AOS-W 8.7.0.0

Alcatel·Lucent
Enterprise

Release Notes

Contents

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 04	Added AOS-207599 under Known Issues.
Revision 03	Removed references to Fremont Devices.
Revision 02	Added following bug IDs under Resolved Issues: ■ AOS-199490 ■ AOS-199107 ■ AOS-200875 ■ AOS-203859 ■ AOS-200228 ■ AOS-201728 ■ AOS-198680 ■ AOS-205655 Added following bug IDs under Known Issues: ■ AOS-201286 ■ AOS-202346 ■ AOS-203495 ■ AOS-205506 ■ AOS-206146 ■ AOS-206147 ■ AOS-206169 ■ AOS-206357 ■ AOS-206540 ■ AOS-206587 ■ AOS-206888
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

Throughout this document, branch switch and local switch are termed as managed device.

For a list of terms, refer Glossary.

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

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10

- Mozilla Firefox 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 on Windows 7, Windows 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

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

Hardware Platforms

AP-505H Access Points

The Alcatel-Lucent AP-505H access points are entry-level, dual-radio wireless AP that can be deployed in either switch-based (AOS-W) or switch-less (Alcatel-Lucent AOS-W Instant) network environments. AP-505H delivers high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with 2x2 MU-MIMO radios, while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards.
- One uplink Ethernet port capable of data rates up to 2.5 Gbps.
- Four downlink Ethernet ports capable of data rates up to 1 Gbps, including two 802.3at PoE PSE ports for supplying power to downlink devices.
- Integrated BLE and Zigbee radios.
- Mesh
- Flexible USB host interface with 5W power sourcing capability.

For complete technical details and installation instructions, see *Aruba AP-505H Access Point Installation Guide*.

AP-518 Access Points

The Alcatel-Lucent AP-518 access points are high performance, multi-radio, outdoor access point that can be deployed in either switch-based (AOS-W) or switch-less (Alcatel-Lucent AOS-W Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point.
- Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Mesh

- Thermal management

For complete technical details and installation instructions, see *Aruba AP-518 Access Points Installation Guide.*

570 Series Access Points

The Alcatel-Lucent 570 Series access points (AP-574, AP-575, and AP-577) are high performance, multi-radio, outdoor access points that can be deployed in either switch-based (AOS-W) or switch-less (Alcatel-Lucent AOS-W Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax wireless services.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point.
- Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Mesh
- Thermal management

For complete technical details and installation instructions, see *Aruba 570 Series Access Points Installation Guide*.

570EX Series Access Points

The Alcatel-Lucent 570EX Series access points (AP-575EX and AP-577EX) are high performance, multi-radio access points suitable for harsh and hazardous outdoor locations that can be deployed in either switch-based (AOS-W) or switch-less (Alcatel-Lucent AOS-W Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax wireless services.

The APs provide the following functionality:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point.
- Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively.
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports.
- Thermal management

For complete technical details and installation instructions, see *Aruba 570EX Series Access Points Installation Guide*.

9012 switch Platform

The 9012 switch is a wireless LAN switch that connects, controls, and intelligently integrates wireless Access Points (APs) and Air Monitors (AMs) into a wired LAN system. The switch has advanced IDS functionality and mobility services that is integrated with per user based enforcement policies for better security. The switch has an in build Bluetooth functionality and hardware integrated NFC support, with the following port configurations:

- 12 x 10/100/1000BASE-T ports
  - 6 x PoP+ ports
  - MDI/MDX
- 2 x USB 3.0 port
- 1 x RJ45 console port
- 1 x Micro USB console port
- Bluetooth

For complete technical details and installation instructions, see *Aruba 9012 Controller Installation Guide*.

GT Netstick GLU-194ST USB Modem Support

AOS-W supports GT Netstick GLU-194ST USB modem on OAW-AP303H Remote Access Points.

Air Slice

Alcatel-Lucent's key RF differentiation, Air Slice, designed for 11ax APs optimizes user experience and assures QoA to enterprise applications. Air Slice combines AppRF and UCC for classifying applications and it also supports custom flow definitions.

AP Boot Time

The AP fast boot is supported on OAW-AP534, OAW-AP535, and OAW-AP555 access points for booting up within a minute with full functionality and configurations.

AP Fast Recovery

530 Series and 550 Series access points now support AP fast recovery feature. On detecting a firmware assert, the AP executes the fast recovery process in the affected radio to avoid rebooting of the AP unnecessarily, thereby reducing the downtime of the AP in the network.

AP Name in Probe Response Frames

The **wlan ssid-profile advertise-ap-name** command will broadcast AP names in probe response frames as a part of the vendor-specific Information Element.

AP USB Management

AOS-W supports new infrastructure to manage any USB device that is plugged to an AP. The infrastructure allows describing a USB device through either CLI configuration or by using predefined descriptors, USB device management through USB ACLs, and supports plugins for USB devices. The infrastructure supports sending notification to other processes and script-based notifications.

BLE Device Management

AOS-W supports BLE device management through the IoT manager. The IoT manager runs as a process on the Mobility Master and allows configuration of BLE devices, provides visibility of detected BLE devices, and categorizes the BLE devices. The BLE devices are managed through a BLE service profile. When a BLE service profile is applied to an AP group , all APs in that AP group inherit the BLE service profile.

Captive Portal

AOS-W now supports captive portal authentication for VAPs in the bridge forwarding mode. This feature is supported for wireless users on all OAW-AP and OAW-RAP models in cluster and non-cluster topology. To support captive portal authentication in the bridge forwarding mode, it is required to enable the **ageout-bridge-user** parameter in the **aaa profile** command.

Cluster

AOS-W supports mixed IP address for APs in cluster. Live upgrade is optimized to take less time to upgrade all devices in the cluster. Cluster-related commands are enhanced to display additional information about cluster heartbeats.

Centralized Licensing

AOS-W allows L3 redundant Mobility Masters to be configured as relay servers.

DAD for IPv6 APs

The Duplicate Address Detection (DAD) feature identifies and prevents IP conflicts in an IPv6 deployment and ensures that the configured unicast IPv6 address is unique before it is assigned to a VLAN interface on the AP.

Dashboard Monitoring

Following are the updates:

- The **Dashboard > Overview** page displays the details of wired clients connected in bridge mode.
- Cluster dashboard is now visible in nodes other than the Managed Network.
- The **Wireless Clients** table under **Dashboard** > **Overview** page displays all the IP addresses for a particular client.
- . The **Mesh Links** table displays the following information:
  - Cluster name
  - Status
  - Uplink Age
  - Portal Access Point
  - Mesh Points
  - Band

Delete Controller IPv4 Address at Device and Node Level

AOS-W allows to delete the switch IPv4 address at the device and group level while migrating from pure IPv4 or dual-stack deployment to native IPv6 deployment. The following changes are introduced as part of the **no controller-ip** command :

1. You can delete the switch IPv4 address in the following scenarios:
   - When a valid switch IPv6 address is available at the same device or group level.
   - When a single IPv4 address is available on the switch.
2. You cannot delete the switch IPv4 address when multiple IPv4 addresses are available. Hence, you must ensure that only the switch IPv4 and its interface address are the last remaining IPv4 entities to be deleted during the migration process. Depending on the scenario, one of the following errors is displayed in the CLI when you issue the **no controller-ip** command:

   ```
   Controller IPv4 cannot be removed. Please configure controller-ipv6 on some other valid vlan or the loopback
   Controller IPv4 cannot be removed. Multiple v4 addresses exist on the controller"
   ```
3. An attempt to delete the switch IPv4 address automatically deletes the last remaining IPv4 addresses on the corresponding VLAN or loopback interface by issuing the following commands:
   - For VLAN interface:

     ```
     interface vlan <id> no ip address
     ```
   - For loopback interface:

     ```
     interface loopback no ip address
     ```
4. An attempt to delete the last remaining IPv4 addresses is prevented by the validation code and displays the following error message in the CLI:

   ```
   Controller IPv4 configured with this address. Execute <no controller-ip> command to auto-delete the interface address.
   ```

Disable AP Factory Reset

AOS-W allows to disable AP factory reset by pressing the reset button on the AP for more than 5 seconds while the AP is operational.

DNS-SL Support for IPv6 Router Advertisements

AOS-W provides support for DNS Search List (DNS-SL) option through IPv6 Router Advertisements that allows the IPv6 clients to resolve incomplete domain names.

Dump Collection Enhancements

Crash dump files can now be transferred to a switch on demand from the AP's flash memory. The following commands have been introduced as pert of this feature:

- `ap get-crash-dumps`: This command allows AP crash dump files to be transferred to the switch flash memory on demand from the AP flash memory.
- `show ap get-crash-dumps-status`: This command displays the status of the crash dump file transfers to a switch.

This feature is enabled only on OAW-AP534, OAW-AP535, and OAW-AP555 access points.

Enhancements to AP Master Discovery

AOS-W now allows users to configure the preferred IP protocol for AP master discovery.

EAP Transactions per Second Statistics

AOS-W now supports the calculation of EAP transactions per second for 802.1X users. The following command have been introduced as part of this feature:

- `dot1x-transactions-monitor set`: This is a set command introduced to set the interval and duration of generating the rate statistics of a 802.1X transaction.
- `dot1x-transactions-monitor`: This is an action command to start or stop the display of the rate statistics under the corresponding show command.
- `show dot1x-transactions-monitor stats`: This is the show command to display the rate statistics, per second, for a 802.1X user. The command output continues to display the stats until the user manually stops the result by executing the stop parameter under the dot1x-transactions-monitor command.

Fast BSS Transition Support for WPA3

AOS-W now supports Fast BSS Transition (802.11r) for the WPA3 modes in both tunnel-forwarding and decrypt-tunnel modes for all APs which support WPA3.

Firmware Diagnostic Logging

AOS-W now supports collection of WLAN firmware diagnostic logs to facilitate firmware debugging. The following command have been introduced as part of this feature:

- `ap debug radio-diag-log`: This command collects WLAN firmware diagnostic logs to facilitate firmware debugging.
- `show ap debug radio-diag-log status`: This command displays the current diagnostic logging status of an AP.

This feature is enabled only on OAW-AP534, OAW-AP535, and OAW-AP555 access points.

Global IPsec Rekey Timer

AOS-W now allows you to reduce the rekey time for IPsec and ISAKMP to enable faster debugging.

GRE Tunnel Statistics

AOS-W now sends GRE tunnel statistics to OmniVista 3600 Air Manager for monitoring.

Green AP

OAW-AP514, OAW-AP515, OAW-AP534, OAW-AP535, OAW-AP555, OAW-AP504, OAW-AP505, AP-505H, AP-518, and 570 Series access points support the Green AP feature.

HE Pooling and Automatic Tri-Radio

AOS-W supports High Efficiency (HE) dedicated radios, pooling of HE clients to HE-preferred radio, and automatic tri-radio mode. AirMatch dedicates HE radios for ClientMatch to steer HE or 802.11ax capable clients to the dedicated radios. All 500 Series, 510 Series, 530 Series, 550 Series, 570 Series, and 570EX Series access points support HE pooling. AirMatch supports automatic tri-radio mode, that is, two 5 GHz radios and one 2.4 GHz radio or the dual band mode of one 5 GHz radio and one 2.4 GHz radio on OAW-AP555 access point.

Hotspot 2.0 Support APs

AOS-W now supports Hotspot 2.0 on 530 Series, OAW-AP555, and 570 Series access points.

Hybrid Model Support for OAW-RAP Terminating on a VMC

AOS-W now supports the hybrid model of deploying OAW-RAPs on a VMC to address cert-related issues.

IKE Initiator Enhancements

The default IKE policy parameters have been changed to DH14 and HMAC-SHA256 from DH2 and HMAC-SHA1. This enhancement impacts the following downgrade scenarios:

- Mobility Master is running a lower version than AOS-W 8.7.0.0 and the managed devices are running AOS-W 8.7.0.0 or later versions.
- VPNC is running a lower version than AOS-W 8.7.0.0 and BOCs are running AOS-W 8.7.0.0 or later versions.
- Managed devices are running a lower version than AOS-W 8.7.0.0 and the APs are running AOS-W 8.7.0.0 or later versions.

If the devices are in one of the above scenarios, the tunnel establish with these devices fails with IKE policy mismatch. To avoid these scenarios, create the following two custom-polices on a Mobility Master or managed devices in advance before doing any upgrade or downgrade:

```
crypto isakmp policy <custom-policy-number1>
version v2
encryption aes128
hash sha2-256-128
group 14
authentication rsa-sig
prf prf-hmac-sha256
!
crypto isakmp policy <custom-policy-number2>
version v2
encryption aes246
hash sha2-256-128
group 14
```

```
authentication rsa-sig
prf prf-hmac-sha256
!
```

Integrated Thermal Management for 570 Series Access Points

570 Series now supports intelligent temperature monitoring system. When enabled, the temperature is dynamically controlled and the AP is allowed to cool down. The feature can be enabled using the **ap system-profile** command or can be configured under the **AP System Profile** using the WebUI.

IoT Data Filter

AOS-W supports IoT data filters that reduce the traffic on the telemetry interfaces.

IP Classification-based Firewall

AOS-W supports IP classification-based firewall. IP classification helps to identify the IP address and geolocation from where malicious activities originate. With the IP classification, any inbound attack from the malicious end points may be stopped at the managed device itself and thereby, protect the client devices behind the managed devices

IPv6 Support for CPPM Downloadable User Role

AOS-W now allows to download the ClearPass Policy Manager (CPPM) user role using the IPv6 address. The IPv6 address is configured in the RADIUS authentication server. The downloadable CPPM user role contains the ACL and policy enforcement profile, which are defined in the ClearPass Policy Manager.

IPv6 Support for VIA

AOS-W allows you to configure IPv6 address of the managed device in VIA connection profile. Hence, you can use either IPv4 or IPv6 address of the managed device to establish connection with the remote server.

Layer 2 GRE Tunnel Fragmentation

AOS-W now supports fragmenting IP packets sent over GRE tunnels. IP packets can be fragmented when the packet length is greater than tunnel MTU.

MAC-Based Debugging

AOS-W now supports per MAC-based debugging in IKE.

Mesh Access List

The mesh access list feature allows each AP to discover only the whitelisted neighboring APs.

Mesh Radio Link Selection for OAW-AP340 Series and 550 Series Access Points

AOS-W now allows to configure the 5 GHz radio used for mesh links. This feature is supported in dual-5 GHz and split-5 GHz radio enabled APs. Show commands related to mesh cluster profiles are also enhanced to display the radio information of mesh APs. This feature is designed to offer better control of the RF environment in mesh networks.

Mixed IP Address Support for APs

AOS-W allows both IPv4 and IPv6 APs to connect to a cluster seamlessly, irrespective of the cluster IP address family.

No Beaconing as BLE Operation Mode

AOS-W does not support **Beaconing** as a BLE operation mode on switches.

No BLE in OAW-AP203H Series, OAW-AP203R Series, OAW-AP207 Series, OAW-AP 220 Series, and OAW-AP228 Access Points

AOS-W does not support BLE in OAW-AP203H Series (OAW-AP203H), OAW-AP203R Series (OAW-AP203R and OAW-AP203RP), OAW-AP207 Series (OAW-AP207), OAW-AP 220 Series (OAW-AP224 and OAW-AP225), and AP_OAW-AP228 Series (AP-228) access points.

OpenSSL Upgrade

AOS-W 8.7.0.0, OpenSSL is upgraded from 1.01c to 1.02t for AOS-W 8.7.0.0-FIPS.

Support for Multiple Policy Domains

AOS-W now supports mulitple policy domains for group profiles.

Spectrum Analysis Support

The OAW-AP504, OAW-AP505, AP-505H, OAW-AP514, OAW-AP515, AP-518, OAW-AP534, OAW-AP535, OAW-AP555 and 570 Series access points now support spectrum analysis feature.

Support for Diffie-Hellman Groups 20 and 21 in Enhanced Open Security

AOS-W now supports Diffie-Hellman Groups 20 and 21 for Enhanced Open Security. Previously AOS-W supported only Diffie-Hellman Group 19 for Enhanced Open Security.

Support for Exposure Notification in IoT Device Class Filter

AOS-W now supports an IoT device class filter Exposure Notification based on the presence of service UUID 0xFD6F and service data 0xFD6F.

Support for Input-Filter on BLE Devices

AOS-W now supports an input-filter for BLE devices. When IoT transport profiles are configured, BLE-devices are filtered based on the IoT transport profiles which may include device class, UUID, or vendor filters. Only BLE devices that should be reported are stored in the BLE-table.

Support for IoT Southbound API

AOS-W now supports an IoT Southbound API that allows interaction with IoT devices and does not require any knowledge of the device by Alcatel-Lucent infrastructure.

Support for Native IPv6 Deployment

AOS-W provides native IPv6 support that allows enterprises to deploy pure IPv6 wireless network in a Mobility Master-Managed Device topology. Hence, all the applications and processes running on the managed devices support IPv6 addresses for seamless communication between Mobility Masters and managed devices.

AOS-W supports native IPv6 deployment for the following applications or scenarios:

- The applications in Mobility Masters and managed devices that are connected directly or through VPNC in an IPv6 network.
- The applications in primary and secondary Mobility Masters that are connected in IPv6 Network.
- OAW-RAP inner IPv6 pool in cluster deployment.
- ClearPass Policy Manager downloadable user role with RADIUS server configured with IPv6 address.
- Communication with server over the following standard protocols:
  - NTP
  - SNMP
  - SCP
  - FTP
  - TFTP
  - RADIUS
- Configuration of ClientMatch in ARM profiles.
- Configuration of **upgrademgr** process to send upgrade requests between Mobility Master and managed devices.
- Scheduled deployments in AirMatch.
- WebCC feature to download database for web classification from cloud service.

Support for SSH Protocol on APs

AOS-W now allows SSH protocol over telnet protocol for high end encryption and enhanced security to avoid any network attack or risk of malicious users. APs running AOS-W 8.7.0.0 have SSH enabled by default.

SHA-2 Support for SSH Authentication

AOS-W now provides the SHA-2 support for SSH authentication. The **ssh** command allows disabling the **hmac-sha1** and **hmac-sha1-96** parameters using the **disable-mac** parameter to enable SHA-2.

Support for Wiliot Sensor

AOS-W now supports Wiliot sensors. Wiliot is a leading provider of battery-free BLE tags. An AP receives BLE data from a Wiliot sensor and streams it over Telemetry-Websocket.

Thermal Shutdown Support

AOS-W supports thermal shutdown feature for all 802.11ax APs and for mesh mode APs.

TLS Version Support in Web-Server

TLS v1.2 is now the default **ssl-protocol** in the **web-server** profile. TLS v1 and TLS v1.1 is disabled by default.

Trusted CA Certificates

AOS-W now allows to upgrade the trusted CA certificates dynamically.

WebUI Support to Configure IoT Transport Profile

The AOS-W WebUI allows configuration of following IoT profiles:

- Transport Stream
- IoT radio profile
- Zigbee service profile
- Zigbee device profile

Wi-Fi Uplink Support on 802.11r APs

AOS-W now provides support for Wi-Fi uplink on all 802.11r enabled APs.

WLAN Details for Specific Clients

AOS-W now supports retrieval of all WLAN driver specific details for each client for client debugging. The following command have been introduced as part of this feature:

- `show ap debug client-info`: This command displays all the details of a specific client in WLAN driver, for client debugging.

WPA3 Opmodes Support for Fast BSS Transition

AOS-W now supports WPA3 opmodes for fast BSS transition. The following list provides the supported opmodes:

- WPA3-Personal (SAE)
- WPA3-Personal (SAE) + Transition Enable
- WPA3-Enterprise Basic (WPA3-AES-CCM-128)
- WPA3-Enterprise Non-CNSA (WPA3-AES-GCM-256)

VLAN Pooling Resiliency

Starting from AOS-W 8.7.0.0, the VLAN pool resiliency feature automatically assigns clients to the next available VLAN ID if a particular VLAN pool is full. This feature is enabled by default and takes effect only when the VLAN assignment type is **EVEN**.

The following CLI commands configure VLAN pool resiliency:

```
(host) [mynode] (config) #vlan-name a assignment even ip-timeout
(host) [mynode] (config) #vlan-name a assignment even max-ip-timeouts
(host) [mynode] (config) #vlan-name a assignment even full-period
```

ZigBee Socket Device

ZigBee Socket Device (ZSD) may be configured and applied as a filter in IoT transport. With ZSD, specify the source endpoint, destination endpoint, destination profile ID, or destination cluster ID and the packets between the ZigBee devices and server are transmitted through the Alcatel-Lucent Telemetry Websocket.

This chapter describes the platforms supported in this release.

Mobility Master Platforms

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

Table 3: *Supported Mobility Master Platforms in AOS-W 8.7.0.0*

Mobility Master Family	Mobility Master Model
Hardware Mobility Master	MM-HW-1K, MM-HW-5K, MM-HW-10K
Virtual Mobility Master	MM-VA-50, MM-VA-500, MM-VA-1K, MM-VA-5K, MM-VA-10K

OmniAccess Mobility Controller Platforms

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

Table 4: *Supported OmniAccess Mobility Controller Platforms in AOS-W 8.7.0.0*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series Hardware OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series Hardware OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series Hardware OmniAccess Mobility Controllers	OAW-4104, 9012
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 in AOS-W 8.7.0.0*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303
OAW-AP303H Series	OAW-AP303H, AP-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345

Table 5: *Supported AP Platforms in AOS-W 8.7.0.0*

AP Family	AP Model
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
370EX Series	AP-375EX, AP-377EX
OAW-AP387	OAW-AP387
500 Series	OAW-AP504, OAW-AP505
500H Series	AP-505H
510 Series	OAW-AP514, OAW-AP515, AP-518
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555
570 Series	AP-574, AP-575, AP-577

Deprecated APs

The following APs are no longer supported from AOS-W 8.7.0.0 onwards:

Table 6: *Deprecated AP Models*

Access Points Series	Model Numbers
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP103 Series	OAW-AP103
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1

Table 6: *Deprecated AP Models*

Access Points Series	Model Numbers
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

Chapter 4
Regulatory Updates

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 businessportal2.alcatel-lucent.com.

The following DRT file version is part of this release:

- DRT-1.0_75772

After upgrading to AOS-W 8.7.0.0, it is recommended to re-store flash backup of data in OAW-4850 switches, that were earlier upgraded from AOS-W 8.3.0.x to AOS-W 8.5.0.8 (or prior versions). This ensures that internal user database entries are not lost. For more details, see Resolved Issues.

Also, the following issues are resolved in this release.

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-119600 AOS-202348	143771	Few APs rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: Rebooting the AP because of FW ASSERT**. This issue occurred in OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 8.2.0.0 or later version.	AOS-W 8.2.0.0
AOS-125897	151952 191568	When a managed device rebooted, APs and clients rebooted without IP addresses and other fields. The fix ensures no fields are missing when clients come up after a reboot. This issue was observed in managed devices running AOS-W 8.0.1.0 or later versions. **Duplicates:** AOS-155697 , AOS-187598, AOS-189036 , AOS-192082 , AOS-192723 , AOS-192731 , AOS-192734, AOS-195746, AOS-198423, and AOS-204676	AOS-W 8.0.1.0
AOS-143514 AOS-143768 AOS-184333 AOS-203809	174823 175163	The **authentication** process crashed unexpectedly. This issue occurred when the **aaa test-server verbose** command was executed. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions. The fix ensures that the Mobility Masters works as expected.	AOS-W 8.2.0.0
AOS-145651 AOS-147206 AOS-180623 AOS-200001	177671 179906 190477	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first**. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-146775 AOS-149709 AOS-201562	179166 183424	A configuration failure was observed when a new ACL rule was added. This issue is resolved by changing the default netdestination name to lower case. This issue occurred because the default netdestination name was in upper case. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-145854 AOS-186448 AOS-186600 AOS-185757 AOS-197564	177936	The WebUI and CLI did not allow a user to change an expired WebUI certificate on a Mobility Master running AOS-W 8.2.1.0. The log file listed the **Error: server certificate <certificate-name> not found in path /sc** error message. The fix ensures that the WebUI and CLI allow a user to successfully change the expired WebUI certificate with a new one on the Mobility Master. This issue occurred while uploading a certificate.	AOS-W 8.2.1.0
AOS-146042 AOS-151140	178173 185322	The log file of a Mobility Master Virtual Appliance displayed the **OID not increasing** SNMP error message. The fix ensures that the SNMP error is not displayed. This issue occurred because of incorrect values of ipaddr. This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.2.0.2.	AOS-W 8.2.0.2
AOS-146406 AOS-197741	178676	Some APs crashed randomly and the clients failed to authenticate to an AP. The fix ensures that the APs work as expected. This issue was observed in OAW-AP330 Series access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-152895	187760	A few OAW-AP300 Series access points running AOS-W 8.2.1.1 or later versions crashed and rebooted unexpectedly. The log file listed the reason for this event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **New Duplicates:** AOS-149841, AOS-153975, AOS-154406, AOS-154483, AOS-154558, AOS-154973, AOS-155411, AOS-155695, AOS-155710, AOS-156409, AOS-157916, AOS-158259, AOS-183215, AOS-183376, AOS-185652, AOS-186768, AOS-191074, AOS-195052, AOS-195058 **Old Duplicates:** 183580, 189185, 189741, 189841, 189944, 190491, 191119, 191565, 191582, 192564, 194698, 195184	AOS-W 8.2.1.1
AOS-153780 AOS-197947	188932	The **STM** process caused high memory utilization on a Mobility Master Virtual Appliance. The fix ensures that the **STM** process does not cause high memory utilization. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-154056 AOS-197865	189298	System LED was blinking with a green light after an AP connected to a managed device and booted up. Enhancements to the wireless driver resolved this issue. This issue occurred when 2.4 GHz radio was disabled. This issue was observed in 510 Series access points running AOS-W 8.4.0.0.	AOS-W 8.4.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-155632	191489	A stand-alone switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Control Processor Kernel Panic**. Enhancements to the wireless driver resolved this issue. This issue occurred when IP options caused the **Datapath** process to crash. This issue was observed in OAW-4x50 Series switches running AOS-W 8.3.0.0 or later versions. **New Duplicates:** AOS-157337, AOS-157417, AOS-158610, AOS-158360, AOS-184786, AOS-186151, AOS-187156, AOS-187576, AOS-187752, AOS-187880, AOS-189198, AOS-189439, AOS-191458, AOS-191603, AOS-192748, AOS-193261, AOS-193272, AOS-193491, AOS-193997, AOS-194310, AOS-194588, AOS-194797, AOS-194817, AOS-196391, AOS-198833 **Old Duplicates:** 193793, 193945, 195329, 195645	AOS-W 8.3.0.0
AOS-156080	192112	A managed device, running AOS-W 8.2.2.2, showed Skype error messages in the HTTPD logs and dropped XML messages that were meant for UCM. The visibility of Skype for Business call records were missing from the WebUI. The fix ensures that the managed device works as expected and does not drop the XML messages that are meant for UCM. **Duplicates**: AOS-182758, AOS-190590, AOS-191121, AOS-191286, AOS-193632, AOS-193733, AOS-203261	AOS-W 8.2.2.2
AOS-156389 AOS-197765	192523	The **pim** process crashed on a managed device in a 12 node cluster setup. The log file listed the reason for the event as **Module terminated: Segmentation fault**. The fix ensures that the managed device works as expected. This issue was observed managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-156552 AOS-196926	192771	The value returned from noise floor calculation on 5 GHz channels for APs was inaccurate when there was interference. The fix ensures that the APs work as expected. This issue was observed in 510 Series access points running AOS-W 8.4.0.0.	AOS-W 8.4.0.0
AOS-157011 AOS-191292 AOS-197670	193362	The output of **show datapath papi counters** command displayed invalid tunnel endpoint information. The fix ensures that the **show datapath papi counters** command displays the correct information. This issue was observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-157882 AOS-200009	194655	The **Dashboard > Overview > Clients** page displayed incorrect roles for wired clients connected to a OAW-RAP. The fix ensures that the WebUI displays the correct role for wired clients. This issue was observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-188090 AOS-196004 AOS-199152	—	The **Dashboard > Overview > Clients** page of the WebUI displayed incorrect usage values intermittently. The fix ensures that the correct usage values are displayed. This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-182579 AOS-195790 AOS-196493 AOS-197868 AOS-197989	—	APs and clients got disconnected frequently from the managed device. The fix ensures seamless connectivity. This issue occurred when heartbeats were randomly missed on the managed device. This issue was observed in managed devices running AOS-W 8.3.0.2 or later versions in a cluster setup.	AOS-W 8.3.0.2
AOS-183317 AOS-198642	—	An AP detected multiple false radars on channel 100, with type ID 255. The fix ensures that the AP works as expected. This issue was observed in 530 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-183630 AOS-200148	—	The **auth** module on managed devices running AOS-W 8.5.0.0 or later versions crashed unexpectedly. This issue occurred when **pefng** license was enabled and disabled on managed devices. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.0
AOS-183640 AOS-184351 AOS-184539 AOS-184540 AOS-198680	—	A memory leak was observed in the **mDNS** process in a managed device. This issue occurred when the **show airgroup ap** or **tar logs** command was executed. This issue is resolved by fixing the memory leak in the **mDNS** process. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-184268 AOS-197642 AOS-198392	—	The command **show ap debug mgmt-frames** displayed an error message, **stm| |ap| Unexpected stm (Station management) runtime error at handle_assoc_req, 7314**. Enhancements to the wireless driver fixed the issue. This issue occurred when the peer APs sent two reassociation requests simultaneously. This issue was observed in access points AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-184474	—	OAW-AP300 Series access points running AOS-W 8.2.2.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for this event as kernel panic: **Rebooting the AP because of FW ASSERT.** Enhancements to the wireless driver resolved this issue. **Duplicates:** AOS-186793, AOS-186872, AOS-186971, AOS-189390, AOS-190362, AOS-192337, AOS-194239, AOS-194677, AOS-195037, AOS-195056, AOS-196028, AOS-196378, AOS-196861, AOS-197722, AOS-200468, AOS-201008, AOS-202766, and AOS-205672	AOS-W 8.3.0.6
AOS-185197 AOS-188490 AOS-189847 AOS-192747 AOS-197045 AOS-199014	—	A Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for this event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20).** The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-186076	—	The STM process in a managed device that is part of a cluster setup crashed unexpectedly. This issue occured when the memory that was allocated for some clients was not released after these clients disconnected from their UAC in a cluster. The fix ensures that the STM process does not crash. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions. **Duplicates:** AOS-187884, AOS-189850, AOS-191866, AOS-192125, AOS-192310, AOS-193177, AOS-193387, AOS-193581, AOS-194218, AOS-194312, AOS-194434, AOS-194929, AOS-194993, AOS-195022, AOS-195125, AOS-195501, AOS-195758, AOS-196681, AOS-196740, AOS-196784, AOS-200947, AOS-201112	AOS-W 8.4.0.2
AOS-187671 AOS-200228 AOS-200230	—	The **mDNS** process in a managed device crashed and the managed device rebooted unexpectedly. This issue occurred because of a memory corruption in the **mDNS** process. This issue is resolved by avoiding memory corruption in the **mDNS** process. This issue was observed in managed devices running AOS-W 8.3.0.7.	AOS-W 8.3.0.7
AOS-187831 AOS-191107 AOS-201728	—	An AirGroup client did not discover an AirGroup server. This issue occurred when the shared AP name contained capital case letters. This issue is resolved making the shared AP name case insensitive. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-188255	—	The **Dashboard > Overview** page of the WebUI displayed incorrect number of users intermittently. The fix ensures that the WebUI displays the correct number of users. This issue was observed in Mobility Masters running AOS-W 8.3.0.8 or later versions. **Duplicates:** AOS-190476, AOS-190946, AOS-192725, AOS-193586, AOS-194784, AOS-196004, and AOS-200375	AOS-W 8.3.0.8
AOS-188485 AOS-193638 AOS-204439	—	The **<ofald 237504> <ERRS> |AP 32438@172.16.4.151 ofald| |sdn| ERRS ofald_datapath_msg_recv_cb:274 Invalid message type 126** error message was displayed every second in APs. The fix ensures that these spurious message is not displayed. This issue was observed in APs running AOS-W 8.4.0.0-FIPS in a Mobility Master - Managed Device topology.	AOS-W 8.4.0.0
AOS-188830 AOS-202343	—	After a reboot, some Mobility Masters running AOS-W 8.3.0.8 lost all existing configurations. This issue occurred when an L2 switchover occurred in a Mobility Master. The fix ensures that the Mobility Master works as expected.	AOS-W 8.3.0.8
AOS-188898 AOS-198730 AOS-199225 AOS-200227	—	The **postgres** module crashed on managed devices running AOS-W 8.2.1.0 or later versions. The fix ensures that the managed devices works as expected.	AOS-W 8.2.2.6
AOS-188979 AOS-201731	—	LEAP authenticated wireless clients were unable to connect to APs. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-189757 AOS-198545 AOS-203096	—	The captive portal redirection did not work when the client's **http GET** packet contained files with .png or .gif format. The fix ensures that files with .png or .gif format are not included. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-189772 AOS-196328 AOS-198374	—	The **dot1x** and **dot2x** processes crashed unexpectedly on a managed device. This fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2
AOS-189845 AOS-200712 AOS-201675 AOS-203365	—	The **dpagent** process crashed on a managed device running AOS-W 8.5.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.0
AOS-189982 AOS-200329	—	The **Configuration >WLANs** page did not display WLANs at lower node levels. This issue occurred when WLAN profiles with same name but different cases were created. The fix ensures that the WebUI displays the list of WLANs. This issue was observed in Mobility Masters running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-190184 AOS-190241 AOS-190347 AOS-190405 AOS-190468 AOS-190487 AOS-190776	—	The database synchronization failed between primary and secondary Mobility Masters in L3 redundancy. The fix ensures that the L3 redundancy works as expected. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-191216 AOS-196523 AOS-198261 AOS-199160 AOS-202300 AOS-203960	—	A managed device running AOS-W 8.0.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2).** The fix ensures that the managed device works as expected.	AOS-W 8.5.0.4
AOS-191394 AOS-203029	—	APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. This issue was observed in 500 Series access points running AOS-W 8.6.0.0 or later versions. Enhancements to the wireless driver resolved the issue.	AOS-W 8.6.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191565 AOS-197819 AOS-200697	—	A Mobility Master Virtual Appliance displayed high memory utilization. The fix ensures that the Mobility Master Virtual Appliance works as expected. This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-191579 AOS-195733 AOS-199406	—	A few users were unable to connect to the wireless network. This issue occurred when the **authentication** process crashed unexpectedly in a managed device. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-192529 AOS-199126	—	A few APs crashed and rebooted unexpectedly. The log file listed the reason for this event as **reboot caused by Kernel panic - not syncing: Fatal exception in interrupt with PC/LR is at asap_ firewall_forward+0xfc/0x92a0.** The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2
AOS-192771 AOS-198102	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20).** The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-192814 AOS-199107	—	The auto associate feature of AirGroup did not work as expected and AP related information on AirGroup server was incorrect when clients roamed between different managed devices. This issue occurred when GSM entries were not updated. The fix ensures that the feature works as expected. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions in centralized or distributed mode.	AOS-W 8.3.0.7
AOS-193033 AOS-198921 AOS-198953	—	Some clients were not redirected to the captive portal page. The fix ensures that the captive portal is working as expected. This issue occurred because the **Nginx** process failed due to a race condition. This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2
AOS-193362 AOS-198030	—	A Mobility Master was unable to establish connection with OmniVista 3600 Air Manager. The fix ensures that the Mobility Master works as expected. This issue occurred when OmniVista 3600 Air Manager was not reachable from the management interface. This issue was observed in Mobility Master Hardware Appliance running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-193377 AOS-205478	—	An AP crashed and rebooted unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. Enhancements to the wireless driver resolved this issue. This issue was observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193383 AOS-203470	—	500 Series access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that APs work as expected.	AOS-W 8.6.0.0
AOS-193560 AOS-197733 AOS-198565 AOS-200262 AOS-204794	—	The number of APs that were DOWN were incorrectly displayed in WebUI. However, CLI displayed the correct status of APs. The fix ensures that WebUI displays the correct status of APs. This issue was observed in Mobility Masters running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-194456 AOS-200656	—	The output of the **show firewall dns-name** command displayed the **iplist** information as 0.0.0.0. The fix ensures that the **show firewall dns-name** command displays the correct **iplist** information. This issue was observed in managed devices that are upgraded to AOS-W 8.3.0.8 version.	AOS-W 8.3.0.8
AOS-194518 AOS-199834	—	APs kept retrying a frame although they receive Block Acknowledgment (BA) packets from clients. The fix ensures that the APs work as expected. This issue was observed in 500 Series access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-194795 AOS-197097 AOS-201048 AOS-204637	—	Some managed devices running AOS-W 8.3.0.0 or later versions did not perform RADIUS authentication. The log file listed the reason for the event as **Failed to send the radius request for Station**. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.0
AOS-194813 AOS-198001 AOS-199579 AOS-200149 AOS-200648 AOS-201658 AOS-204458	—	The **mDNS** process in a managed device crashed and the managed device rebooted unexpectedly. This issue occurred because of a memory leak. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-195100 AOS-198302 AOS-204455	—	The health status of a managed device was incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master WebUI. The fix ensures that the correct health status is displayed. This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-195163 AOS-197980	—	The **ofc_cli_agent** process in a Mobility Master crashed unexpectedly. The fix ensures that the Mobility Master works as expected. This issue occurred due to mongo database buffer corruption. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195414 AOS-198954	—	The **profmgr** process crashed on a switch. This issue occurred when interface access mode was configured on the Mobility Master. The fix ensures that the Mobility Master works as expected. This issue was observed in OAW-4008switches running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-195498	—	Clients were unable to locate the AP accurately. The fix ensures that clients are able to locate the AP accurately.	AOS-W 8.7.0.0
AOS-195546 AOS-199490 AOS-199985	—	A memory leak was observed in the **mDNS** process in a managed device. This issue occurred when AirGroup was enabled in distributed mode. The fix ensures that the managed devices works as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-195600	—	Users were unable to discover Apple TV. The issue occurred because AirGroup mDNS packet sessions were flagged with 'o' flags during a Skype call initiation by UCC when AirGroup was enabled in Centralized mode. The fix ensures that users are able to discover Apple TV. This issue was observed in the Mobility Masters running AOS-W 8.3.0.8 or later versions. **Duplicates:** AOS-197877, AOS-199284, AOS-199741, AOS-199006, AOS-200095, AOS-200188, AOS-200197, AOS-200406, AOS-203177	AOS-W 8.3.0.8
AOS-196215 AOS-199712	—	Some clients were unable to manage multiple clusters using a single Mobility Master. This issue occurred when the Mobility Master assumed that the clusters are on the same VLAN and cannot reuse the same VRRP ID in the cluster profile. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196220 AOS-201396	—	An AP displayed the error message, **wlan: [0:E:BSSCOLOR] ol_ath_offload_bcn_tx_status_event_handler: beacon tx failed.** The fix ensures that the AP work as expected. This issue was observed in access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.2
AOS-196312	—	Access points were unable to connect to a cluster. This issue occurred because the **ap_move** flag was not cleared after the **apmove** command was executed. The fix ensures that the **ap_move** flag is cleared after the **apmove** command is executed. This issue was observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions. **Duplicates:** AOS-199450, AOS-199937, AOS-200235, AOS-200605, AOS-200453, and AOS-201990	AOS-W 8.3.0.0
AOS-196325 AOS-200875	—	A Mobility Master rebooted unexpectedly. This issue occurred because of high memory usage. The fix ensures that the Mobility Master works as expected. This issue was observed in a Mobility Master running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196455 AOS-198362	—	A Mobility Master sent incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196489 AOS-199172	—	GSM entries for AirGroup servers were not updated when MAC authenticated clients moved between APs. The fix ensures that the GSM entries are updated with new bssid of the APs. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-196560 AOS-197671 AOS-198844 AOS-199170 AOS-199375 AOS-200690	—	A few APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic, aruba_am_tx_elem_handler+0x404**. The fix ensures that the access points work as expected. This issue was observed in OAW-AP534, OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-196594 AOS-201532	—	A few 802.1X clients were deauthenticated and lost connectivity to an AP. The fix ensures that the clients are able to connect to the AP. This issue occurred when the PMK ID sent by the clients was not renewed. This issue was observed in APs running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.3
AOS-196604 AOS-198814	—	The **STM** process on a managed device crashed and the APs moved to the backup managed device. The fix ensures that the APs do not move to the backup managed device. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-196683	—	Access points came up without standby APs. This issue occurred in a cluster when AP channel scanning detected an invalid AP and skipped scanning the remaining APs. The fix ensures that the APs work as expected. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196847 AOS-196941 AOS-198485 AOS-201783	—	The **Dashboard > Infrastructure > Controller** page did not display the list of available switches. The fix ensures that the WebUI displays the list of switches. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196869	—	OAW-AP515 access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **BadAddr:a3b303d7370b0 PC:wlc_mutx_bw_policy_update+0x408/0x28b8**. The fix ensures that the APs work as expected. **Duplicates:** AOS-199431, AOS-199587, AOS-199592, AOS-201056, AOS-201803, AOS-206525, AOS-206706, AOS-206894, AOS-201192, AOS-201589, AOS-203260, and AOS-203650	AOS-W 8.6.0.0
AOS-196896 AOS-197050 AOS-200076 AOS-200077	—	OAW-AP325 access points running AOS-W 8.5.0.3 or later versions crashed and rebooted unexpectedly. This issue occurred during the **stm** process crash when more than 256 clients connected to a OAW-RAP or OAW-AP on bridge mode got deleted. The fix ensures that the APs work as expected.	AOS-W 8.5.0.3

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196911 AOS-198963	—	Some users were unable to connect to APs. Enhancement to the wireless driver fixed the issue. This issue was observed in OAW-AP555 access points running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-196928 AOS-196066 AOS-196943 AOS-197742 AOS-198048 AOS-198328 AOS-198682 AOS-199156	—	Users were unable to discover the wired AirGroup server and experienced packet drops when a UCC Skype call was initiated. This issue occurred when AirGroup was enabled in centralized mode. The fix ensures that the users are able to discover the wired AirGroup servers. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197127	—	A managed device crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2).** This issue was observed in OAW-4x50 Series switches running AOS-W 8.3.0.7 or later versions in a cluster setup. **Duplicates:** AOS-197060, AOS-197130, AOS-197137, AOS-197161, AOS-197163, AOS-198720, AOS-201821, and AOS-204938	AOS-W 8.3.0.7
AOS-197160 AOS-198571 AOS-200427 AOS-201607	—	A few managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2.** The fix ensures that the managed device works as expected. This issue occurred due to corrupt ACL entries. This issue was observed in managed devices running AOS-W 8.3.0.8 in a cluster-setup.	AOS-W 8.3.0.8
AOS-197224 AOS-204629	—	A Mobility Controller Virtual Appliance running AOS-W 8.4.0.4 or later versions returned RADIUS attribute values in incorrect order causing firewall to drop data packets. The fix ensures that the Mobility Controller Virtual Appliance returns RADIUS attribute values in correct order.	AOS-W 8.4.0.4
AOS-197393 AOS-200407	—	Radios experienced high number of resets and packet drops were also observed on APs. The fix ensures that the APs work as expected. This issue was observed in OAW-AP340 Series access points running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-197536 AOS-198286 AOS-200371	—	Many clients got disconnected from APs. This issue occurred when a new VLAN was added. The fix ensures seamless connectivity. This issue was observed in access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.0
AOS-197631	—	Policy-based routing was not applied when IPsec map was configured as nexthop. The fix ensures that the correct policy-based routing is applied. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197786 AOS-197827 AOS-198927	—	A few clients were unable to pass traffic on APs. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197812	—	A mismatch of user roles was observed in the WebUI and CLI of the Mobility Master and managed device. The fix ensures that there is no mismatch. This issue occurred when UDR was configured to assign user role to clients. This issue was observed in both Mobility Masters and managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-197912	—	Multicast traffic was not forwarded to the clients when UAC and AAC were different. The fix ensures that the multicast traffic is forwarded to the clients. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-197918	—	Redirect pause was enabled although Welcome page was disabled in captive portal. The fix ensures that when the welcome page is disabled, the redirect pause is ignored. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-197939 AOS-198087	—	After configuring the heartbeat threshold in the WebUI, the VRRP IDs got reset to the default values. The fix ensures that the VRRP Ids are not reset to the default values. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197977 AOS-198348 AOS-198349	—	High memory consumption was observed in **dot1x1** and **dot1x2** processes. This issue occurred due to memory leak when the EAP-fragmentation feature was enabled. The fix ensures dot1x1 and dot1x2 process do not consume high memory. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.1
AOS-197993 AOS-198889	—	A managed device crashed unexpectedly and high CPU utilization was also observed on the managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-197994	—	FTP ALG in a session based ACL did not trigger correctly. The fix ensures that the FTP ALG works as expected. This issue occurred when DPI was enabled. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-198003	—	Network firewall dropped fragmented packets and hence clients faced connectivity issues. The fix ensures seamless connectivity. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198007	—	An AP was unable to ping a managed device and it switched between clusters. The fix ensures that the AP works as expected. This issue is observed in APs running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-198024	—	Some users were unable to access any page after the fifth page using the **Maintenance > Access Point** page in the WebUI. The fix ensures that the users are able to access any page. This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198110	—	The output of the **configuration device move to** command displayed the error message, **trusted Illegal Operation: There is Session ACL Defined. Cannot make the port untrusted.** The fix ensures that the command works as expected. This issue occurred when the **trusted** command was executed before and after configuring the session ACL. This issue was observed in Mobility Masters running AOS-W 8.3.0.9 or later versions.	AOS-W 8.3.0.9
AOS-198112	—	The WebUI displayed an error message **Invalid IPv4** when users tried to configure OmniVista 3600 Air Manager IPv6 address under **Configuration > System > AirWave** in the Mobility Master node hierarchy. The fix ensures that the OmniVista 3600 Air Manager IPv6 address can be configured using the WebUI. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198157	—	A stand-alone switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (Intent:cause: 86:56)**. The fix ensures that the switch works as expected. This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198165	—	The Authentication process crashed in a managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-198173 AOS-197956	—	The **show ap association** command displayed the association ID of a de-authenticated client and hence other clients were unable to use that particular association ID. The fix ensures that the association ID of a de-authenticated client is cleared. This issue occurred when the opmode was changed from wpa2 to wpa3. This issue was observed in Mobility Masters running AOS-W 8.5.0.10.	AOS-W 8.5.0.10
AOS-198218	—	After reboot, the status of the GRE tunnel of a standby switch was UP instead of DOWN in a VRRP instance and this resulted in a network loop. The fix ensures that the status of the GRE tunnel is correct. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198232	—	A managed device was unable to forward RADIUS server statistics through SNMP walk. This issue was resolved by combining the RADIUS server statistics of **802.1X** and **authentication** processes. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.5

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198241	—	The **show switches** command displayed the **Configuration State** of OAW-4850 switches and OAW-4104 switches, as **LAST SNAPSHOT**. This issue is resolved when the managed devices are upgraded to AOS-W 8.6.0.1. This issue was observed in managed devices after a successful upgrade of the Mobility Master to AOS-W 8.6.0.1.	AOS-W 8.6.0.1
AOS-198266	—	Some MAC authenticated clients were unable to reauthenticate even after enabling reauthentication. The fix ensures that the clients got reauthenticated. This issue was observed in stand-alone switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198281	—	The details of the **Up** time under **Managed network > Dashboard > Access Points > Access Points** table did not get updated correctly. The fix ensures that the correct details are displayed. This issue was observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-198290 AOS-198836	—	The output of the **show ip interface brief** command displayed incorrect radio channel information for AAC and non S-AAC managed devices. The fix ensures that the command works as expected. This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-198370	—	The **Managed network > Configuration > Task > Bulk configurationupload** page displayed an error message, **Incorrect header field(Controller VLAN)** while uploading the bulk edit configuration. The fix ensures that the WebUI does not display the error message. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198382	—	The output of the **show aaa state messages** command did not contain any name for the opcodes 204 and 253. The fix ensures that the correct names are mapped to each opcode. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198475	—	Some users were unable to upgrade the Mobility Master Virtual Appliance to AOS-W 8.5.0.0 or later versions. The fix ensures that the users are able to upgrade to a later version of AOS-W. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198483	—	The WebUI did not have an option to map the **rf dot11-60GHz-radio-profile** to an AP group. The fix ensures that the WebUI provides the option to map the **rf dot11-60GHz-radio-profile** to an AP group. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-198488	—	An AP rebooted unexpectedly and set an **F** flag. Enhancements to the wireless driver resolved this issue. This issue occurred when an 801.1X client was connected to the AP in bridge mode or tunnel mode for wired 802.1X authentication. This issue was observed in OAW-AP205H and OAW-AP303H access points running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198511	—	Few managed devices displayed an error, **Similar name certificate already exists on the same or different path. upload with a different name when a new certificate was uploaded**. The fix ensures that the new certificate is uploaded successfully. This issue occurred when the same new certificate was uploaded with its old name because the certificate manager received the crypto pki-import command twice for a single certificate addition. This issue was observed in managed devices running AOS-W 8.4.0.5 or later versions.	AOS-W 8.4.0.5
AOS-198527 AOS-198824	—	The output of **show switches** command displayed the configuration state of the managed device as **NO MM License**. This issue occurred due to license synchronization failure. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198542	—	A few clients were disconnected due to the **Tx fail reached maximum** error. The fix ensures that the state of variables in AP power-save state machine is updated correctly. This issue occurred due to an incorrect state of variables in the AP while peer **STA** is in power save state, that lead to the packets being sent out to the **STA** in power save state. Since the peer STA was in power save state, it did not acknowledge the packets and the AP exhausted the maximum retries and disconnected the clients. This issue was observed in OAW-AP315 access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-198604	—	The **Managed Network > Maintenance > Software Management > Controllers and Clusters** table displayed **Failed** as the upgrade reason in the WebUI. The fix ensures that the correct reason is displayed. This issue occurred when the managed devices had a cluster software upgrade. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-198605	—	A few APs failed to transition to a standby managed device during a datacenter failover. Enhancements to the wireless driver resolved this issue. This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-198610	—	A few managed devices were missing VRRP IP address after rebooting randomly. The fix ensures that the managed devices do not miss the IP addresses. This issue occurred in managed devices running AOS-W 8.3.0.6 in a cluster setup.	AOS-W 8.3.0.6
AOS-198669 AOS-198885	—	All rules configured using **aaa server-group** command were displayed in lowercase. The fix ensures that the rules are displayed in the correct letter cases. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198670	—	Forward slash **(/)** did not search for the next hit in CLI output. The fix ensures that the forward slash leads to the next hit in CLI output. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.8

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198671	—	An AP did not send authentication response frames to the client's authentication request. Enhancements to the wireless driver resolved this issue. This issue occurred due to a fake radar detection causing deferred channel change, when the CSA was enabled. This issue was observed in OAW-AP135 access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-198738	—	Some users were unable to access CLI using SSH. The fix ensures that the users can access CLI using SSH. This issue occurred in an IPv6 network when the multicast packets were not sent to the Mobility Master Virtual Appliance. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-198741	—	Some users were unable to configure IPsec tunnels on a few of third party VPN peers and the switch sent the error message, **INVALID SYNTAX.** The fix ensures that the users are able to configure IPsec tunnels. This issue occurred when the third party VPN peers propose IKEV2_FRAGMENTATION_SUPPORTED notify payload but did not send the IKE_AUTH payload as fragments. This issue was observed in stand-alone switches running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-198743	—	A few IPv6 enabled OAW-RAPs rebooted unexpectedly. The fix ensures that the APs work as expected. This issue occurred when the Mobility Master was configured with VRRP IP. This issue was observed in OAW-RAPs running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198787 AOS-198929	—	A OAW-RAP did not come up on a managed device when Verizon U730L modem was used. The fix ensures that the OAW-RAP comes up on the managed device. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198817 AOS-202396	—	A few APs failed to perform 802.1x authentication. This issue occurred when dot1x authenticated access points were upgraded to AOS-W 8.6.0.1. The fix ensures that the APs work as expected. This issue was observed in OAW-AP105 access points running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.1
AOS-198822 AOS-203559 AOS-203959	—	The **show iap table, show user-table internal** and **show global-user-table list** command outputs did not display any entries. The fix ensures that the correct command output is displayed. This issue occurred after upgrading to AOS-W 8.4.0.4. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-198825	—	A managed device displayed multiple stale entries for client-match pending events. The fix ensures that the managed device does not display multiple stale entries. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.9

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198828	—	APs did not send temperature values to the server. This issue occurred when the APs did not properly relay RTLS Aeroscout tag to the server. The fix ensures that the access points work as expected. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-198834 AOS-200088 AOS-200555 AOS-201312 AOS-202608	—	Some managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **rebooted due to Soft Watchdog reset (Intent:cause:register de:86:70:4)**. This issue was observed in OAW-4750XM switches running AOS-W 8.3.0.10 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.10
AOS-198849 AOS-198850	—	Some users were unable to configure 2.4 GHz radio profile in the **Configuration > System > Profiles > 2.4 GHz radio profile** page and the WebUI displayed the error message, **Feature is not enabled in the license**. The fix ensures that the users are able to configure the 2.4 GHz radio profile. This issue was observed in stand-alone switches running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198991	—	Users were unable to add VLAN to an existing trunk port using the **Configuration > Interfaces >VLANs** page of the WebUI. The fix ensures that the users are able to add the VLANs. This issue was observed in Mobility Masters running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.2
AOS-199205	—	A wired client in a different subnet could not ping the wireless client. This issue occurred when Policy Based Routing was added to the User Role for a wireless client. The fix ensures that the wired client is able to ping the wireless client. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-199217 AOS-199709	—	Cluster heartbeats were randomly missed on managed devices running AOS-W 8.3.0.10 or later versions in a cluster setup. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.10
AOS-199238	—	A managed device running AOS-W 8.4.0.4 or later versions displayed an error log, **ctamon_gsm_ update_section_intf_stats: Failed to Update GSM section intf_stats for , intf_num:0x40e3d6e0, error 43, error_htbl_key_not_found**. The fix ensures that the managed device works as expected.	AOS-W 8.4.0.4
AOS-199250	—	CPPM entries were not updated. This issue occurred when the **show airgroup cppm entries** command was issued. Enhancements to the CPPM request management resolved this issue. This issue was observed in managed devices running AOS-W 8.0.0.0.	AOS-W 8.0.0.0
AOS-199291	—	AAA server sent incorrect authentication response. The fix ensures that the AAA server does not send any incorrect response. This issue was observed in Mobility Masters running AOS-W 8.7.0.0.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199381	—	Users were unable to connect to the backup SSID of a OAW-RAP. This issue occurred when users tried to connect after an AP reboot. The fix ensures that seamless connectivity. This issue was observed in OAW-RAPs running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.2
AOS-199492	—	An AP was not displayed in the output of the **show airgroup aps** command and the auto associate feature stopped working. This issue occurred when an AirGroup domain was configured in distributed mode. The fix ensures that the AP is displayed in the output of the command and auto associate feature works 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-199539	—	All the profiles listed under an AP group were marked as default except the VAP profile. The fix ensures that all profiles are not marked as default. This issue was observed in managed devices running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-199551	—	The **show command** issued using API did not display the WPA passphrase text. The fix ensures that API displays the passphrase text intead of hash code.	AOS-W 8.7.0.0
AOS-199663 AOS-204384	—	After reboot of mesh auto APs, the configuration changes and mesh auto setting were reset. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.5
AOS-199667 AOS-199736	—	The system was unresponsive when the **show tech-support** command was executed. This issue occurred when the **show datapath dhcp binding** command duplicated the output entries. The fix ensures that the command works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-199696	—	Managed devices failed to establish connection with **IF-MAP** enabled ClearPass Policy Manager. This issue occurred when same certificates were added using different names. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-199707	—	A managed device running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20.** The fix ensures that the managed device works as expected.	AOS-W 8.6.0.0
AOS-199769	—	Users were unable to upgrade cluster using REST API. The response, **Are you sure you want to continue(y/n)** was displayed. The fix ensures that users are able to upgrade cluster using REST API.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199884	—	Mobility Master running AOS-W 8.5.0.5 or later versions logged the following error messages, **PAPI_ Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** The fix ensures that the error messages are not displayed.	AOS-W 8.5.0.5
AOS-199926	—	The **show ip ospf database** command displayed routes in reverse order. The fix ensures that routes are displayed in the correct order. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-199933	—	Mobility Master running AOS-W 8.4.0.4 or later versions failed to synchronize the RAP whitelist from Activate. This issue occurred when the full-name or the description fields of a RAP whitelist entry had a space. The fix ensures that the Mobility Master works as expected.	AOS-W 8.4.0.4
AOS-199947	—	The **Lic. FeatureBit** parameter under the License Client Table changed to enabled for Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance.This issue occurred when EVAL license was deleted and the licenses were displayed as 0. This issue was observed in stand-alone switches running AOS-W 8.3.0.11 or later versions.	AOS-W 8.3.0.11
AOS-199989	—	Managed device running AOS-W 8.6.0.2 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**. The fix ensures that the managed device works as expected.	AOS-W 8.6.0.2
AOS-200002 AOS-200649	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **crashed and rebooted due to Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. The fix ensures that the managed device works as expected. This issue occurred due to high CPU utilization. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200006	—	OAW-AP303H access points running AOS-W 8.5.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: CPU stall**. The fix ensures that the APs work as expected. **Duplicates:** AOS-199878, AOS-198897, AOS-200080, AOS-202641, AOS-205480, and AOS-205671	AOS-W 8.5.0.4
AOS-200071 AOS-201068	—	Some clients received **U-APSD disabled in association** response though they were able to connect to an SSID without any issues. This issue did not allow the client to enter power saving mode and reduced the talk time from 12 hours to 3 hours. The fix ensures that the clients do not receive any error message. This issue was observed in access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.6.0.2
AOS-200084 AOS-204429	—	OAW-AP305 access points running AOS-W 8.4.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT**. The fix ensures that the APs work as expected.	AOS-W 8.4.0.4

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200102 AOS-200779	—	Clients took a long time to failover to another managed device in a cluster. The fix ensures that the clients failover seamlessly. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a cluster setup.	AOS-W 8.5.0.5
AOS-200104 AOS-205532	—	The **profmgr** process crashed unexpectedly. The fix ensures that the **profmgr** process works as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-200130	—	Users were unable to change the port status to trusted or untrusted using either WebUI or CLI. The fix ensures that users can change the port status. This issue was observed in standby switches running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-200146 AOS-201993	—	The **STM** process on OAW-AP535 access points running AOS-W 8.4.0.0 or later versions crashed. The fix ensures that the access point works as expected.	AOS-W 8.6.0.0
AOS-200187	—	Mobility Master assigned duplicate IP addresses to Branch office switches from the VLAN pool. The fix ensures that duplicate IP addresses are not assigned. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200252	—	OAW-AP515 access points running AOS-W 8.6.0.2 or later versions logged an error message, **wlc_isr:MI_BUS_ERROR: MI_PSMX_INT 0x28002440, wlc_hw->clk:1.** The fix ensures that APs work as expected.	AOS-W 8.6.0.2
AOS-200277 AOS-204071	—	Managed devices running AOS-W 8.5.0.8 or later versions logged the error message, **There is only 996 MB left on the flash. At least 1000 MB of free flash space is recommended to keep the system stable**. The fix ensures that the error message is not displayed.	AOS-W 8.5.0.8
AOS-200319	—	OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.7 crashed and rebooted unexpectedly. The log file lists the reason for the event as **Kernel panic: WLAN FW crashes with Assertion vdev_handle->type == WAL_VDEV_TYPE_STA failed.** The fix ensures that the APs work as expected.	AOS-W 8.5.0.7
AOS-200420	—	Data traffic from VPNC concentrator was not routed back to the managed device. This issue occurred when the managed device was provisioned with two uplinks. The fix ensures that the managed device works as expected. This issue was observed in branch office switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200442	—	OAW-AP535 access points running AOS-W 8.5.0.7 crashed and rebooted unexpectedly. The log file listed the reason for the event as **WLAN FW Crash at ar_wal_peer.c:7218 Assertion !CHK_TID_FLG(ptid, WAL_TID_IN_SCHEDQ) failed.** The fix ensures that the APs work as expected.	AOS-W 8.5.0.7

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200446	—	Some users were unable to make changes to the Cluster Profile under **Configuration > Services > Cluster** tab of the WebUI. This issue occurred when there was no VRRP ID configured but the Cluster Profile requested for a VRRP passphrase. the fix ensures that the users are able to make changes to the cluster profile. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200462	—	A few managed devices running AOS-W 8.3.0.8 or later versions did not respond to the SNMP queries from Airwave regarding rogue information. This issue occurred when: there was a mismatch in the message length between **WMS** process and **AM** process. The managed device was running a higher version of AOS-W than that of the AP. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.8
AOS-200534 AOS-203370	—	The output of the **show ap active** command displayed **SA (AAC=0.0.0.0)**. The fix ensures that the STM process updates the AAC IP address when mesh radio is configured. This issue occurred because AAC IP address was not updated when a mesh AP was configured. This issue was observed in managed devices running AOS-W 8.5.0.7 or later versions in a cluster setup.	AOS-W 8.5.0.7
AOS-200568 AOS-202762 AOS-203588	—	GSM channel entries were not replicated from managed device to Mobility Master. The fix ensures that the GSM channel entries are replicated to the Mobility Master. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200582 AOS-201040 AOS-202577	—	Many sessions with **O** flag were created in a managed device. This issue occurred when OpenFlow connections flapped and a datapath session did not match the correct ACE rules. Enhancements to the ACE and ACL policies resolved this issue. This issue was observed in managed devices running AOS-W 8.5.0.7.	AOS-W 8.5.0.7
AOS-200588	—	A new radio profile that was created under an AP group in the **Configuration** > **AP Groups** page was not applied for that AP group in the WebUI. The fix ensures that the new profile is applied and stored under the relevant AP group. This issue occurred when the user selected an AP group from the **AP Groups** table and clicked **Profiles** to create a new profile under RF Management for that group. This issue was observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-200595 AOS-203897	—	WebUI displayed the error message, **Internal Server Error** when users copied files to SCP server using the **Diagnostics > Technical Support > Copy Files** page. The fix ensures that the WebUI does not display the error message. This issue was observed in OAW-4850 switches running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-200689	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **BUG:failure at net/core/skbuff.c:1647/consume_skb()!**. Enhancements to the wireless driver resolved the issue. This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.2

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200694	—	The **datapath** process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.7.0.0 in a cluster topology.	AOS-W 8.7.0.0
AOS-200699 AOS-200760	—	A few users were unable to delete the configured SNMPv3 trap hosts. The fix ensures that the users are able to delete the configured SNMPv3 trap hosts. This issue occurred due to the absence of IPv4 and IPv6 address type flags. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-200733	—	A few APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8**. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.3 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.3
AOS-200805	—	API returned a success message when an undefined cluster profile was upgraded. The fix ensures that a success message is not sent when an undefined cluster profile is upgraded.	AOS-W 8.7.0.0
AOS-200871 AOS-202284	—	After upgrading the managed devices to AOS-W 8.6.0.3, a large number of SNMP traps were sent to AirWave and the SNMP trap **wlsxAPChannelChange** did not display the **wlsxTrapAPARMChangeReason** field. The fix ensures that excessive SNMP traps are not sent to AirWave and the trap **wlsxAPChannelChange** displays all the fields.	AOS-W 8.5.0.7
AOS-200974	—	Incorrect device type information was displayed in the output of the **show user-table** command. The fix ensures that the correct device type information is obtained from CPPM and displayed in the user table of the managed device. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.2
AOS-200976 AOS-202577 AOS-204027 AOS-204410 AOS-204811 AOS-205437 AOS-206673	—	AirGroup stopped working on managed devices. The fix ensures that AirGroup works as expected. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions in a cluster setup.	AOS-W 8.6.0.3
AOS-201042	—	A large number of packet drops were observed in few APs. The fix ensures that the packets are not dropped. This issue occurred because the AP SAP MTU datapath tunnel was set to 1514. This issue was observed in APs running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201046	—	A couple of switches were unable to form a cluster. As a result, the output of the **show lc-cluster group-membership** command displayed the cluster status as SECURE-TUNNEL-ESTABLISHED and ISOLATED. The issue is resolved by increasing the heartbeat threshold so that both the switches have the same heartbeat timeout. This issue occurred because the switches were unable to exchange heartbeats between them. This issue was observed in OAW-4550 switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201068 AOS-202817	—	Some clients were getting **U-APSD disabled in association** response though they were able to connect to an SSID without any issues. This issue did not allow the client to enter power saving mode and reduced the talk time from 12 hours to 3 hours. This issue was observed in APs running AOS-W 8.3.0.0 or later versions. The fix ensures that the phones do not drop packets.	AOS-W 8.3.0.0
AOS-201117	—	A few users witnessed a constant increase in the **Rx Failure** parameter values in the output of the **show datapath frame apname** command. The fix ensures that the correct Rx Failure values are displayed. This issue occurred due to a misinterpretation between the Rx Failure and the Rx Packets values. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-201138	—	The VLAN broadcast-multicast traffic optimization configured in managed device blocked FDB update messages generated by the managed device. The fix ensures that broadcast-multicast traffic optimization allows the FDB update frames to pass through. This issue occurred when the **fdb-update-on-assoc** parameter under **wlan virtual-ap <profile-name>** command was enabled in a Layer-2 cluster. This issue was observed in managed devices and stand-alone switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201150 AOS-201997 AOS-203888 AOS-204328	—	An AP crashed and rebooted unexpectedly. The log file lists the reason for the event as: **AP Reboot reason: External-WDT-reset**. This issues occurred when the APboot used an older version of ESDK PCIE driver and set some bits, but the kernel did not reset the bits. The fix ensures that the AP works as expected. This issue was observed in 510 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-201152	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as BUGSoftLockup:CPU#1 stuck for 22s! [kworker/1:2:2288] PC:__udelay+0x30/0x48 Warm-reset. The fix ensures that the AP works as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-201200	—	The **show license-pool-profile** command did not display the output when executed in the **/mm/mynode** hierarchy. The fix ensures that the **show license-pool-profile** command displays the desired output. This issue was observed in Mobility Masters running AOS-W 8.3.0.6 or later versions.	AOS-W 8.5.0.5

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201210	—	When the **show aaa authentication-server radius statistics** command was executed, a few RADIUS authentication servers always displayed the **expAuthTm** value as 0. The fix ensures that the RADIUS authentication servers display the correct value of **expAuthTm** parameter. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201211	—	The **Configuration** > **Access Points** > **Campus APs** page did not display any AP in the WebUI though the **Dashboard** > **Infrastructure** > **Access Devices** page displayed the list of provisioned APs. The fix ensures that the list of APs are displayed in the **Configuration** > **Access Points** > **Campus APs** page in the WebUI. This issue was observed in Mobility Masters running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-201240	—	A few users were unable to add a trusted VLAN using the **Interface** > **Ports** > **Allowed VLANs** page and the WebUI displayed the **VLANs common found in Trusted & Untrusted** error message. The fix ensures that the users are able to add the trusted VLAN in the **Allowed VLANs** page. This issue occurred when the Mobility Master automatically issued the **no trusted vlan** command. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.2
AOS-201250	—	A few managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - low on free memory**. The fix ensures that the managed devices work as expected. This issue was not limited to any switch platform or AOS-W release version.	AOS-W 8.5.0.5
AOS-201273 AOS-201395	—	IPsec tunnels were not established between Mobility Master and managed devices in an IPv6 environment, and switch-IP address is not displayed in the managed devices. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.0
AOS-201329 AOS-203946	—	In a configuration node hierarchy, CPsec toggling did not work at the lower nodes. This issue occurred when the managed device was downgraded from AOS-W 8.3.0.12 to AOS-W 8.3.0.10. This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions. The fix ensures that the CPsec toggling works even at the lower nodes.	AOS-W 8.3.0.10
AOS-201439 AOS-201448	—	A few APs crashed and rebooted unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**. The fix ensures that the APs work as expected. This issue was observed in OAW-AP303H Series access points running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201541	—	Configuring a radius modifier in the WebUI required configuring a second dynamic field but it was optional in CLI. This issue is resolved by allowing the configuration of the radius modifier without having to configure the second dynamic field in the WebUI. This issue was observed in a managed device running AOS-W 8.6.0.2.	AOS-W 8.6.0.2

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201547	—	The **show openflow-controller forwarding-db** command was not part of tech-support. This issue is resolved by adding the **show openflow-controller forwarding-db** command to tech-support. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-201581	—	A few APs continuously displayed unnecessary syslog messages. The fix ensures that the syslog messages are not displayed. This issue occurred when one or more clients were added to the APs, as well as after reboot of the managed device and the APs. This issue was observed in 510 Series access points running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201612	—	Role policies configured on a Mobility Master were displayed in a different order on the managed devices in the **Configuration** > **Roles & Policies** > **Roles** tab in the WebUI. The fix ensures that the role policies are displayed in the correct order in the WebUI. This issue occurred when the default ACLs get deleted during the initial configuration synchronization after upgrade. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.8
AOS-201681	—	Data traffic to clients on radio 2 failed unexpectedly on APs. The fix ensures that the APs work as expected. This issue occurred due to cluster failover. This issue was observed in tri-radio enabled OAW-AP555 access points running AOS-W 8.6.0.3.	AOS-W 8.6.0.3
AOS-201706	—	The BSSID of few APs in MultiZone were wrongly classified as **suspected-rogue** though the BSSIDs were added as valid in the **wms ap <bssid> mode valid** CLI command. The fix ensures that BSSIDs are always classified as valid for the APs. This issue occurred when MultiZone was enabled and APs were assigned to the Data zone. This issue was observed in APs running AOS-W 8.6.0.2 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.2
AOS-201735	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: BadPtr:0000004c PC:anul_aon_rbuf_rd+0x140/0x1c8 [anul] Warm-reset**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.2
AOS-201831	—	The **S-UAC** process in a cluster member sent the **fdb-update-on-assoc** message sporadically. This issue is resolved by sending the **fdb-update-on-assoc** message only when **fdb-update-on-assoc** is enabled and the station is not dormant. This issue was observed in managed devices running AOS-W 8.5.0.5 in a cluster topology.	AOS-W 8.5.0.5
AOS-201955 AOS-202341	—	A managed device, running AOS-W 8.3.0.8 or later versions, crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) ((Intent:cause:register 54:86:0:2c)**. This issue occurred due to incorrect ingress and egress values. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.8

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202029	—	Captive portal customizations were not synchronized to the managed device. That is, the default page was displayed although the customizations were saved when the captive portal profile name was configured with blank spaces. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions. This issue is resolved by adding double quotes in the file name.	AOS-W 8.3.0.7
AOS-202034	—	The **STM** process in a managed device crashed unexpectedly, due to which few APs were unable to connect to the managed device. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions. The fix ensures that the managed devices works as expected.	AOS-W 8.6.0.0
AOS-202085 AOS-204529 AOS-204861 AOS-206217	—	The IP address of Wired Clients in **Dashboard > Overview > Clients** page was displayed as **0.0.0.0**. The fix ensures that correct IP addresses are displayed. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-202110	—	The Active switch field displayed a hyphen (-) for some APs under **Dashboard > Infrastructure > Access Devices** page in the WebUI. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions. The fix ensures that the Active switch column displays the IP address for all the APs.	AOS-W 8.2.0.0
AOS-202129 AOS-204127	—	The **Configuration > AP groups** page did not have the **Split radio** toggle to enable the tri-radio feature. The fix ensures that the toggle switch is available. This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-202195	—	A managed device, running AOS-W 8.3.0.6 or later version, crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the managed device works as expected.	AOS-W 8.3.0.6
AOS-202257	—	Some OAW-40xx Series switches displayed the warning message, **At least 1000 MB of free flash space is recommended to keep the system stable. Please clean up your flash filesystem** although some switches in the series have less than1GB memory allocated to it. This issue is resolved by changing the warning message to **At least 600 MB of free flash space is recommended to keep the system stable. Please clean up your flash filesystem**. This issue was observed in OAW-40xx Series switches running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202290	—	The error message, **Cannot modify existing server-group from different node in config path** was displayed when users tried to create or modify aaa server group. This issue occurred when similar naming conventions were used for different folders under the same hierarchy. This issue was observed in Mobility Masters running AOS-W 8.5.0.6 or later versions. The fix ensures that the Mobility Master works as expected.	AOS-W 8.5.0.6

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202309	—	Few APs running AOS-W 8.1.0.0 rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.1.0.2
AOS-202341	—	A managed device running AOS-W 8.3.0.8 or later versions crashed and rebooted unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) ((Intent:cause:register 54:86:0:2c).** The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.8
AOS-202370	—	Some managed devices reset when the **activate sync** command was issued. This issue occurred when the node paths that are configured for Activate and Mobility Master use different cases. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. The fix ensures that the case insensitive function is used when the two nodes are compared.	AOS-W 8.5.0.5
AOS-202423	—	A switch crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the switch works as expected. This issue was observed in OAW-4010 switches running AOS-W 8.6.0.2 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.2
AOS-202426 AOS-203652	—	Few 510 series APs running AOS-W 8.6.0.4 crashed and rebooted unexpectedly. The log files listed the reason for the event as **PC is at: wlc_phy_enable_hwaci_28nm+0x938 - undefined instruction: 0 [#1]**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.4
AOS-202448	—	Few OAW-AP535 access points running AOS-W 8.6.0.3 rebooted unexpectedly. The log files listed the reason for this event as **FW Crash: wlan_peer.c:408 Assertion !peer->peer_delete_in_progress failed**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.3
AOS-202450	—	Remote APs, running AOS-W 8.5.0.7 or later versions, rebooted unexpectedly. This issue occurred when Mobility Master modified the existing whitelist database entries when the **activate whitelist download** command was executed. The fix ensures that the Remote APs work as expected.	AOS-W 8.5.0.7
AOS-202515 AOS-202658	—	Few AP running AOS-W 8.5.0.2 or later versions, crashed and rebooted unexpectedly. The log file listed the reason for the event as **Panic:assert Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.2
AOS-202551	—	An AP logged the error message, **An internal system error has occurred at file parser.c function parse_mgmt line 656 error parse_mgmt Size mismatch on frame**. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.7 or later versions. The fix ensures that the AP works as expected.	AOS-W 8.5.0.7

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202640	—	The **stm** process in a managed device crashed unexpectedly. This issue occurred because of a missing null check when accessing DNS record for zero IP insertion. This issue is resolved by adding the null check before accessing the DNS record. This issue was observed in managed devices running AOS-W 8.0.0.0.	AOS-W 8.0.0.0
AOS-202691	—	The **Key Management** column in the **Configuration > WLANs** page of the WebUI displayed multiple **wpa2-psk-tkip** entries. This issue occurred when multiple wpa2-psk-tkip opmode SSIDs were created. This issue was observed in stand-alone controllers running AOS-W 8.5.0.4 or later versions. The fix ensures that the Key Management column displays only one entry for **wpa2-psk-tkip**.	AOS-W 8.5.0.4
AOS-202739	—	Some APs, running AOS-W 8.3.0.9, were displaying the error message, **WPA Passphrase not configured for AP because the wpa_psk_keytype was set to '0'**. The fix ensures that the APs work as expected.	AOS-W 8.3.0.9
AOS-202743 AOS-203498 AOS-203507 AOS-204322	—	The **Configuration > Interfaces > VLANs** tab did not display the IP addresses of Mobility Master and managed devices. The fix ensures that WebUI displays the IP addresses. This issue was observed in Mobility Masters and managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-202803	—	The **cluster was fractured during the upgrade** error message was displayed during the cluster live upgrade process. As a result, the cluster live upgrade was not performed. The fix ensures that the cluster live upgrade process is performed successfully and the error message is not displayed. This issue was observed in Mobility Masters running AOS-W 8.5.07 or later versions.	AOS-W 8.5.0.7
AOS-202994	—	All the processes were killed when the Reload API was run. The fix ensures that the Reload API works as expected. This issue was observed in Mobility Master running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203097	—	WebUI prompted that additional VLANs will be deleted when user tried to delete a VLAN. This issue occurred in a stand-alone switchesr running AOS-W 8.3.0.10 or later versions. This issue is resolved by removing the wrong reference of port channel with VLAN in the VLAN table.	AOS-W 8.3.0.10
AOS-203135	—	The **AP ASAP** process crashed on a managed device. This issue was observed in OAW-AP310 Series access points running AOS-W 8.4.0.6 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.4.0.6
AOS-203168	—	Some managed devices disconnected from the cluster frequently. Also, the cluster heartbeats were randomly missed, which led to packet loss. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions in a cluster setup. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.3

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203170	—	The **class attribute** field was missing in accounting packets of the VIA connection profile. This issue occurred when IKEv2 was enabled in VIA connection profile. This issue was observed in managed devices running AOS-W 8.4.0.1 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.4.0.1
AOS-203184	—	Users were unable to perform captive portal authentication when login URL of the captive portal profile pointed to ClearPass Policy Manager. The fix ensures that the users are able to perform captive portal authentication. This issue was observed in managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-203183	—	Incorrect values were returned when an SNMPGet was performed in a managed device running AOS-W 8.2.0.0 or later versions This issue occurred while collecting AP LLDP neighbor details. The fix ensures that the correct values are displayed when the SNMPGET is executed.	AOS-W 8.6.0.2
AOS-203201	—	The managed device was unable to download configurations from the Mobility Master using VPNC. This issue was observed in managed devices running AOS-W 8.2.2.6 or later versions. The fix ensures that the managed device works as expected.	AOS-W 8.2.2.6
AOS-203219	—	The URL hash key was not appended to the captive portal redirect URL. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions. The fix ensures that the URL Hash Key is hashed to the redirect URL.	AOS-W 8.6.0.4
AOS-203237	—	A UDMD core file was generated in an AP. This issue occurred because the allocated memory was more than the system memory. Improvements to memory management resolved this issue. This issue was observed in APs running AOS-W 8.7.0.0	AOS-W 8.7.0.0
AOS-203249	—	A OAW-4850 switch running AOS-W 8.3.0.8 rebooted, lost all configuration, and booted up on an alternative partition that was running a different AOS-W version. The fix ensures that the switches work as expected.	AOS-W 8.3.0.8
AOS-203336	—	The **Dashboard** > **Infrastructure** > **Access Points** page of the WebUI and the **show log** command output display different values for last AP reboot time. The fix ensures that the correct values are displayed for last AP reboot time. This issue was observed in stand-alone switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-203357	—	Traffic outage was observed in a managed devices when the role of wired user gets updated as a tunneled user with a different VLAN. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.7.0.0
AOS-203398	—	An iBeacon message that was sent from a managed device to an external server had an incorrect timestamp. The fix ensures that the managed device sends the iBeacon message with the correct timestamp. This issue was observed in managed devices running AOS-W 8.6.0.3.	AOS-W 8.6.0.3

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203702 AOS-204024 AOS-204423 AOS-204544 AOS-205440 AOS-207087 AOS-207197	—	OAW-40xx Series, OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM switches running AOS-W 8.5.0.8 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)** . The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.8
AOS-203119	—	APs, configured as a mesh port, rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: aruba bin debug dev etc lib mnt proc sbin sys tmp usr var TARGET ASSERT DUE TO INCORRECT CRC LEGACY RECOVERY aruba bin debug dev etc lib mnt proc sbin sys tmp usr var**. This issue was observed in OAW-AP387 access points running AOS-W 8.4.0.2 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.4.0.2
AOS-203322 AOS-205170	—	The command **tar clean logs** did not remove the logs.tar.7z file. This issue was observed Mobility Masters running AOS-W 8.6.0.4. The fix ensures that the command works as expected.	AOS-W 8.6.0.4
AOS-203374	—	VIA authentication timed out although the server responded without any delay. This issue was observed in OAW-4550 switches running AOS-W 8.0.0.0 or later versions. The fix ensures that the VIA authentication works without delay.	AOS-W 8.3.0.0
AOS-203418	—	The custom server-certificates were ignored when the factory certificates were sent by the Remote APs. This issue occurred because the Remote APs did not trust the certificates sent by the Mobility Master Virtual Appliance. This issue was observed in Remote APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-203438	—	The configuration for EIRP made through the WebUI were not visible in the stand-alone switches running AOS-W 8.6.0.3. The fix ensures that the configuration for EIRP is visible.	AOS-W 8.6.0.3
AOS-203459	—	It took a long time to import a guest provisioning file with very few users to the Mobility Master's local database. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions. The fix ensures that the file is imported in optimum time.	AOS-W 8.6.0.3
AOS-203498	—	After upgrading to AOS-W 8.5.0.7, IP address field is blank in **Configuration > Interaces > VLANs > VLAN** page in the managed devices WebUI. The fix ensures that the IP address is displayed.	AOS-W 8.5.0.7

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203521	—	A warning message, **An internal system error has occurred at file sapd_stp.c function sapd_add_stp_if line 159 error Unable to add eth2 to STP device: Device or resource busy** is displayed in the log files of the managed device although no configuration changes were made. This issue was observed in managed devices running AOS-W 8.3.0.0 or later version. The fix ensures that the warning message is not displayed.	AOS-W 8.3.0.0
AOS-203585 AOS-204245	—	An error message, **aruba_change_channel 735 Waiting for VAP INIT to complete** was displayed in the log files for OAW-AP334 access points running AOS-W 8.7.0.0. This issue is resolved by changing the logging level to debug.	AOS-W 8.7.0.0
AOS-203712 AOS-205655	—	An Avaya Spectalink wireless client device rebooted unexpectedly with the error message, **No AVPP response from 192.168.249.001**. The fix ensures that the client device works as expected. This issue is observed in managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-203859	—	A Windows client was unable to get WINS server information from a managed device. The fix ensures that the Windows client gets the WINS server information from a managed device. This issue was observed in managed devices running AOS-W 8.3.0.11 or later versions.	AOS-W 8.3.0.11
AOS-203860	—	The VIA installer file was unable to synchronize the logo, banner, or welcome html between the Mobility Master and managed devices. This issue was observed in Mobility Masters and managed devices running AOS-W 8.3.0.0 or later versions. The fix ensures that the VIA installer is able to synchronize all the files.	AOS-W 8.6.0.2
AOS-203927	—	VIA license consumption was higher than the number of users connected to VIA in a managed devices running AOS-W 8.6.0.2 or later versions. The fix ensures that the number of licenses being used matches the number of users connected.	AOS-W 8.6.0.2
AOS-203934	—	User was unable to access previously backed up data when the new backup-logs application was installed. This issue was observed in managed devices running AOS-W 8.7.0.0. The fix ensures that the user is able to access the backed up data.	AOS-W 8.7.0.0
AOS-203958	—	Blacklisted clients are visible in **Dashboard > Security > Blacklisted Clients** although these clients were removed using the WebUI. This issue was observed in Mobility Masters running AOS-W 8.6.0.2.	AOS-W 8.6.0.4
AOS-204025	—	Users were unable to add VLANS to the **Allowed VLANs** field for the trunk port under **Configuration** > **Interfaces** > **Ports** page in the WebUI. The fix ensures that the VLANs are added and displayed in **Allowed VLANs** field. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204120	—	Upgrade of a Nordic USB dongle failed when an unsupported TI USB dongle was plugged in to an AP. This issue occurred when a TI USB dongle was detected before a Nordic USB dongle. This issue is resolved by skipping the upgrade of the unsupported TI USB dongle and checking the next USB dongle in the device list. This issue was observed in APs running AOS-W 8.7.0.0	AOS-W 8.7.0.0
AOS-204142	—	A few users were assigned the default 802.1X roles from AAA profile instead of SDR-configured roles. The fix ensures that the SDR-configured roles are assigned to the users. This issue occurred when the **no cert-cn-lookup** parameter under **aaa authentication dot1x** command was configured on the 802.1X profile. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.6.0.4
AOS-204304	—	The k-value for 5 GHz in 80 MHz was incorrect for some APs. This issue occurred when the calibration values were not correct. This issue is resolved by updating the k-value of 36/80, 149/80, and 36/40 for the APs. This issue was observed in OAW-AP505 and OAW-AP515 access points running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-204326 AOS-204591	—	Clients were unable to connect to OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.4 . This issue occurred on APs operating in 5 GHz mode. The fix ensures seamless connectivity. The issue occurred when the APs negotiated a higher power from the switch through LLDP software.	AOS-W 8.6.0.4
AOS-204414	—	Radius source interface was not working in managed devices running AOS-W 8.3.0.8 or later versions. This issue occurred when RadSec was enabled and managed devices did not accept global radius source-interface configuration for RadSec connections. The fix ensures that the radius source interface works as expected in managed devices.	AOS-W 8.3.0.8
AOS-204428 AOS-204450	—	OAW-AP303H access points running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt.** The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
AOS-204532	—	Configuration made on managed devices were not displayed in the Mobility Master that the managed devices were connected to. This issue was observed in managed devices running AOS-W 8.4.0.1 or later version. The fix ensures that the managed devices work as expected.	AOS-W 8.4.0.1
AOS-204367	—	A map name was not displayed in the output of the **show crypto ipsec sa** command. The fix ensures that the **show crypto ipsec sa** command displays the output. This issue was observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-204628	—	APs provisioned as Remote APs successfully form an IPsec tunnel but did not broadcast SSIDs. This issue occurred when the custom elliptical curve certificate was used to authenticate. This issue occurred in OAW-AP320 Series access points running AOS-W 8.3.0.0 or later versions. The fix ensures that the APs are able to broadcast SSID.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204663	—	The **show running-config** command did not display a few user roles. The fix ensures that the command displays all user roles. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-204691	—	Some VIA users were unable to download connection profile. This issue occurred when the user role exceeded 32 characters. The fix ensures that VIA users are able to download the connection profile. This issue was observed in stand-alone switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.2
AOS-204697	—	The **Auth** field for 802.1X PUTN users was incorrectly updated as **tunneled-user-MAC** instead of **tunneled-user-Dot1x** when the s**how user-table** command was executed. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions. The fix ensures that the correct output values are displayed when the **show user-table** command is executed.	AOS-W 8.6.0.4
AOS-204917 AOS-205979	—	The **dpagent** process crashed unexpectedly. The log file listed the reason for this event as **Memory usage limit exceeded for process: dpagent current pages**. The fix ensures that the dpagent process works as expected. This issue was observed in managed devices running AOS-W 8.5.0.10.	AOS-W 8.5.0.10
AOS-204924	—	When the switch was downgraded from AOS-W 8.5.0.8 to AOS-W 8.3.0.6, it crashed continuously. The fix ensures that the switch works as expected. This issue was observed in OAW-4005 switches running AOS-W 8.3.0.6.	AOS-W 8.6.0.2
AOS-204948	—	An AP crashed and rebooted. The log file listed the reason for this event as **kernel panic: Fatal exception with NIP: e445c71c LR: e4490ac0 CTR: c0567b30**. The fix ensures that the AP works as expected. This issue was observed in access points running AOS-W 8.5.0.7.	AOS-W 8.5.0.7
AOS-205010	—	The **OFA** process crashed in a switch, due to an increase in the number of IP user events. The fix ensures that the switch works as expected. This issue was observed in switches running AOS-W 8.5.0.8.	AOS-W 8.5.0.8
AOS-205013	—	Layer 2 VLANs configured with option 82 were missing when the managed devices were reloaded. The fix ensures that VLAN configurations are available after reload. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-205025	—	The switch did not retrieve cluster inner-IP from the whitelist database as the request was initiated from an OAW-IAP. This issue occurred when a switch used external authentication for OAW-RAP whitelisting. This issue is resolved by provisioning the OAW-IAP as OAW-RAP. This issue was observed in switches running AOS-W 8.6.0.4.	AOS-W 8.6.0.4

Table 7: *Resolved Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205098	—	Since the **profmgr** process was continuously restarting on the Mobility Master with controller-ipv6 loopback configured on managed devices, the configuration was not pushed to the managed devices. The fix ensures that the **profmgr** process works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.8.	AOS-W 8.5.0.8
AOS-205112	—	Managed device running AOS-W 8.3.0.7 or later versions rebooted unexpectedly. This issue occurred when the **OFA** process crashed due to low memory. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.7
AOS-205253 AOS-205644	—	SSH public key authentication failed on OpenSSH v7 client. The fix ensures that SSH public key authentication works as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-205634	—	The WebUI did not display the port channel membership. This issue occurred when port members were added to the PC-0 port channel. The fix ensures that the WebUI displays the port channel membership. This issue was observed in managed devices running AOS-W 8.6.0.4.	AOS-W 8.6.0.4
AOS-205903	—	The hostname of a managed device changed to a random value and persisted even after reconfiguring the hostname. The fix ensures that the hostname is retained. This issue was observed in managed devices running AOS-W 8.5.0.8.	AOS-W 8.7.0.0
AOS-205972	—	The **show ip route** command did not provide the correct output. The fix ensures that the **show ip route** command displays the correct output. This issue was observed in managed devices running AOS-W 8.4.0.0.	AOS-W 8.4.0.0

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

Limitations

Following are the limitations observed in this release.

Support for WPA3+802.11r in Multi-version

A Mobility Master and managed device should run at least AOS-W 8.7.0.0 to use 802.11r or fast BSS transition on WPA3 security mechanisms.

In a multi-version environment, that is, if a managed device runs AOS-W version 8.6.0.0 or lower and if 802.11r is enabled with a WPA3 opmode, a configuration error occurs. This can be verified by issuing the **show switches** and **show configuration failure** commands.

Known Issues

Following are the known issues observed in this release.

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191031	—	Few 802.11ax clients experience poor MU-MIMO performance. This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-199545	—	An AP beacons with high efficiency even though there are no clients connected. This issue is observed in 500 Series access points running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-199564	—	ZTP fails with option 43 although all the attributes are correctly entered. This issue is observed on Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.0.0
AOS-200251	—	Multiple GRE firewall parameters can be configured simultaneously. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-200533	—	The Skype for Business SDN API does not work with Skype SDN server 2019. This issue is observed in a Mobility Masters running AOS-W 8.7.0.0.	AOS-W 8.7.0.0

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201098		The PPPoE connection is lost when ACL is either configured or removed from the uplink port. This issue is observed in OAW-4005 switches running AOS-W 8.2.0.0 or later versions. **Workaround:** Perform subsequent flapping of the PPPoE interface.	AOS-W 8.4.0.0
AOS-201264	—	A VIA client fails to send IKE packets to the managed device for rekey in an IPv6 network. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-201286	—	The **Boot partition**, **Backup partition**, **Country**, and **Serial number** fields are not displayed after clicking **Show more > Name** in the **Dashboard > Infrastructure > Controllers** page in the WebUI for a dual stack or native IPv6 managed device although these fields are displayed for an IPv4 managed device. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202038	—	An incorrect SNR value is displayed in the Mesh portal dashboard. This issue is observed in OAW-AP555, OAW-AP535, and OAW-AP505 access points running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202095	—	The value of RX and TX bytes is not updated in the **Wired Clients** dashboard. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202346	—	In a dual stack or native IPv6 deployment, when the **no ipv6 enable** command is issued on the Mobility Master, all managed devices lose connectivity to the Mobility Master and when the command is issued on a managed device, that managed device loses connectivity to the Mobility Master. This issue is observed in Mobility Master running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202413	—	APs are unable to obtain IP addresses because only /64 IPv6 subnet masks are supported in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202424	—	When users remove the AirGroup profile by issuing sub-commands under **airgroupprofile activate** command, the sub-commands sometimes do not work. This issue occurs when the users disable or enable any existing AirGroup profile. This issue is observed in both Mobility Master and managed devices running AOS-W 8.6.0.2 or later versions. **Workaround:** Issue the **no airgroupprofile activate** or **airgroupprofile activate** command.	AOS-W 8.6.0.2
AOS-202531	—	After a live upgrade is initiated, the user is unable to stop the upgrade as the **Cancel** button is disabled in the WebUI. This issue is observed managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202781	—	Clients are unable to ping any device in the network and an error message, **An internal system error has occurred at file gsm_sapm.c function sapm_lookup_gsm_bucketmap line 263 error sapm_lookup_gsm_bucketmap failed for Essid v4_cluster_v6_ssid (len 18) Error=43 (error_htbl_key_not_found)** is displayed. This issue occurs due to cluster failover. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202829	—	AirMatch assigns allow_all after solver run when an AP is operating in Tri-radio mode. This does not allow HE-pooling steer attempts to complete. This issue is observed in APs running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-202923	—	When the **show datapath frame** command is executed, an increase in the **Invalid GRE Fragment Received** counter is observed in switches running AOS-W 8.7.0.0. This issue occurs because the switch IPv6 GRE tunnel fragmentation is not working as expected.	AOS-W8.7.0.0
AOS-202956	—	The managed device is not listed under the Mobility Master, although the managed device is able to ping the Mobility Master. This issue is observed in OAW-4104 switches running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203179	—	The branch office switch is not listed under the Mobility Master when VPNC master is changed from IPv4 to IPv6, although there is a tunnel established between VPNC and branch office switch. This issue is observed in switches running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203495	—	A local IPv6 prefix is displayed as [128] instead of /64, information related to IPv6 RA Gateway is not displayed, and a managed device does not send Router Solicitation. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203528	—	The output of the **show tech-support user mac <client-mac>** command does not display the **show user-table ip** and **show ap remote debug mgmt-frames ap-name <ap-name>** sub-commands. This issue is observed in OAW-4024 stand-alone switches running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203545	—	OAW-AP535 access points running AOS-W 8.7.0.0 crashes and reboots unexpectedly. The log file lists the reason for the event as **rebooted caused by internal watchdog reset.**	AOS-W 8.7.0.0
AOS-203606	—	OAW-AP535 access points running AOS-W 8.7.0.0 crashes due to firmware assert. The log file lists the reason for the event as **PC : 0x00000000, ERR_COMMON_PHY_NOC_ERR_TIMEOUT:0 Ucode Asserted:, PHYA**.	AOS-W 8.7.0.0
AOS-203670	—	An error occurs when **Certificate** type is changed from **Custom** to **Factory** due to incomplete commands. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203675	—	User is able to configure Mobility Master Virtual Appliance with Mobility Master Hardware Appliance. This issue is observed in OAW-41xx Series switches configured as a Mobility Master Virtual Appliance.	AOS-W 8.7.0.0

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203743	—	DPI classification does not work when the HTTP based rule is applied to custom-app. This issue is observed managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203951	—	The **Show Report** option displays an error message in the **Diagnostics** > **Access Point** > **System Information** page in the WebUI. This issue occurs when the user creates the AP file name by using **–** (hyphen) or _ (underscore) character in the **Output file name** field of the **System Information** page. This issue is observed in APs running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-204032	—	The SNMP trap for OID **wlsxNUserEntryAuthenticated** is not generated when the user is authenticated using 802.1X RADIUS server. This issue is observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-204503	—	The stateless address auto-configuration (SLAAC) is not functional when DNS-SSL is advertised by the switch. This issue is observed in access points running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-204551	—	Few iPhone clients, connected to wpa3-sae-aes profile, are unable to roam between APs. This issue occurs when **opmode-transition** is disabled. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-204553	—	Mesh point entry is missing from the mesh link table after successfully setting up mesh. This issue observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-204834	—	AP rebootstraps every 10-15 minutes and clients are failing to boot up on the AP. This issue is observed IPv6 access points connected to OAW-4104 switches and Mobility Master Virtual Appliance in a native IPv6 branch office deployment.	AOS-W 8.7.0.0
AOS-205087	—	A branch office switch does not come up on a standby Mobility Master. This issue is observed after Layer-2 VRRP switchover in a dual-stack deployment. This issue was caused due to unsupported additional configurations such as local IPv6 in the branch office switch connected to the Mobility Master. **Workaround**: Remove the additional configurations.	AOS-W 8.7.0.0

AOS-205140	—	AppRF ACLs using a voice role are blocking WebRTC calls and this issue is observed when users upgrade to AOS-W 8.7.0.0. This issue occurs when WebRTC audio and video ACLs are not part of the default **voip-applications-acl**.
		Workaround: Add WebRTC audio and video ACLs to the user role using the following command:
		`ip access-list session webrtc`
		`any any app alg-webrtc-audio permit`
		`any any app alg-webrtc-video permit`	

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205266	—	Few OAW-AP305 and OAW-AP325 access points running AOS-W 8.7.0.0 detect fake radar of **typeid 11** although the APs are in the DFS channel.	AOS-W 8.7.0.0
AOS-205371	—	Few AP-505H access points running AOS-W 8.7.0.0 are displayed as AP-50 on AirWave.	AOS-W 8.7.0.0
AOS-205506	—	The **Controllers > Infrastructure > Clusters > Controllers** page in the WebUI of a Mobility Master displays an incorrect number of managed devices and cluster members. This issue is observed in a dual stack or native IPv6 deployment with managed devices running AOS-W 8.7.0.0	AOS-W 8.7.0.0
AOS-205573	—	Clients are unable to establish a tunnel if the peer gateway matches the secondary IPv6 address because the IKE process establishes a tunnel only using the first available IPv6 address as the source. This issue occurs when a multi-homed IPv6 VLAN interface is configured to be part of site-to-site VPN. This issue is observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.7.0.0
AOS-205606	—	AOS-W Switch is unable to derive a Downloadable user role from IPv6 ClearPass Policy Manager. This issue is observed in a Per-User Tunneled Node setup.	AOS-W8.7.0.0
AOS-205621	—	Following issues are observed in a bridge mode captive portal: ■ The certificate private key is not encrypted on AP flash. ■ The certificate is due to expire on September 8th, 2020 This issue is observed in APs running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-205663	—	Few OAW-AP505 access points running AOS-W 8.7.0.0 detect fake radar of **typeid 12**.	AOS-W 8.7.0.0
AOS-205666	—	Performance degradation is observed in OAW-AP535 access points running AOS-W 8.7.0.0 when **OFDMA** is enabled in **wlan he-ssid-profile** command.	AOS-W 8.7.0.0
AOS-205726	—	The output of **show mon-serv-lc-table** command on a Mobility Master does not display a managed device that is in the topology. This issue is observed in a setup where the Mobility Master is connected to managed devices configured in a dual stack.	AOS-W8.7.0.0
AOS-205749	—	In a cluster configuration, the Tx counters are not incremented over LACP. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-205981	—	Few OAW-AP225 access point running AOS-W 8.7.0.0 detect fake radar of **typeid 8**.	AOS-W 8.7.0.0

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206057	—	Poor performance is observed in OAW-AP535 access points running AOS-W 8.7.0.0 when the MU-MIMO is enabled.	AOS-W 8.7.0.0
AOS-206084	—	Few echo packets are transmitted to the mesh portal although the mesh portal is down. This issue is observed in mesh points running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206128	—	Managed devices lose connectivity with Mobility Master and all the APs get disconnected from the Mobility Master. This issue occurs when the uplink port of the Mobility Controller Virtual Appliance is marked as not trusted. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206146	—	Clearing the L2 GRE tunnel counters fails. This issue is observed in a dual stack or native IPv6 topology with managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206147	—	A directly connected L2 GRE tunnel is displayed as default route when the **show ipv6 route** command is issued. This issue is observed in a dual stack of native IPv6 deployment with managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206163	—	The status of **STM** process changes to busy after 15 SSIDs are created in a MultiZone cluster. This issue is observed in OAW-4550 switches running AOS-W 8.7.0.0. **Workaround:** Restart the switch.	AOS-W 8.7.0.0
AOS-206169	—	The log file of a managed device displayed **the <ERRS> |pim| System encountered an internal communication error. Error occurred when message is being sent fr om source application 127.0.0.1:PIM destination application 0.0.0.0:PIM at file papi_intf.c function papi_send_status_callback line 155.** error message. This issue is observed in a dual stack of native IPv6 deployment with managed devices running AOS-W 8.7.0.0.	AOS-W 8.
AOS-206172	—	The DDS peer is deleted, due to an error in the crypto-map creation. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206207	—	When the **show aaa server-group** command is executed, a value is displayed against VLAN but not the role although the Server Derivation Rule (SDR) is configured with two rules setting; VLAN and role values. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206330	—	The **wl0: PSM microcode watchdog fired at 144523 (seconds). Resetting" "psm watchdog at 144523 seconds** error message is displayed on OAW-AP515 access points connected to switches running AOS-W 8.7.0.0.	AOS-W8.7.0.0

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206357	—	The log file of a managed device displayed **<ERRS> |ucm| Unexpected UCC runtime error returned zero replicator IP with SUCCESS !!"** error message although UCC is not supported in native IPv6 deployment. This issue is observed in a dual stack of native IPv6 deployment with managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206430	—	The WebUI does not have an option to configure a managed device as VPNC, but this option is available in CLI.	AOS-W8.7.0.0
AOS-206540	—	The L2 IPv6 GRE tunnel has an MTU of 1100 although the MTU is expected to be 1280. This issue is observed in a dual stack of native IPv6 deployment with managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206565	—	Bandwidth contract is not applied whe **web-cc-category** is configured on a native IPv6 setup.	AOS-W8.7.0.0
AOS-206577	—	When the **no MTU** command is issued, it returns a validation error. This issue is observed when a Layer-2 IPv6 GRE tunnel is formed between managed devices.	AOS-W8.7.0.0
AOS-206587	—	The output of the **show crypto ipsec sa** command on a managed device displays **IP Compression Enabled**. This issue is observed in dual stack of native IPv6 deployment on OAW-41xx Series switches running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206653	—	The **SAPD** process crashes on a managed device and IPv6 APs are stuck in **D** flag. This issue is observed in CPsec-enabled VPNCs.	AOS-W 8.7.0.0
AOS-206695	—	Datapath crash is observed on virtual Mobility Controller Virtual Appliance connected to a Mobility Master over IPv6. The log file lists the reason for the event as **Segmentation fault @ get_drbg_random ()**.	AOS-W8.7.0.0

Table 8: *Known Issues in AOS-W 8.7.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206873	—	The secondary 802.11a radio profile is not used for the second 5 GHz radio. This issue occurs when split 5 GHz or dual 5 GHz is set to automatic opmode. This issue is observed in managed devices running AOS-W 8.7.0.0.	AOS-W8.7.0.0
AOS-206888	—	A few APs take up to 30 minutes to be operational and join the managed device, when they are provisioned for the first time in a native IPv6 deployment. This issue is observed in OAW-AP515 and OAW-AP555 access points running AOS-W 8.7.0.0 in a cluster setup. **Workaround**: Set the **IP_preference** value to IPv6 when the APs boot up, so that the APs can come up in 2 to 3 minutes when they are provisioned the next time.	AOS-W 8.7.0.0
AOS-207599	—	The local WebUI for some APs does not work in the following scenarios and displays the **ERR_SSL_SERVER_CERT_BAD_FORMAT** error message: ■ The AP is new out-of-the-box and is in its factory default state with the Aruba Instant 8.7.0.0 manufacturing build. ■ The web browser used to access the local WebUI is Google Chrome, Microsoft Edge 79 and later versions, or Apple Safari. This issue is observed in AP-505H, 570 Series, AP-577, and AP-518 access points shipped with the Aruba Instant 8.7.0.0 software image. **Workaround**: Use either Internet Explorer, Microsoft Edge Legacy, or Mozilla Firefox web browsers to access the local WebUI. **NOTE:** This issue impacts all other AP platforms if they are rebooted in the factory default state after upgrading to Aruba Instant 8.7.0.0.	AOS-W 8.7.0.0

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

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

Topics in this chapter include:

Important Points to Remember

To upgrade your managed device or Mobility Master:

- 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 Master Licensing Guide*.
- Multiversion is supported only if the Mobility Master is running two code versions higher than the code versions running on the managed devices. For example multiversion is supported if a Mobility Master is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.3.0.0 and will not be supported if the managed devices are running AOS-W 8.2.0.0 or AOS-W 8.4.0.0.

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 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 69 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 69 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 69 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 Master, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups.

In the CLI

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

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 Master 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.

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

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.

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

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

The upgrade does not take effect until reboot. If you chose to reboot after upgrade, the Mobility Master 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 Master.
3. Execute the **ping** command to verify the network connection between the Mobility Master 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 Master.
   ```
   (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 Master 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 69 for information on creating a backup.

In the CLI

The following steps describe how to verify that the Mobility Master 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 69 for information on creating a backup.

Downgrading AOS-W

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

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 69.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master 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 Master 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 Master 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 Master 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 Master or managed device reboots after the countdown period.
4. When the boot process is complete, verify that the Mobility Master 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 Master 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 Master or managed device to boot with your pre-upgrade configuration file.
   ```
   (host) # boot config-file <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your pre-upgrade AOS-W version is stored.
   ```
   (host) #show image version
   ```

CAUTION

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

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Master 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.