleted after IPsec encryption. The fix ensures proper validations are made, preventing the AP crash. This issue was observed in devices running AOS-W 8.6.0.21.	AOS-W 8.6.0.21
AOS-246051	Some controllers were unable to copy an image from the flash memory to the system partition. The error seen for this operation was: **Error determining image version**. The fix ensures the controller copies an image successfully. This issue was observed in OAW-4x50 Series controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246097	Some OAW-AP535 access points randomly disabled the ANI feature. The issue was due to an unintended trigger of the ANI periodic check, which disabled the feature. The fix ensures that the ANI feature stays enabled. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246103 AOS-247433 AOS-240688	Some OAW-AP635 and OAW-AP535 access points rebooted randomly with **reboot reason - kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_send.c:11778 first**. This occurred due to issues with M3 controllers recovery, to which the APs are connected to. The fix ensures the access points perform as expected. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-246124	In some OAW-4750XMswitch, a Kernel crash was observed due to a incorrect memory assignment in the **rt6i_node pointer**. The fix converts the direct assignment of **rt6i_node pointer** to **rcu_ assign_pointer** to ensure that the pointer assignment does not fail. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246164 AOS-249753	The **profmgr** process crashed unexpectedly when configuration changes were applied to an **aaa server-group**. The fix ensures the process does not crash in this context. This issue was observed in managed devices running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-246176	When the auth process was unable to classify a client, the **Client Device Type** and **Client OS** version was displayed empty in the CLI. As a result, ClientMatch did not apply default settings. The fix ensures the process works as expected. This issue was observed in access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-246184	Some access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **ar_wal_tx_sch_status.c:645 Assertion (PPDU_QUEUE_ID(tx_ctxt) != TX_INVALID_QUEUE || PPDU_SCH_ID(tx_ctxt)**. The issue was related to the AP image version, which has been updated to fix the problem. This issue was observed in APs running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-246198	Some users received the error **There is no IP address configured for Vlan 220** when attempting to ping from a source VLAN. The issue occurred even if the L3 interface was configured correctly and the VLAN was up and running. The fix ensures the ping works as expected. This issue was observed in managed devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246203	Some OAW-AP635 access points unexpectedly rebooted. The log files listed the reason for the event as: **PC is at ieee80211_get_he_bsscolor_info+0xfc/0x7a8 [umac]**. The fix ensures the access points work as expected. 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-246263	Mobility Conductors running AOS-W 8.10.0.7 or later versions experienced an unexpected **mDNS** process crash. The issue was related to buffer data corruption while responding to query packets having **sub-ptr** records. The fix ensures the **mDNS** process executes as expected.	AOS-W 8.10.0.7
AOS-246324 AOS-242197	MongoDB experienced corruption issues after the OmniAccess Mobility Controller rebooted. As a result, an error message, **A/C power cycle** was displayed. The issue occurred due to multiple processes in **INIT** state, which caused the corruption issues. The fix ensures customers can run the **process cleanup name dbstart_mongo** command for database cleanup when needed. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-246358 AOS-243849	Provisioning failed for the UAC-AP when changing the CPsec mode from enable to disable. The fix ensures the UAC-AP tunnel can be deleted correctly when keepalive times out, and ensures the provision succeeds after disabling the CPsec. This issue was observed in access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-246583	The OAW-4750XM OmniAccess Mobility Controllers experienced unexpected crashes as a result of a failure in the **tnld_node_mgr** process. The fix ensures the process works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246604	NVDA reader displayed toggle buttons as blank when the user selects the button. The fix ensures WebUI toggle buttons display as expected. This issue was observed in switches running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-246679 AOS-251757	Some OAW-RAPs failed to come online due to receiving duplicate inner IP addresses. This problem occurred randomly across various OAW-RAPs. A discrepancy was discovered between the Allow list entries on the OmniAccess Mobility Controller and those on the managed devices for the affected OAW-RAPs. The fix ensures the RAPs work as expected. This issue was observed on OAW-RAPs running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246730	Some OAW-AP535 access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **Reboot caused by kernel panic Take care of the TARGET ASSERT first(wlan_peer.c:3218 Assertion (vdev->bss->ni_ chan.phy_mode >= peer_ratectrl_params.phymode)**. The fix ensures the access points work as expected. The issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246732	90xx series switches hung up during boot up if the RJ45 console cable was connected to the controller but not to the console server or computer (in case of USB console access). The fix ensures the switches boot up correctly. This issue was observed in controllers running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-246836	OmniAccess Mobility Controllers running AOS-W 8.10.0.7 or later versions did not accept 4240 Gateways being added as managed devices. When attempted, the switches displayed two errors: ■ Error 1: **Device addition failed. Some effective configuration is not compliant to new device model**. ■ Error 2: **Device addition failed. Configured VLANs count at Managed Network exceeds the max supported vlans-1**. The fix ensures 4240 Gateways can be added to the network topology.	AOS-W 8.10.0.7
AOS-246839	The usage of ECDSA certificates in a web-server profile caused the unavailability of the WebUI. The fix ensures the WebUI works as expected when using ECDSA certificates. This issue was observed in switches running AOS-W 8.10.0.7 and 8.10.0.7-FIPS or later versions.	AOS-W 8.10.0.7
AOS-246884	Some managed devices failed to download CA certificates when the name reached a string length of 31 characters. The fix ensures CA certificates download as expected. This issue was observed in managed devices running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-246937	The mDNS module of controllers crashed multiple times which caused an abnormal number of restarts. The fix ensures the controllers work as expected. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-246960	Some Mobility Conductor upgrades triggered license changes which caused the unintended loss of configured user-roles and ACLs in managed devices. The fix ensures that managed devices keep their configurations as expected. This issue was observed in OAW-4010 controllers running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-246966	Some 7240OmniAccess Mobility Controllers crashed and rebooted unexpectedly. The log files listed the reason for the crash as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures the controllers work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247070	Some switches crashed and rebooted with the reason **Datapath timeout (Intent:cause: 86:56)**. The crash was related to sessions deleted due to a QAT response timeout. The fix ensures the switches work as expected. This issue was observed in OAW-4104switches running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-247147 AOS-251395	Some Mobility Conductors running AOS-W 8.10.0.7 or later versions experienced classification issues with the WLAN Management System database. The fix ensures Mobility Conductors work as expected.	AOS-W 8.10.0.7
AOS-247206	The OAW-AP535 access points has an EAP non-complete issue. The fix ensures the software works as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.11.2.0 or later versions.	AOS-W 8.11.2.0
AOS-247326	The output of the **show running configuration** command displayed VLAN IDs and descriptions on separated lines instead of one. The fix ensures the information is displayed as intended. This issue was observed in managed devices running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-247335 AOS-247335 AOS-247967 AOS-248500 AOS-249709	Some 9240 Gateways rebooted with reason **Reboot Cause: Datapath timeout (Intent:cause: 86:56)**. This issue occurred due to passing DPI packets to CPU with id **0**. The fix ensures that these packets are not sent to the DPI engine. This issue was observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-247371	Some Korea-located APs detected false **typeid 43** radars due to an outdated DFS driver. The fix includes a patch with the latest Korean DFS standard, which eliminates these false detections. This issue was observed in APs running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-247387	The **Configuration > Access Points > Allowlist** section of the WebUI did not appropriately sort the AP allowlist by **Name** when the entry list exceeded one page. The fix ensures that sorting works appropriately across all pages. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247457 AOS-248519 AOS-249153	Some OAW-4850switches unexpectedly crashed. The log files listed the reason as: **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20)**. The fix ensures the controllers work as expected with ipv6 configurations and connections. This issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-247508	Whenever machine authentication and user authentication were enabled in conjunction, full 802.1X authentication took a long time to finish processing. This issue was related to a false trigger of the **denylist-sco-attack** process. The fix ensures the authentication process works as expected. The issue is observed in devices running AOS-W 8.11.2.0 or later versions.	AOS-W 8.11.2.0
AOS-247551	The output of the **show aaa auth-survivability-cache** command displayed station names in uppercase. The fix ensures the output is displayed in lowercase where expected. This issue was observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-247611	Some switches were displaying different channel assignments causing APs to not broadcast the datazone SSID. The fix ensures the correct information is displayed. This issue was observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-247648	Some OAW-AP315 access points incorrectly displayed an **r** flag in the standby AP Anchor (SAAC) controller when running the **show ap database** command. The issue occurred due to a regulatory domain mismatch between the primary and standby controllers. The fix ensures **r** flags are displayed correctly in SAAC. This issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247718	Data traffic was not flowing through the tunnels between the APs and the controller, even though the tunnel was restored. The fix ensures data traffic seamlessly flows through the tunnels between devices. This issue was observed access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247721	Mobility Conductors in a standby setup failed over and crashed unexpectedly. The log files listed the reason as **Datapath Exception**. The fix ensures the Mobility Conductor works as expected. This issue was observed in Mobility Conductors running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247819	In SNMP walks IPv6 clients with no IP address caused that the SNMP table was not ended rightly. As a result, the OID was not increasing and the SNMP walk stopped and did not move the next client. The fix ensures the SNMP walk performs as expected in this scenario. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-247823	Wired clients connected to some OAW-AP515 access points were unable to authenticate and were not seen on the switch. This issue was observed in Campus APs with multizone profile enabled on the AP. The fix ensures wired clients connect as expected in this scenario. This issue was observed in APs running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-247832	Some switches unexpectedly crashed and rebooted with the reason **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause: 86:34)**. The issue was related to the **ipv6 helper-address** parameter causing the crash when configured through the **interface vlan** command. The fix ensures the **ipv6 helper-address** configuration works as expected and does not cause the controller to crash. This issue was observed in 9240switches running AOS-W 8.11.1.1 or later versions.	AOS-W 8.11.1.1
AOS-247899	AirGroup clients were unable to discover wired servers or they were not found in the server list under client device. This occurred due to an error in clearing entries of old users and, hence, no space for new users. The fix ensures old entries are deleted properly and entries are available for users with all information required to respond to client queries. This issue was observed in Mobility Conductors running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-247952	The output of the **show ap bss-table ap-name** and **ap monitor ap-list ap-name** commands showed incorrect Tx BSSID flag information. Some VAPs showed an incorrect **(*+)** flag next to their bssid in the CLI output. The fix ensures the table output of the commands is accurate. 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-248092	Some APs displayed their SSID incompletely if there were more than 31 characters when using an XML API query due to the location field being truncated. The fix ensures the SSID displays correctly. This issue was observed in APs running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248120	In 9240 controllers running AOS-W 8.10.0.7 or later versions, clients failed to authenticate through EAP when many clients connected to AP-315 access points. The issue occurred because multicast frames were sent with WMM headers. The fix ensures that multicast packets are always sent without WMM headers to support non-WMM clients.	AOS-W 8.10.0.7
AOS-248121	The AVS process caused OAW-AP577 access points to crash after recovering from low temperatures since the AVS voltage was not high enough. An increase of the AVS default voltage fixed the issue. This issue was observed in OAW-AP577 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-248151	Some OAW-AP535 access points crashed and rebooted unexpectedly. The log file listed the reason for reboot as **Ap crashed at sched_algo_txbf.c:1909 Assertion 0 failedparam0 :zero, param1 :zero, param2 :zero**. The fix ensures the access points perform as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-248178 AOS-250372	The **Diagnostics > Tools > Spectrum Analysis** page of the WebUI did not display any data when a sensor from the **Connected Sensors** list was selected. The graphs displayed the message **No data to display**. However, this information was available through the CLI. The fix ensures the sensor data is displayed accurately in the WebUI. This issue was observed in switches running AOS-W 8.10.0.9.	AOS-W 8.10.0.9
AOS-248196	In a two-node cluster using OSPF for AP-MD connectivity, disabling the AP's reachability to one of the controllers designated as S-AAC, resulted in the absence of AMON messages being sent from the AAC to the OmniAccess Mobility Controller. The fix ensures AMON messages are correctly sent to the OmniAccess Mobility Controller. This issue was observed in access points running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-248203 AOS-250675	Some AP-654 and AP-605 access points randomly crashed when configured in a 6 GHz mesh. This issue occurred due to a loop in the mesh link status. The fix ensures the access points work as expected. This issue was observed in access points running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-248267 AOS-251592	The RADIUS/RADSec server could not connect to the FQDN host after rebooting the switch, resulting in IP loopbacks. The issue occurred due to replication problems during validation. The fix ensures the switch works as expected. This issue was observed in standalone switches running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248282	OAW-4010 switches displayed PVST+ issues where the removal of VLANs led to the incorrect transmission of PVST+ BPDUs with both PVID and 802.1Q VLAN ID set to 0. A check was added to avoid transmission of BPDUs with PVID equal to 0. This issue was observed on switches running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-248337	Multiple APs failed to upgrade to AOS-W 8.10.0.7, causing rebootstraps and high CPU load. This issue was caused due to a limitation in the byte size of the ESSID list. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248371	The OAW-4750XM switch failed to copy out **crash.tar** when the file size was larger than 2 GB. The fix ensures the switch works as expected. This issue was observed in OAW-4750XM switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248405 AOS-249646	The **login_fcgi** process crashed unexpectedly in some switches. This issue was related to the memory required for executing the process being insufficient. The fix increases the memory allocation for the process to ensure no crashes happen. This issue was observed in OAW-4750XM switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-248415	In some switches, the **fpapps** process displayed the error message **fpapps_amon_uplink_update_compression_stats: Cannot retrieve compression info**. This log meant that the switch failed to retrieve compression data. The fix ensures the switch can fetch such data successfully. This issue was observed in 9240 switches running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248466	The switch discovery preference field disappeared when changing it from ADP to Static, under **Dashboard > Configuration > Access Point > Provision**. The fix ensures the field displays as expected. This issue was observed in switches running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248473	In some OAW-AP535 access points the **ANI Desense level (Min)** went higher than **ANI Desense level (Max)** level. This issue occurred due to a regulatory limitation. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248537	PMF frames from client were corrupted by switch while decrypting and forwarding them to AP when client was connected to WPA3 Enterprise (GCM) (256 bit) Tunnel Mode SSIDs. As a result, devices experienced low throughput. This issue was observed in 9000 Series switches and VMC controllers running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
AOS-248680 AOS-248673 AOS-249682 AOS-250174 AOS-250197 AOS-251978 AOS-251054 AOS-251324	Some OAW-AP515 and OAW-AP575 access points crashed, rebooted and reconnected to the network. The log files listed the reason for the event as **BUGSoftLockup:CPU#1 stuck for 22s! [kworker/1:3:27856] PC:wlc_bmac_suspend_mac_and_ wait+0x21c/0x440 [wl_v6**. This issue occurred on a Mobility Conductors-Managed Devices setup after upgrading to from AOS-W 8.10.0.7 to AOS-W 8.10.0.8. The fix ensures the access points perform as expected. This issue was observed in access points running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248742	A BSSID mismatch was occurring during WPA3 SAE authentication, resulting in frames being sent to incorrect access points. The fix ensures that the values match. This issue was observed in switches running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-248891	Some OAW-AP515 access points unexpectedly crashed and rebooted. The log files listed the reason for the event as **BadPtr:000000d8 PC:wlc_ampdu_dotxstatus_ regmpdu+0x700/0xba0**. The fix ensures the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-248899	The syslog server of some wireless switches was flooded with error messages related to OpenFlow. Logs such as **ofa: <238503> <5843> |ofa| |sdn| ERRS ofml_openflow_mac_bridge_add_ap:322 AP client(mac-address) not found** were repeatedly displayed on switches with varying MAC addresses. These errors were related to roaming when connected to remote APs and can be safely ignored. The fix ensures the switches work as expected. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248925	In the **System > General > Clock** page of the WebUI, the **Timezone** and **Date and Time** did not display the correct configuration. The fix ensures the correct information is displayed. This issue was observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248961	Layer 3 interface displayed as **Down** on managed devices. As a result, guest users were unable to authenticate. The fix ensures guest users are able to pass the authentication process and managed devices work as expected. This issue was observed on managed devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-248972	Some OAW-AP534, OAW-AP535, OAW-AP555, AP-634, OAW-AP635 and OAW-AP655 access points unexpectedly rebooted. The log files listed the reason for the reboot as **Reboot caused by WLAN firmware TARGET ASSERT at twt_ap.c:847**. The fix ensures the access points work as expected. This issue was observed in access points running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-249028 AOS-251475	After upgrading from AOS-W 8.6.0.20 to AOS-W 8.10.0.7 or later versions, the **HTTPD** process crashed with reason **Segmentation fault**. The issue occurred due to an incorrect parameter sent to a log function. The fix ensures the switchesperform as expected.	AOS-W 8.10.0.7
AOS-249066 AOS-250718	The **auth** process crashed and reloaded, causing connectivity issues when more than 37 dormant IP addresses were associated with a single MAC address. The fix ensures the **auth** process works as expected. This issue is observed in switches running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249123	Some switches crashed unexpectedly due to the **impystart** process. The fix ensures the process works as expected. The issue was observed in switches running AOS-W 8.10.0.5 or later versions.	AOS-W 8.10.0.5
AOS-249133 AOS-249273	Some 9240 switches running AOS-W 8.10.0.4 or later versions rebooted with **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause: 86:34)**. This issue was caused by gradual memory leak within the **fpapps** process. The fix ensures the switches perform as expected.	AOS-W 8.10.0.4

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-249197	Some AirGroup servers were not discovered by clients. Devices such as Mersive Solstice Pods do not appear in Apple clients' screen mirroring device list. This issue was related to AirGroup's refresh logic when using discovery packets, and is seen when there were nine or more MDNS service profiles configured in the AirGroup profile. The fix ensures that servers are discovered by clients as expected. This issue was observed in managed devices running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249253	APs failed to establish standby tunnels upon DHCP failure which caused datapath user, route, and route-cache information to be removed. The fix ensures the APs work as expected. This issue was observed in access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.7
AOS-249260	Some Mobility Controller Virtual Appliance deployments crashed when running AOS-W 8.10.0.7 or later versions. This issue was observed whenever the CLI password was passed as NULL. The fix ensures such deployments work as expected.	AOS-W 8.10.0.7
AOS-249529	When a cluster member becomes reachable and the status of the peer changes to **DISCONNECTED**, there is a log entry indicating **peer disconnected**, like so: **<ERRS> |cluster_mgr| Peer x.x.x.x heartbeat missed, Disconnected**. This log was not available in switches running AOS-W 8.10.0.7 or later versions. This issue occurred due to modifications in the cluster heartbeat mechanism. The fix ensures the log is available.	AOS-W 8.10.0.7
AOS-249565	After an upgrade to 8.10.0.9, Central??? On-Premises was unable to monitor all managed devices and the error **Unknown Trusted Certificate. Please upload the certificate before configuring in the profile** was displayed when showing the profile error logs. The fix ensures the monitoring works as expected. This issue was observed in switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.9
AOS-249589	In some switches the STM process continuously crashed. As a result, it was not possible to terminate access points on the controllers. The fix ensures the switches perform as expected. This issue was observed in OAW-4550 OmniAccess Mobility Controllers running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-249749	Neighbor AP information was incomplete in the output of the **show ap arm state** command. The fix ensures the information is correctly displayed. This issue was observed in APs running AOS-W 8.10.0.8 or later versions.	AOS-W 8.10.0.8
AOS-249754 AOS-249851	The SNMP walk failed to retrieve data for the fan tray OID. The fix ensures the fan tray OID is displayed correctly. This issue was observed in controllers running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249755	Users were able to connect to Mobility Conductors through SSH despite the subnet being disallowed in the ACL port session. The fix ensures only ACL-allowed clients are able to connect. This issue was observed in Mobility Conductors running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-249765	Some APs crashed and rebooted due to memory issues. The issue occurred when TWT statistics for pending session did not match the TWT statistics for reported session. The fix ensures that the APs work as expected. This issue was observed in access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-249815	Tunnel performance with MTU 1500 was poor. This issue was caused due to the AP's internal Traffic Allocation Framework (TAF). The fix includes an update to the AP driver, which resolves the tunnel performance problem. This issue was observed in switches running AOS-W 8.11.2.0 or later versions.	AOS-W 8.11.2.0
AOS-249961	Handy terminals could not associate to some OAW-AP300 Series APs running AOS-W 8.10.0.7 or later versions. The issue was related to a conflict with the DoS prevention feature of AOS-W, which, when enabled, prevented the AP driver from getting crucial data for device association. The fix ensures the DoS prevention feature in the AP profile does not interfere with device association, making APs work as expected.	AOS-W 8.10.0.7
AOS-249976	The **show ap debug radio-stats**, **show ap debug bss-stats commands** and MIB (**wlanAPRxDataBytes64**) were showing Rx data byte values lower than the actual received values at 5 GHz. The fix ensures the values are accurate. This issue was observed in switches running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-250070	Some APs were unable to upgrade from AOS-W 8.x to AOS-W 10.x. The issue was related to APs getting stuck at the pre-validation stage. The fix ensures that APs can be upgraded successfully. This issue was observed in OAW-AP615 access points running AOS-W 8.11.0.0 or later versions.	AOS-W 8.11.0.0
AOS-250148	AirGroup's **Transport State** was stuck on initializing status. The issue was related to the current handling of OpenFlow flows in AOS-W SDN switches. The fix ensures the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.10.0.9
AOS-250346	Some OAW-AP345 access points rebooted unexpectedly. The logs listed the reason as **AP Reboot reason: BadPtr:00000000 PC:0x0 Warm-reset**. The fix ensures the APs work as expected. This issue was observed in OAW-AP345 access points running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9
AOS-250349 AOS-241587	After upgrading to AOS-W 8.11.2.1, some AirGroup printers were no longer discoverable, preventing users from connecting. The issue occurred because few of the AirGroup server records were being dropped while responding to user queries. The fix ensures all the available servers can be discovered by users. This issue was observed in switches running AOS-W 8.11.2.1 or later versions.	AOS-W 8.11.2.1
AOS-251055	Some APs were unable to use SCP for dump server collection on IPv6. The fix ensures the AP works as expected. This issue was observed in APs running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6

Table 6: *Resolved Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-251130	The OID **sysExtFanStatus** on the Alcatel-Lucent 9240 switches previously reported the status of the external fans as 2 (inactive) inaccurately. The fix improves the monitoring of fan status by utilizing ALARM signals and will now update the **sysExtFanStatus** value to 1 (active) when there is no ALARM, and to 2 when there is a MAJOR ALARM (indicative of 0 RPM or fan failure) for the fan. This issue was observed in controllers running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-251173	Some APs did not send the correct DHCP decline package type whenever there was an IP address conflict. The fix ensures the message type is sent in alignment with RFC-2131, which resolves the issue. This issue was observed in OAW-AP315 access points running AOS-W 8.10.0.7 or later versions.	AOS-W 8.10.0.7
AOS-251522	OAW-4240 switches were not displayed in the WebUI under **Configuration > License > Capacity License** field, preventing their addition to the capacity license. The fix ensures the switches are visible in the WebUI. This issue was observed on switches running AOS-W 8.11.2.1 or later versions.	AOS-W 8.11.2.1
AOS-251905	Some switches did not display the OS type of devices in the WebUI dashboard. The fix ensures the OS type is displayed in the WebUI. This issue was observed in switches running AOS-W 8.10.0.6 or later versions.	AOS-W 8.10.0.6
AOS-252186 AOS-251237	In the **Configuration > System > CPsec** page of the WebUI, the option **Only accept APs from specified ranges** did not display the table to add the ranges. The fix ensures the table is displayed as expected. This issue was observed in managed devices running AOS-W 8.10.0.9 or later versions.	AOS-W 8.10.0.9

Chapter 7
Known Issues in AOS-W 8.12.0.0

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

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-250636	The maximum number of management user creation for SSH public key is not properly capped at 10 for switches running AOS-W 8.12.0.0. This allows for unlimited user creation.	AOS-W 8.12.0.0
AOS-250714	The wireless driver of AP-605H access points logs various occurrences of the **wl1: bcn inactivity detected** error when running AOS-W 8.12.0.0. This behavior is observed in the 2.4 GHz radio.	AOS-W 8.12.0.0
AOS-249176	The IP address of standby 9240 switches does not display for IPv6-configured APs. This issue is observed on 9240 switches running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-250058	IAP-VPN tunnels do not form because of a failure in the certification verification. This issue is observed in systems running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-249983	Rogue client detection does not work properly when attempting to transmit packets from the same MAC address but multiple different IP addresses. However, the service works appropriately in a single-MAC, one-IP-address scenario. This issue is observed on managed devices running AOS-W 8.12.0.0	AOS-W 8.12.0.0
AOS-245523	OpenFlow flows do not get installed back into the controller whenever one or both active OpenFlow services (UCC or AirGroup) are disabled and then re-enabled. This issue is observed in switches running AOS-W 8.12.0.0. **Workaround:**Restart the OpenFlow controller or reload the Mobility Conductor for services to work appropriately.	AOS-W 8.12.0.0
AOS-248941	After the configuration of **custom-app** with HTTP rules, the datapath session does not display in DPI table. This issue is observed in devices running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-248302	Some AP-605H access points drop TCP packets throughput within the d-tunnel when 6 GHz VAP is enabled. This issue is observed in access points running AOS-W 8.12.0.0.	AOS-W 8.12.0.0

Table 7: *Known Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-250457	Port 17 is not working correctly as traffic goes through and is shown as open. This issue is observed in Mobility Conductors running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-249672	An alert is triggered displaying that there is beacon inactivity detected on 5 GHz radio. The log files list the reason as **bcn inactivity detected**. This issue is observed in controllers running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-248307	The **database on-demand cleanup** process crashes after running the **process cleanup name dbstart_mongo** command. This issue is observed in Mobility Conductors running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-249241	The Skype service might sign out on multiple devices with active calls when the SSID is in tunnel mode. This issue is observed in OAW-AP635 access points running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-250642	The output of the **show ble_relay iot-profile** does not display AP group details and MAM/MBM profiles might not connect to servers. This issue is observed in access points running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-250211	The **Configuration > Services > Airgroup > service-based policy-> Sevices** page does not display any information for AirGroup configured services for the applied profile. his issue is observed on Mobility Conductors running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-249098	In some AP-605H access points, the output of the **show ap bss-table ap-name** command show a negative value under **EIRP/max-EIRP** column. This occurs when the 6 GHz radio is changed from AM mode to AP mode. This issue observed in access points running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-250654	When public certificates are uploaded for public key authentication, the reference counter is not updated correctly. This can be observed in the logs of the **show mgmt-user ssh-pubkey | include yash_ecssh** command. This issue is observed in controllers running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-247132 AOS-248181 AOS-248540 AOS-248933 AOS-249606	Some switches crash unexpectedly. This issue occurs when the software version of switches is upgraded to AOS-W 8.12.0.0. This issue is observed in switches running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-248005	Cluster upgrade fails on OAW-RAPs when CPSEC is enabled. This issue is observed in OAW-RAP clusters running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-248978	Access points experience connectivity issues when WPA3-SAE encryption is used. This issue is observed in APs running AOS-W 8.12.0.0.	AOS-W 8.12.0.0

Table 7: *Known Issues in AOS-W 8.12.0.0*

New Bug ID	Description	Reported Version
AOS-249539	Access points operating as a mesh portal are unable to change the static channel to 100E. This issue is observed in AP-605H access points running AOS-W 8.12.0.0.	AOS-W 8.12.0.0
AOS-250145	The WebUI freezes after a new user is configured using **+** icon while the **read-only** or **root** option is enabled. This issue is observed in switches running AOS-W 8.12.0.0.	AOS-W 8.12.0.0

Chapter 8
Upgrade Procedure

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

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

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Conductor Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Conductor, or two versions lower. For example multiversion is supported if a Mobility Conductor is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.5.0.0, AOS-W 8.4.0.0, or AOS-W 8.3.0.0.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 72 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 72 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 72 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Low Free Flash Memory

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

Prerequisites

Before you proceed with the freeing up the flash memory:

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

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

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

Freeing up Flash Memory

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

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

   Table 8: *Flash Memory Requirements*

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

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

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

2. If the available free flash memory is less than the limits listed in Table 8, issue the following commands to free up more memory.
   - **tar crash**
   - **tar clean crash**
   - **tar clean logs**
   - **tar clean traces**
3. Issue the **show storage** command again to check if the available space in **/flash** is more than the minimum space required for AOS-W upgrade as listed in Table 8

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

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

     Please clean up the /flash and try upgrade again.

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

     Please clean up the /flash and try upgrade again.

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

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

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

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

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

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

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

****

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

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

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 68.

NOTE

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

In the WebUI

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

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

NOTE

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

4. Log in to the AOS-W WebUI from the Mobility Conductor.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

NOTE

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

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

In the CLI

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

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

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

or

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

or

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

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

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Conductor.

```
(host)#reload
```

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

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

Verifying the AOS-W Upgrade

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

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 72 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 72 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 72.
2. Verify that the control plane security is disabled.
3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

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

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

a. Enter the FTP or TFTP server address and image file name.

b. Select the backup system partition.

c. Enable **Reboot Controller after upgrade**.

d. Click **Upgrade**.

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

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

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

In the CLI

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

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

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

or

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

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

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

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

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

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

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

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

5. Reboot the Mobility Conductor or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

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