AOS-W 8.8.0.0

Alcatel·Lucent
Enterprise

Release Notes

Copyright Information

Open Source Code

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 02	Added the **Enhancements to Air Slice** feature to the **New Features and Enhancements in AOS-W 8.8.0.0** section.
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

NOTE

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

Terminology Change

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

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

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal.al-enterprise.com
Email	ebg_global_supportcenter@al-enterprise.com

Contact Center Online	
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

Chapter 2
New Features and Enhancements

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

Support for Session ACL on IPsec Map

AOS-W supports session ACL on IPSec map. This allows a user to control the traffic flowing inside the IPSEC tunnel by defining permit or deny ACE rules as part of the session ACL.

Support for First Packet DPI Classification

AOS-W supports first packet DPI classification. By performing first packet DPI classification, traffic can be routed without interrupting any sessions and application-based policy based routing can be performed.

Cluster Updates

Live Upgrade

- Cluster live upgrade is now supported with IPv6 setup.
- Cluster live upgrade is enhanced to handle failures more gracefully and take less time to upgrade a cluster. For example, the time taken for AP image preload retries is reduced and even if one switch fails to upgrade in a cluster, the other switches are upgraded on a best effort basis instead of aborting the upgrade.

Deny Inter-User Bridging

This feature prevents the forwarding of Layer-2 traffic between wired or wireless users even when the users are on different switches in a cluster.

Dashboard Monitoring

Access Devices Details

The **Infrastructure** dashboard in the WebUI displays the following additional information for an AP that is down:

- Timestamp - Displays the date and time from when the AP is down.
- Reason - Displays the reason due to which the AP is down.

An **Outer IP** addresses column is added to the Access Points table. . When an AP’s role is provisioned from Campus AP to Remote AP, the AP has two IP addresses, Inner IP and Outer IP addresses. This column lists the OAW-RAP Outer IP address of an AP.

Detected Radios Details

The **Security** dashboard in the WebUI displays a new field **Match Source** under **Detected Radios** table, which provides information about the various types of sources used for manual reclassification of monitored APs. Following are the list of various source types that are stored in the WMS database:

- Admin
- OmniVista 3600 Air Manager
- WebUI
- Rest API
- Unknown

Disable Ethernet Link and PoE PSE of Wired Downlink Ports

AOS-W now allows to disable the Ethernet link and/or PoE PSE of the wired downlink ports during AP failover. AOS-W also configures the wired port down time after the AP fails over to backup cluster or falls back to the primary cluster.

Dynamic Packet Event Capture

AOS-W now supports Dynamic Packet Capture. This feature automates packet captures on the AP, based on anomalous events detected by the APs.

Enhancements to 530 Series and 550 Series Access Points

The 530 Series and 550 Series access points are now optimized for better power management based on the following scenarios:

- For PoE 802.3at on E0 and PoE 802.3af on E1, the AP power changes to failover mode and gives priority to E0 port so that the overall power is IEEE 802.3at.
- For PoE 802.3bt on E0 and PoE 802.3af on E1, the AP power changes to failover mode and gives priority to E0 port so that the overall power is IEEE 802.3bt.

Enhancements to Air Slice

Air Slice is now supported on 500 Series, 510 Series, 530 Series, 570 Series and OAW-AP555 access points.

Enhancements to Dual 5 GHz Mode Option on OAW-AP340 Series APs

AOS-W now allows to control the two radios separately in dual 5 GHz mode of OAW-AP340 Series access points. Hence, you can use different 802.11a radio profiles–dot11a-radio-profile for radio 0 (lower 5 GHz band), and dot11a-secondary-radio-profile for radio 1 (upper 5 GHz band) in dual 5 GHz mode.

Fast Roaming with Mesh APs

AOS-W supports fast roaming for APs deployed in a wireless mesh network in fast moving environments, such as buses or the subway. To support fast roaming, mobility mesh points perform a scan of other mesh points in the backgound, and then choose the best neighbor to connect from all the neighbors.

GRE Tunnel Traffic Load Distribution

The traffic load passing through a GRE tunnel can now be distributed across multiple CPUs instead of one to load balance the traffic.

Reserving IP Addresses

AOS-W now allows to manually reserve IP addresses from a DHCP pool for specific devices or MAC addresses in a large deployment. With manual IP reservation, managed devices can assign the same IP address to a client whenever the client requests for a network connection.

SNMP Trap on VLAN Probe Failure

A new SNMP trap, **wlsxClusterVlanProbeStatus**, is generated when VLAN probe fails. To view the list of SNMP traps, run the command, `show snmp trap-list`.

Support for 802.11mc Fine Timing Measurement responder mode

802.11mc Fine Timing Measurement (FTM) responder mode can be enabled on 500 Series, 500H Series, 510 Series, 530 Series, 550 Series, 560 Series, and 570 Series access points. FTM allows to calculate the distance between an STA and the nearby AP.

Support for DHCP Pool for VIA VPN users

AOS-W now supports getting a VIA client IP address from an external DHCP server instead of internal L2TP pool.

Support for DHCPv6 Relay-Option

The DHCPv6 Relay-Option (Option 18 and Option 37) feature allows the DHCPv6 relay agent to insert circuit and remote specific information in the form of a TLV (type-length-value) into the client message, which is forwarded to the DHCPv6 server.

Support for Per-AP Override

The per-AP override feature allows to configure specific configuration at per-AP level to override AP group level settings in the WebUI.

Support for SNMP Trap Group

AOS-W supports SNMP trap groups that allow to select specific traps to be configured within the group. Hence, all defining SNMP trap groups can send different traps to various trap receivers.

Support for Web-Server Configuration and Custom Certificate in APs

To provide enhanced security, the following configurations available on switches are applied to APs automatically when a virtual AP is created with captive portal authentication in bridge forwarding mode:

- Web server profile configuration
- Custom certificate

Support for New Modem

OAW-40xx Series and OAW-41xx Series switches now support GTC Netstick GLU-194ST USB Modem.

Upgrading using Mobility Master File Server

The flash storage on the Mobility Master is used as a file server for live upgrade and this locally stored image can be downloaded by the managed devices using HTTP protocol. You can upload firmware images from the WebUI of the Mobility Master by downloading it from the Aruba website.

NSS CPU Usage

The output of the **show ap debug system-status** command displays the NSS CPU usage. The NSS CPU usage will be displayed only for OAW-AP534, OAW-AP535, and OAW-AP555 access points.

Enhancements to Mesh Scanning Process

AOS-W now allows users to configure how often the topology mesh scanning should be performed to find a better mesh link. Issue the following commands to optimize the scan interval time period:

```
(host) [mynode] (config) #ap mesh-radio-profile <profile-name>
(host) [mynode] (Mesh Radio profile "default") #optimize-scan-interval <time period in hours>
```

Support for Uplink MU-MIMO Transmission

AOS-W now supports the uplink MU-MIMO transmission of 802.11ax protocol for OAW-AP535 and OAW-AP555 access points. The uplink MU-MIMO transmission helps in achieving throughput gains when applications need to upload a large amount of data. It also enables the multiple spatially separated clients to access the channel at the same time and it is also useful in scenarios where stations have limited number of antennas. The uplink MU MIMO transmission is supported only in 5G band. Navigate to **Configuration > System > Profiles > Wireless LAN> High Efficiency SSID > Advanced** and enable the **HE UL MU-MIMO** check-box to enable uplink MU-MIMO in HE capability. The supported ranges are 800ns and 1600ns.

Execute the following command in config mode to enable uplink MU-MIMO transmission:

```
(host) (config)wlan he-ssid-profile <profile-name> he-ul-mu-mimo
```

Troubleshooting Ethernet Related Issues

The output of the **show ap debug system-status** and **show ap tech-support** commands now display details related to ethernet ports. This helps in troubleshooting issues related to ethernet ports.

QOSMOS Image Upgrade

The QOSMOS proto bundle has been upgraded to 1.500-20 version.

WebUI Support for Users with AP-Provisioning Role

AOS-W now extends WebUI support for users with **ap-provisioing** role. When a user with an **ap-provisioning** role logs in, the **Dashboard** page provides an enhanced visibility only to the **Managed Network** node hierarchy of the network. The **Dashboard** page contains the following sub-categories:

- Overview
- Infrastructure
- Traffic Analysis
- Security
- Services

Configuration > Access Points and **Configuration > Tasks** are the only configuration pages visible for users with the **ap-provisioning** role.

WebUI Support to Display Redundant Mobility Masters

Starting from AOS-W 8.8.0.0, the WebUI displays the list of all Mobility Masters including Layer 2 and Layer 3 Redundancy Mobility Masters in the **Mobility Master** node hierarchy. Also, the text **Active** is displayed next to the name of the Mobility Master indicating that the particular Mobility Master is active. This text is displayed only when redundancy is configured.

Wi-Fi Uplink Support in Tri-Radio and Dual 5 GHz Mode

AOS-W now allows Wi-Fi Uplink feature on OAW-AP345 access points in Dual 5 GHz mode and on OAW-AP555 access points in tri-radio mode.

WMS Reclassification

For each classification type that is sent to an AP, the AP now sends a **PROBE_RAP_ACK** message to inform WMS that it has received the classification type. If there is no acknowledgment from the probe, WMS will resend the classification type to the AP. The number of retries allowed is 5 times.

Enhancements to the HE Pooling

Starting from AOS-W 8.8.0.0, AirMatch allows efficient use of available channels by dedicating specific number of channels to HE and non-HE radios. Prior to ArubaOS 8.8.0.0, AirMatch assigned the entire band of channels to HE radios. This enhancement allows efficient allocation of channels to HE and non-HE radios. A new flag, **A** has been introduced in following commands indicate radios assigned by AirMatch:

- show airmatch debug reporting-radio

- show airmatch debug optimization
- show airmatch debug solver feasibility optimization

RTLS Payload

AOS-W 8.8.0.0 increments the output parameter, **TAG** of the **show amon-sender stats-counters-all** command to indicate the RTLS frames received from the AMON receiver.

Discovering Disconnected Antennas

The **show ap antenna status** command has been introduced to display the operational antenna status of APs. This command helps in identifying broken or disconnected antennas and thus, helps in faster troubleshooting.

Enhancements to Fast BSS Transmission

Fast BSS transition is now operational with WPA3-Enterprise CNSA mode with GCM-256 encryption.

IoT Enhancements

IoT Authentication Type

AOS-W 8.8.0.0 introduces a new IoT authentication type, **Client Credentials**. The new authentication type can be configured in the IoT transport profile in the WebUI or CLI.

IoT Transport Type

AOS-W introduces a new transport type, **Azure-IoTHub** to send IoT data to the Azure IoT Hub. The Azure-IoTHub transport type allows secure, bi-directional communication between devices and the Azure cloud through a managed device that acts as a gateway. BLE devices are allowed to send data to the Azure cloud and serial devices are allowed to send and receive data to and from the Azure cloud. The new transport type can be configured in the IoT transport profile in the WebUI or CLI.

IoT Dashboard

The **IoT** dashboard in the WebUI displays the IoT data transport and information of the IoT devices in the network. The graphs in the IoT dashboard show information about the IoT infrastructure found under the selected node in the network hierarchy.

IoT Support for BLE Data forwarding for all Device Classes

AOS-W now allows forwarding of BLE data for all device classes. The BLE data forwarding can be configured in the IoT transport profile in the WebUI or CLI.

IoT Support for BLE Vendors

AOS-W now supports the following BLE vendors:

- Blyott
- DirAct
- Google
- GWAHygiene
- Minew
- Polestar

IoT Support for Per Frame Filtering

AOS-W now supports applying transport profile filters to each frame rather than on the device. This allows bleDataForwarding to treat deviceClass filter as packet filter. The per frame filtering can be configured in the IoT transport profile in the WebUI or CLI.

IoT Support for Piera Sensor

AOS-W now supports USB-based dongles from Piera.

IoT Support for SES Imagotag

AOS-W now allows an AP to authenticate with SES-Imagotag ESL server and verify the TLS FQDN. AOS-W also supports channel 127 for SES Imagotag ESL.

IoT Support for SoluM ESL Gateway

AOS-W now supports Solu M NEWTON USBG2 GW Zigbee-based USB gateway.

IoT Support for Zigbee Sniffer

AOS-W now supports a Zigbee sniffer command. This command helps in debugging Zigbee features running on an AP.

Support for Datazone Redundancy

MultiZone's datazone now supports redundancy to avoid long time service outage and the user can configure a backup switch or cluster for a datazone configuration.

Support for Microsoft Teams

AOS-W now supports Microsoft Teams users using voice or video calls, application-sharing, and file-transfer in a wireless environment. AOS-W detects Teams calls initiated from the Teams client and over the web browser. AOS-W classifies the Teams flows as Teams application, identifies the media traffic as voice, video, desktop-sharing, and indicates prioritization with the applicable QoS tag (WMM/DSCP). AOS-W provides visibility to Teams calls sessions with UCC score on uplink and downlink voice traffic and provides end-to-end call quality by using the graph API.

WiFi Co-existence Support for OAW-AP534, OAW-AP535, and OAW-AP555 APs

AOS-W 8.8.0.0 introduces Wi-Fi and BLE co-existence support for OAW-AP534, OAW-AP535, and OAW-AP555 access points. This prevent simultaneous transmissions on the radio of an AP.

Zero-Wait Dynamic Frequency Selection

Dynamic Frequency Selection (DFS), a mandate for radio systems operating in the 5 GHz band to identify and avoid interference with Radar systems now supports the zero-wait feature. When an 802.11 radio detects radar, it vacates its channel and switches to another channel. This might result in a one minute outage. Starting from AOS-W 8.8.0.0, the zero-wait DFS feature provides seamless change of channels and avoids the one minute outage. Hence, stations do not lose its connectivity when an AP moves to a DFS channel. This feature is enabled by default. Issue the following command to disable this feature:

```
(host) [mynode]  #rf dot11a-radio-profile <name>
(host) [mynode] (802.11a radio profile "name") #no zero-wait-dfs
```

New Knob to Specify 802.1x Auth Timeout

AOS-W now allows configuration of the 802.1X authentication timeout option as suitable for customer environments.
The new options are **Configuration > Access Points > Timeout bypass** and **Configuration > Access Points > Timeout retries**.

Also, see the new CLI options at **ap provisioning-profile | apdot1x-timeout-bypass** and **ap provisioning-profile | apdot1x-timeout-retries**.

Ability to Specify NTP Server Using FQDN

AOS-W now allows users to add NTP servers using a hostname/FQDN instead of an IP address.

Role-based Robust Age-out Mechanism for Wired Clients

AOS-W introduces a role-based robust age-out mechanism for wired passive clients where a wired client, such as a printer, will not be deleted from the system without its network un-reachability being verified by ICMP first.

Option to Select Keytype in CSR Attribute

The RSA-2048 with SHA256 was selected by default in the csr attribute. The EST feature is now enhanced to allow users to specify the keytype in a csr attribute. The default server configuration is accepted first during the enrollment/re-enrollment process. If the server does not provide the csr attribute, then the user-configured csr attribute is accepted.

Captive Portal DUR Restriction

With this enhancement, users can push Captive Portal profiles along with the user role from CPPM.

Updates to the UCC Table

Custom SIP entry is replaced with the actual application name or protocol in the Services/Wireless Calls (UCC) table column ALG.

ACL Hits-Table Enhancements

This feature implements a change in behavior for ACL hits-indices allocation for expanded Application Control Engines (ACEs).

Changes to Firmware Upgrade

Starting from this release, AOS-W allows a firmware upgrade without changing the default boot option.

Firewall ACL Description Field

A description field is added in the UI to enable users to add a short note stating why the ACL was created.

Enhancements to Auth Requests From IKE

AOS-W now addresses VIA and native VPN scalability issues by increasing the max queue size for auth requests from IKE across all switchplatforms.

VoIP Aware Scan Timer

A new parameter, **voip-aware-scan-timer**, is added to the **rf arm-profile** command to enable users to set the VoIP Aware scan timer range between 50 ms-1000 ms.

RFE Master List

AOS-W introduces a new CLI sub-command, **show master-l3redundancy | switches**, to see the L3 redundant peer switch details along with active and standby switch details.

Enhancements to the disable-crc-workaround Command

Starting from AOS-W 8.8.0.0, users can issue the **disable-crc-workaround** command when port flaps of the uplink switch are not detected by the Mobility Master. This command dumps all the PHY register data like alarms, warnings, signal strength and hence, will be helpful for debugging.

It is to be noted that when this configuration is enabled, the CRC workaround will be initiated only when the uplink switch shuts down and come up and not when the the device is stable.

```
(host) [mynode] (config) #disable-crc-workaround
(host) [mynode] (config) #write memory
```

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 8.8.0.0*

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 8.8.0.0*

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 8.8.0.0*

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-AP303P
OAW-AP303H Series	OAW-AP303H, AP-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345

Table 5: *Supported AP Platforms in AOS-W 8.8.0.0*

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, AP-375ATEX
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 8.8.0.0 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_79479

Chapter 5
Resolved Issues

This chapter describes the resolved issues in this release.

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-134310 AOS-141737 AOS-209401	162993 172569	The database synchronization between master and standby Mobility Master failed. The fix ensures that database synchronization works as expected. This issue occurred when TLS v1.2 was enabled in the SSL protocol of a web server profile. This issue was not limited to any specific switch model or AOS-W release version.	AOS-W 8.3.0.0
AOS-138391 AOS-209275	168088	APs established tunnels with an incorrect MTU size. This issue occurred when jumbo frames were enabled. The fix ensures that the APs do not establish tunnels with an incorrect MTU size. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-138446 AOS-210178	168158	A few APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Rebooting the AP. NSS FW crashed**. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.9 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.9
AOS-139078 AOS-206173	168983	Some access points did not connect or experienced low throughput. The fix ensures that AP 305 access points work as expected with high throughput. This issue was observed in AP 305 access points running AOS-W 6.5.1.10 or earlier versions.	AOS-W 6.5.1.0
AOS-149413 AOS-196453	183040	The **Dashboard > Overview > Remote Clients** page of the WebUI did not display any value for **OS** and **connected to** fields. The fix ensures that WebUI displays the **OS** and **connected to** fields. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-154005 AOS-210273 AOS-217372		Some managed devices log the error message, **INFO> |dot1x-proc:1| Sending request for Switch IP6** although there are no IPv6 configurations in the network. This issue was observed in managed devices running AOS-W8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-154778 AOS-197721	190234	Some Virtual OmniAccess Mobility Controllers running AOS-W 8.3.0.0 or later versions crashed unexpectedly. This issue occurred in AirMatch when invalid **utf8** character was used in **ap-name string**. The fix ensures that the Virtual OmniAccess Mobility Controllers work as expected.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-155667 AOS-182789 AOS-185224 AOS-186048 AOS-186473 AOS-188296 AOS-190743 AOS-191883 AOS-191900 AOS-212581	191528	A few Remote APs running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for this event as, **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures that the Remote APs work as expected.	AOS-W 8.3.0.0
AOS-158621 AOS-213582	195659	The **profmgr** process crashed and the Mobility Master rebooted unexpectedly. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-184269 AOS-186423 AOS-207317	–	A few APs were unable to join a cluster and rebooted with **unable to contact switch: HELLO-TIMEOUT error message**. This issue occurred when the cluster leader receives a deactivate event from DDS of a different managed device that was a previous leader. This issue was observed Managed devices running AOS-W 8.3.0.6.	AOS-W 8.3.0.6
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, AOS-205672, AOS-207947 and AOS-212668	AOS-W 8.2.2.0
AOS-184519 AOS-207777	–	Users were unable to delete the VLAN even though the VLAN was not mapped on any node or group on the managed device running AOS-W 8.3.0.4. The fix ensures that the managed device works as expected.	AOS-W 8.3.0.4
AOS-185127 AOS-187183 AOS-211154	–	The **CFGM** process in a Mobility Master stopped responding and went into **PROCESS_NOT_RESPONDING_CRITICAL** state. As a result, the output of the **show switches** command displayed the **Module Configuration Manager is busy. Please try later** error message. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

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 ArubaOS 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-212645	AOS-W 8.4.0.2
AOS-186738 AOS-206968 AOS-207432 AOS-210156	–	The certificate reference count incremented by 1. The fix ensures that the certificate reference count is accurate and does not increment. This issue occurred when the managed device was reloaded after uploading the captive portal server certificate. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.8
AOS-187395 AOS-188564	–	The AAA test to the external server failed when executed from the **Diagnostics > Tools > AAA Server Test** page of the WebUI. This issue occurred when the user entered the ", %, and # special characters in the **Password** field and clicked the **Test** option. As a result, the WebUI displayed the **Authentication** field as **failed** and **Processing time (ms)** field as **N/A**. The fix ensures that the AAA test to the external server is successful. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-187672 AOS-213397	–	Memory leak was observed in the arci-cli-helper process. The fix ensures that the Mobility Masters and managed devices work as expected. This issue was observed in Mobility Masters and managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-188255 AOS-190476 AOS-190946 AOS-192725 AOS-193586 AOS-194784 AOS-196004 AOS-200375 AOS-210787	–	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.	AOS-W 8.3.0.8
AOS-188972 AOS-194746 AOS-208631 AOS-209396 AOS-213627	–	The **Dashboard > Security > Blacklisted Clients** page of the Mobility Master WebUI displayed the blacklisted clients though the clients were removed from the managed device. The fix ensures that the removed blacklisted clients are not displayed in the WebUI. This issue was observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions in a cluster setup.	AOS-W 8.7.1.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-189772 AOS-196328 AOS-198374 AOS-210163	–	The **dot1x** and **dot2x** processes crashed unexpectedly on a managed device. This fix ensures that themanaged 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 AOS-210684	–	The **dpagent** process crashed on a managed device running ArubaOS 8.5.0.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.0
AOS-189890 AOS-197999 AOS-199500 AOS-201061 AOS-203111 AOS-203779 AOS-204282 AOS-211069	–	Datapath crash was observed when upgrading Virtual Mobility Controllers. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 and later versions.	AOS-W 8.3.0.0
AOS-191031	–	A few 802.11ax clients experienced poor MU-MIMO performance. Enhancements to the wireless driver resolved this issue. This issue was 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-191081 AOS-211007	–	Some iPhones connected to Wi-Fi were unable to access the network. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.10
AOS-191446 AOS-201647 AOS-212947	–	A user was unable to change the password of PSK authenticated SSID profiles from lower node levels. This issue occurred when the AP group was mapped to an IoT profile. The fix ensures that the users can change the password. This issue was observed in managed devices running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191216 AOS-196523 AOS-199160 AOS-203960 AOS-207725 AOS-208396 AOS-208723	–	A managed device running AOS-W 8.5.0.4 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-193383 AOS-195770 AOS-196219 AOS-203470 AOS-207584 AOS-210908	–	A few 500 Series 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 **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-193560 AOS-198565 AOS-200262 AOS-208110 AOS-204794 AOS-209989 AOS-212249	–	The number of APs with **DOWN** status were incorrectly displayed in the **Dashboard > Overview** page of the WebUI. However, the CLI displayed the correct status of the APs. The fix ensures that WebUI displays the correct status of the 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-193701 AOS-209485	–	The **Rx Data Bytes** value in the **show ap debug radio-stats** command was lower than the actual value. The fix ensures that the correct number of data bytes are received. This issue was observer in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-194052 AOS-210810	–	A few clients were unable to obtain IP addresses. This issue occurred when High Efficiency was enabled on the WPA2-PSK SSID profile of the APs. The fix ensures that the clients are able to obtain the IP addresses. This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.2
AOS-194113 AOS-203184 AOS-213027 AOS-213861 AOS-217082	–	Users were unable to perform captive portal authentication when log in URL of the captive portal profile pointed to ClearPass Policy Manager. The fix ensures that 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

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-194228 AOS-207226	–	The **show ap monitor ap-list** command displayed incorrect channel bandwidth. The fix ensures that the command displays the correct channel bandwidth. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-194316 AOS-210475	–	A few OAW-AP205 access points running AOS-W 8.5.0.1 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception: PC is at _wl_del_monitor LR is at anul_assert_func**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.1
AOS-194520 AOS-209634	–	The VRRP preempt delay timer did not reset even after receiving heartbeats from the VRRP-Master, though VRRP preempt was enabled with preemption delay. The fix ensures that the VRRP preempt delay timer is reset upon receiving the heartbeat from the VRRP-master before the preempt delay timer expires. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-194919	–	The **HTTPD** process in a OmniAccess Mobility Controller Virtual Appliance crashed unexpectedly. The log file listed the reason for the event as **Reboot Cause: User reboot (Intent:cause 86:50)**. This issue occurred when the OmniAccess Mobility Controller Virtual Appliance was scanned for a security vulnerabilities. This issue was observed in OmniAccess Mobility Controller Virtual Appliances and stand-alone switches running AOS-W 8.2.0.0 or later versions. **Duplicates**: AOS-195565, AOS-205648, AOS-206010, AOS-208602, AOS-208661, AOS-209625, AOS-212628, AOS-213869, and AOS-216546.	AOS-W 8.2.0.0
AOS-194978 AOS-209883 AOS-216838	–	A few OAW-AP515 access points running AOS-W 8.4.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Critical process /aruba/bin/stm [pid 12217] DIED, process marked as RESTART**. The fix ensures that the APs work as expected. This issue occurred because the **STM** process crashed while connecting High Efficiency clients to the AP.	AOS-W 8.5.0.8
AOS-195101	–	The traffic between master redundancy Mobility Masters was dropped causing a few process to be in **PROCESS_NOT_RESPONDING** state. Hence, configurations were not synchronized between the peers. This issue was observed in the **ipsec-mark-mgmt-frames** parameter was enabled using the **firewall wireless -bridge-aging** command. This issue was resolved by disabling the **ipsec-mark-mgmt-frames** parameter using the **firewall wireless -bridge-aging** command. This issue was observed in Mobility Masters running AOS-W8.2.0.0 or later versions.	AOS-W8.2.0.0
AOS-195350	–	A few OAW-AP555 access points running AOS-W 8.6.0.0 or later versions crashed unexpectedly. The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-195424 AOS-214200	–	OAW-AP535 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 **Reboot caused by kernel panic: Fatal exception in interrupt.** The fix ensures that the AP works as expected.	AOS-W 8.6.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195655 AOS-210147	—	Some users connecting to OAW-AP515 access points running AOS-W 8.6.0.0 or later versions were unable to pass traffic intermittently. The fix ensures that clients are able to pass traffic.	AOS-W 8.6.0.0
AOS-196325 AOS-200875 AOS-213037	—	A Mobility Master rebooted unexpectedly. This issue occurred due to high memory consumption. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196399	—	Cluster DDS traffic caused IP reassembly failures in datapath. The fix ensures that the managed devices works as expected. This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-196704 AOS-203119 AOS-209446	—	APs operating as a mesh portal crashed and rebooted. The log file listed the reason for the event as: **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. The fix ensures that the AP works as expected. This issue was observed in APs running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
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:64690a3b303db3 PC:wlc_mutx_bw_policy_update+0x408/0x28b8 [wl_v6] Warm-reset**. This issue occurred when 4 or more MU capable clients were connected to the AP. The fix ensures that the APs work as expected. **Duplicates:** AOS-199587, AOS-199592, AOS-199431, AOS-201056, AOS-201803, AOS-201192, AOS-201589, AOS-203260, AOS-203650, AOS-206706, AOS-206894, and AOS-207985	AOS-W 8.6.0.0
AOS-196911 AOS-198963 AOS-211840 AOS-214329	—	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-196988 AOS-213453	—	The **UTILD** process crashed while adding or removing blacklisted clients. This issue occurred when audit was enabled. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-197134	—	User roles were incorrectly listed as downloaded user roles and the error message, **user role already exists** was displayed. The fix ensures that the correct user roles are listed and the error message is not displayed. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197210	—	WebUI took a long time to display data. The fix ensures that the WebUI displays data without any delay. This issue was observed in stand-alone switches running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197216 AOS-202623 AOS-202964 AOS-209603 AOS-209740	–	The Datapath process crashed on a managed device. The log file listed the reason for the event as **datapath exception**. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions. The fix ensures that Managed devices work as expected.	AOS-W 8.5.0.2
AOS-197494	–	The **Show datapath debug opcode** command displayed hexadecimal output. The fix ensures that the command displays decimal output. This issue was observed in managed devices running AOS-W 8.3.0.1 or later versions.	AOS-W 8.3.0.1
AOS-197548 AOS-209545	–	MAC authentication was not initialized when IPv6 was globally disabled. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.3.0.13.	AOS-W 8.3.0.13
AOS-197548 AOS-209545	–	MAC authentication was not initialized when IPv6 was globally disabled. The fix ensures that the MAC authentication works as expected. This issue was observed in managed devices running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-197552 AOS-206767	–	Some OAW-AP305 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 interrupted**. The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
AOS-197768 AOS-208134 AOS-208194	–	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 **ut_page+0x8/0x50 and LR is at skb_release_data+0x70/0xc8**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-198044 AOS-207046	–	The mesh topology information was not synchronized among all the managed devices in a cluster. As a result, the output of the **show ap mesh topology** command did not display full information of all mesh portals and mesh points under a specific mesh topology. The fix ensures that the mesh topology information is synchronized among all the managed devices in a cluster. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a cluster setup.	AOS-W 8.5.0.0
AOS-198363	–	Clients were either unable to connect to the APs or were getting disconnected when the **SAPD** process over utilizes CPU memory. The fix ensures that the clients connect to the APs as expected. This issue was observed in OAW-APAP-324 running AOS-W 8.4.0.0 or later versions. **Duplicates**: AOS-209306, AOS-209658, AOS-214321, AOS-215719, AOS-215729, AOS-216418, AOS-218389, and AOS-218459.	AOS-W 8.4.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198834 AOS-200088 AOS-200555 AOS-201312 AOS-202608 AOS-206935 AOS-211609	–	A few managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **Soft Watchdog reset (Intent:cause:register de:86:70:4)**. The fix ensures that the managed devices work as expected. This issue was observed in OAW-4750XM switches running AOS-W 8.3.0.10 or later versions.	AOS-W 8.5.0.8
AOS-199230 AOS-208835	–	The **cfgm** process crashed unexpectedly on a Mobility Controller Virtual Appliance running AOS-W 8.5.0.5 or later versions. The fix ensures that the Mobility Controller Virtual Appliance work as expected.	AOS-W 8.5.0.5
AOS-199384 AOS-208088	–	A few APs running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic : PC is at wlc_twt_scb_get_schedid+0x8/0x38.** Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.0
AOS-199545 AOS-212851	–	Some APs reported low noise floor after upgrading the cluster to AOS-W 8.7.1.0. The fix ensures that the APs work as expected.	AOS-W 8.7.1.0
AOS-199803 AOS-206120 AOS-213768 AOS-214906 AOS-217228	–	Both CLI and WebUI of the Mobility Master did not display the list of wired users connected to the network. The fix ensures that the Mobility Master displays the list of wired users connected to the network. This issue was observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-199991 AOS-202416 AOS-215419	–	A few controllers forwarded gratuitous ARP packets over standby L2 GRE tunnel and this caused network loop. This issue was resolved by adding ICMP keepalive message support for GRE tunnels. This issue was observed in stand-alone controllers running AOS-W8.5.0.0 or later versions	AOS-W 8.5.0.0
AOS-200349 AOS-201711 AOS-202341 AOS-207639 AOS-209036 AOS-209741 AOS-210176	–	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
AOS-200552 AOS-202047	–	Some managed devices running AOS-W 8.5.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:30:2)**. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.5

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200601 AOS-200812 AOS-207772	–	A few switches were unable to detect the Huawei E3372h-153 (HiLink Mode) 4G LTE USB Modem. The fix ensures that the switches are able to detect the modem and and connect the 4G LTE USB modem for cellular network connectivity. This issue was observed in OAW-40xx Series switches running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-200689 AOS-208662	–	APs 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.	AOS-W 8.6.0.0
AOS-200733 AOS-209999	–	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-200745 AOS-204174	–	Some APs running AOS-W 8.6.0.4 or later versions rebooted unexpectedly. The log file listed the reason for the event as **Reboot reason: External-WDT-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.4
AOS-200762	–	Disabling Prohibit IP spoofing in the firewall did not work as expected. The fix ensures that users are able to disable the Prohibit IP spoofing feature. This issue occurred because the ARP request frame got flooded as a broadcast instead of unicast. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-200766 AOS-201434 AOS-209172	–	A few session ACL were deleted after a reload of the managed device running AOS-W 8.3.0.0 or later versions. The fix ensures that the ACLs are not deleted.	AOS-W 8.3.0.0
AOS-200801	–	A few clients were unable to connect to APs, and incorrect ACL index values were displayed in the AP datapath. The fix ensures that the APs work as expected. This issue occurred when the clients were connected through bridge mode SSID, and the **SAPM** process sent duplicate access control entries. This issue was observed in APs connected to a stand-alone switch running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-200950 AOS-203934	–	User was unable to access previously backed up data when the new backup-logs application was installed. The fix ensures that the user is able to access the backed up data. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200976 AOS-202577 AOS-204027 AOS-204410 AOS-204811 AOS-205437 AOS-206673 AOS-209771	–	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-201003 AOS-212135	–	Some OAW-RAPs were unable to come up in a cluster. The fix ensures that the OAW-RAPs work as expected. This issue was observed in managed devices running AOS-W 8.0.2.0 or later versions.	AOS-W 8.0.2.0
AOS-201149 AOS-208332 AOS-211746	–	Some OAW-AP515 access points running AOS-W 8.6.0.2 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot reason: BadPtr:00000000 PC:ppr_create_prealloc+0x3c/0x90 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.2
AOS-201166 AOS-207939 AOS-209042	–	A switch crashed and rebooted unexpectedly after the **HTTPD** process was restarted. The log files listed the reason for the event as **Reboot cause: Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c)**. The fix ensures that the switch works as expected. This issue was observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-201233 AOS-214547	–	The **Dashboard > Overview > Clients** page in the **Managed Network** node hierarchy of the WebUI displayed an incorrect **Client Bandwidth**. The fix ensures that the WebUI displays the correct bandwidth. This issue was observed in Mobility Masters running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-201340 AOS-210406	–	Memory leak was observed in the **auth** process of stand-alone switches. The fix ensures that the stand-alone switches work as expected. This issue was observed in stand-alone switches running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-201376	–	The measured power, **Meas. Pow** column in the output of the **show ap debug ble-table** command was updated when the Tx power of an AP was changed. The fix ensures that the measured power, **Meas. Pow** column in the output of the **show ap debug ble-table** command is updated when the Tx power of an AP is changed. This issue was observed in APs running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-201379	–	Some managed devices running AOS-W 8.6.0.2 or later versions in a cluster setup experienced high CPU utilization. This issue occurred when managed devices failed to load balance clients after re-joining the network. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.2
AOS-201454	–	Uplink routing using next-hop list failed after uplink failover. This issue occurred when uplink VLAN 4093 received IP address from a NAT device. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201519	–	A few APs running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **PC is at 0x0; LR is at ieee80211_get_txstreams**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.0
AOS-201674 AOS-207166	–	The VLAN-ID/Named VLAN is invalid error message was displayed for a few user roles on the managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.2
AOS-201699 AOS-205472 AOS-208964 AOS-208995	–	A user was unable to send or receive traffic. This issue occurred when an ACL was unavailable for the user role. The fix ensures that the managed devices work 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-201757 AOS-202085 AOS-203489 AOS-204529 AOS-204861 AOS-206217 AOS-207968 AOS-211571 AOS-212105	–	The IP addresses of wired clients in **Dashboard > Overview > Clients** page were displayed as 0.0.0.0. The fix ensures that the correct IP address are displayed in the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-201763	–	Some users were unable to access CLI using SSH. The fix ensures that the users can access CLI using SSH. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-201812 AOS-201813	–	Disabled VLANs generated the **wlsxVlanLinkDown** and **wlsxVlanInterfaceEntryChanged** traps. The fix ensures that the traps are not generated. This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-202034 AOS-205799 AOS-207736 AOS-208473	–	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 work as expected.	AOS-W 8.6.0.0
AOS-202126 AOS-215134		The **profmgr** process restarted continuously on the Mobility Master and hence configurations were not forwarded to the managed devices. The fix ensures that the configurations are forwarded to the managed devices. This issue was observed in managed devices running AOS-W8.5.0.8 or later versions.	AOS-W 8.5.0.8

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202219 AOS-207452	–	The radio mode of mesh APs was incorrectly displayed as Mesh Portal in the **Dashboard > Overview> Radios** page in the WebUI. The fix ensures that the radio mode is displayed as Mesh Point in the WebUI. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.11
AOS-202243	–	The **Security > Authentication > Servers > Server Group** page of the WebUI displayed the error message, **Error in getting 'show aaa server-group XXXX' data:null**. The fix ensures that the Mobility Masters work 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
AOS-202274	–	The **TRAPD** process crashed unexpectedly in a managed device running AOS-W 8.3.0.0 or later version. The fix ensures that the managed device works as expected. This issue was observed in managed device running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.3.0.0
AOS-202349 AOS-211337	–	A few users were unable to map the captive portal authentication profile under guest-logon user role, and the **Failed to remove reference of role guest-logon captive-portal profile default** error message was displayed. The fix ensures that the users are able to map the captive portal authentication profile under guest-logon user role. 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-202497 AOS-212608	–	Some APs running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file displayed the reason for the event as, **Kernel panic: PC is at wlc_apps_psp_resp_complete+0x24**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.5
AOS-202519	–	The interface tunnel with IPv6 failed to accept Unique Local Address (ULA) as a valid address. The fix ensures that the interface tunnel with IPv6 accepts ULA as a valid address. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-202552	–	The **Dashboard >Traffic Analysis > AppRF** page of the WebUI displayed **UNKNOWN value for WLANs, Roles,** and **Devices**. The fix ensures that the WebUI page displays the correct output. This issue was observed in managed devicesrunning AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-202743 AOS-203498 AOS-203507 AOS-204322 AOS-207506 AOS-211066	–	The **Configuration** > **Interfaces** > **VLANs** tab did not display the IP addresses of Mobility Masters 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

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202803 AOS-210539	–	The **cluster was fractured during the upgrade** error message was displayed during the cluster live upgrade process. As a result, cluster live upgrade failed. The fix ensures that users are able to upgrade clusters. This issue was observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.7
AOS-203257	–	Users were unable to delete an existing management server that was already configured in the Mobility Master. The log file listed the reason for the event as **The Delete Error in deleting reference to Profile 'default-amp' [2]**. The fix ensures that the users are able to delete the management server. This issue was observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-203517 AOS-204709 AOS-213765	–	The Datapath module crashed in a few managed devices unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. This issue occurs when data packets undergo multiple GRE encapsulation. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-203536	–	A few clients took a long time to roam between APs. The fix ensures that clients do not take a long time to roam between APs. This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-203614 AOS-209261	–	The Mobility Master dashboard does not display the number of APs and clients present in the network. The fix ensures that the dashboard displays the number of APs and clients present in the network. This issue was observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-203652	–	A few APs running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for this event as **InternalError: Oops - undefined instruction**. Enhancements to the wireless driver resolved this issue. **Duplicates:** AOS-206320, AOS-208333, AOS-209043, AOS-209044, AOS-209813, AOS-210218, AOS-210302, AOS-210478, AOS-210479, AOS-210592, AOS-210654, AOS-210659, AOS-211611, AOS-211775, AOS-211776, AOS-211779, AOS-211780	AOS-W 8.6.0.4
AOS-203702 AOS-204024 AOS-204423 AOS-204544 AOS-205440 AOS-206804 AOS-207087 AOS-207197 AOS-207632	–	7000 Series, 7205, 7210, 7220, 7240, 7240XM 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

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203702	–	A few switches 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 switches work as expected. This issue was observed in OAW-40xx Series, OAW-4450, OAW-4550, OAW-4650, OAW-4750, and OAW-4750XM controllers running AOS-W 8.5.0.8 or later versions. **Duplicates**: AOS-204024, AOS-204423, AOS-204544, AOS-205440, AOS-207087, AOS-207179, AOS-207197, AOS-207306, AOS-207477, AOS-207632, AOS-208014, AOS-208481, AOS-208930, AOS-209395, AOS-209757, AOS-211986, and AOS-217904	AOS-W 8.5.0.8
AOS-203743	–	DPI classification did not work when the HTTP-based rule was applied to custom-app. The fix ensures that the DPI classification works as expected. This issue was observed managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-203773 AOS-215658	–	A few users were unable to access network destinations after configuring the alias for the specific network. The fix ensures that the users are able to access the network destinations. This issue occurred because the destination IP address was not configured for the network. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-203910 AOS-204905 AOS-206578 AOS-217020	–	The stand-alone switches running AOS-W 8.6.0.3 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.3
AOS-203910 AOS-204905 AOS-209155 AOS-209692 AOS-217020	–	The stand-alone controllers running AOS-W 8.6.0.3 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. The fix ensures that stand-alone controllers work as expected.	AOS-W 8.6.0.3
AOS-203926 AOS-217462 AOS-217578	–	Voice traffic using **noe** protocol did not get tunneled through the split-tunnel forwarding mode. This issue occurred when **Openflow** was enabled. The fix ensures that the traffic gets tunneled as expected. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-203958 AOS-205068	–	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 8.6.0.2

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204027 AOS-204410 AOS-204811 AOS-205437 AOS-206739 AOS-207085 AOS-207590	–	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-204142 AOS-207644	–	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 in the **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-204187	–	The command **vpn-peer peer-mac** did not support Suite-B cryptography for custom certificates. The fix ensures that the command supports Suite-B cryptography custom certificates. This issue was observed in Mobility Masters running AOS-W 8.2.2.8 or later versions.	AOS-W 8.2.2.8
AOS-204195	–	A few clients were not able to find ESSID in air. This issue occurred when **Beacon Failed** rate was too high. This issue is resolved by increasing the range of the **energy-detect-threshold** parameter of the **rf dot11a-radio-profile** command. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-204326 AOS-205256	–	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.	AOS-W 8.6.0.4
AOS-204334 AOS-205224 AOS-212129	–	The **Upgrademgr** process got stuck and stopped responding after a reboot of the Mobility Master. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions.	AOS-W 8.7.0.0
AOS-204364	–	High channel utilization was observed in some APs, and the issue was continuously displayed until the APs were rebooted. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-204378 AOS-209939	–	A few clients were unable to roam properly when 802.11r feature was enabled. The fix ensures that clients can roam between APs when 802.11r feature is enabled. This issue was observed in APs running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204385 AOS-208159	–	Incorrect position of access policies were observed in the **Configuration > Roles & Policies > Policies** page of the WebUI as well as from the CLI. The fix ensures that the access policies are positioned correctly. 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-204545 AOS-208184 AOS-208757 AOS-209190	–	A switch crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:f0:2)**. The fix ensures that the switch work as expected. This issue was observed in OAW-4750XM switches running AOS-W 8.5.0.0 or later versions	AOS-W 8.5.0.0
AOS-204764 AOS-207049	–	AP configurations were reset and APs moved to the default AP group after a reboot. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-204780	–	Mobility Masters running AOS-W 8.3.0.0 or later versions displayed the **Valid Client Misassociation** log even when the valid clients connected to a valid SSID. The fix ensures that the Mobility Master work as expected.	AOS-W 8.3.0.0
AOS-204797	–	A client was unable to connect to OAW-AP303H Series access points running AOS-W 8.6.0.0 or later versions in a Mobility Master-Managed Device topology. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.0
AOS-204842 AOS-208889	–	Mobility Masters running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Soft Watchdog reset (Intent:cause:register de:86:70:4)**. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.3.0.0
AOS-204917	–	The **dpagent** process on managed devices running AOS-W 8.5.0.0 or later versions crashed unexpectedly. The log file listed the reason for this event as **Memory usage limit exceeded for process: dpagent current pages**. This issue occurred due to high memory utilization. The fix ensures that the managed devices work as expected. **Duplicates**: AOS-205979, AOS-207203, AOS-207924, AOS-207992, AOS-208343, AOS-208934, AOS-208920, AOS-209865, AOS-211415, AOS-204917, AOS-211428, AOS-212034, and AOS-213957	AOS-W 8.5.0.0
AOS-205025 AOS-209326	–	The switch did not retrieve cluster inner-IP from the whitelist database as the request is initiated from an OAW-IAP. This issue occurred when the switch used external authentication for OAW-RAP whitelisting. This issue was resolved by provisioning the OAW-IAP as a OAW-RAP. This issue was observed in switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-205171	–	Mobility Masters and managed devices running AOS-W 8.5.0.7 or later versions displayed a log message, **Received MAP_ADD from IKE for default-local-master-ipsecmap**. This issue occurred when tunnels were established. The fix ensures that the Mobility Masters and managed devices work as expected.	AOS-W 8.5.0.7

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205319 AOS-206993 AOS-211103 AOS-212027 AOS-216577 AOS-218524	–	A few APs running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: PC is at put_page+0xc/0x54**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.5
AOS-205326	–	An 802.11ax client failed to complete a download throughput test. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-205344	–	A few clients experienced slow connection speed when they connected to APs using mobile devices. This issue was observed in regions that operate under legacy regulatory rules. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-205371	–	OmniVista 3600 Air Manager displayed Alcatel-Lucent AP-505H as Alcatel-Lucent AP-50. The fix ensures that OmniVista 3600 Air Manager displays the device list correctly. This issue was observed in Virtual OmniAccess Mobility Controllers running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-205621	–	Following issues were observed in a bridge mode captive portal: • The certificate private key was not encrypted on AP flash. • Users were unable to replace an expired certificate. The fix ensures that the certificate private key is encrypted on AP flash and users are able to replace an expired certificate. This issue was observed in APs running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-205634 AOS-212820	–	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 devicesrunning AOS-W 8.6.0.4 or later versions	AOS-W 8.6.0.4
AOS-205636	–	A few 802.1X clients experienced random timeouts. This issue was observed in OAW-AP203RP access points running AOS-W 8.0.0.0 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.0.0.0
AOS-205666	–	Performance degradation was observed in OAW-AP535 access points running AOS-W 8.7.0.0 when OFDMA was enabled in the **wlan he-ssid-profile** command.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205667	–	A wrong role was assigned to bridged mode wired port in initial role. This issue is resolved by changing the role name to be case insensitive. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-205684	–	The post authentication role for a bridge-Captive Portal client was carried forward from one VAP to another. This issue is resolved by resetting the role when the authenticated bridge-Captive Portal client switches ESSID. This issue occurred when an authenticated bridge-Captive Portal client switched to a different ESSID and the client kept the authenticated role from the bridge-Captive Portal. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-205702	–	A few 7280 switches running AOS-W 8.3.0.0 or later versions disconnected TCP session and hence, internal captive portal stopped working. The fix ensures that the switches work as expected. This issue occurred due to **nginx** process crash.	AOS-W 8.3.0.0
AOS-205728 AOS-210336 AOS-213490	–	The **show license-usage client** command did not display the entire list of managed devices. The fix ensures that the command displays the entire list of managed devices. This issue was observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-205783	–	Although the session timeout of the bridge captive portal has expired, some clients continued to stay in the post authentication role. The fix ensures that the client does not stay in the post authentication role after session timeout expires. The issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-205869	–	Users were unable to delete ACLs and the error message, **Invalid data: FW CP ACL not found** was displayed. The fix ensures that users are able to delete ACLs. This issue was observed in managed devices running AOS-W 8.3.0.12 or later versions.	AOS-W 8.3.0.12
AOS-205935 AOS-211851	–	Management users created on Mobility Master were not synchronized on standby Mobility Master. The fix ensures that the entries are synchronized between the Mobility Master and the standby Mobility Master. This issue was observed in Mobility Masterrunning AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-205189 AOS-205996 AOS-207870 AOS-212331 AOS-212416 AOS-214376 AOS-214747 AOS-216952	–	A user experienced network latency. This issue occurred due to high CPU utilization in a managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W8.5.0.5 or later versions.	AOS-W 8.5.0.5

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206041 AOS-212553	–	The default gateway was not listed in IP route output when Managed Device tries to failover to secondary Managed Device. This issue was observed in Mobility Master running AOS-W 8.5.0.2 and later versions. Resetting the uplink configuration fixes the issue.	AOS-W 8.5.0.2
AOS-206045	–	A managed device running AOS-W 8.5.0.4 or later versions initiated multiple radius access requests simultaneously. The fix ensures that only one radius access request is initiated.	AOS-W8.5.0.4
AOS-206047	–	The AirGroup cache entries were deleted. The fix ensures that the AirGroup cache entries are not deleted. This issue occurred when the maximum threshold limit was reached. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W8.6.0.4
AOS-206057	–	Poor performance was observed in OAW-AP535 access points running AOS-W 8.7.0.0 when the MU-MIMO was enabled. Enhancements to the wireless driver resolved this issue.	AOS-W8.7.0.0
AOS-206071	–	The **Dashboard > Security > Bandwidth** page did not display information about the HT-type of the APs. The fix ensures that the WebUI displays the HT-type of the APs. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W8.6.0.4
AOS-206115	–	High efficiency and very high throughput values disabled using **wlan ht-ssid** profile command were displayed in the output of **show ap bss-table** command. The fix ensures that the AP BSS table does not display the disabled values. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.9
AOS-206123	–	Packet loss was observed on APs running AOS-W 8.2.2.0 or later versions. The fix ensures that the APs work as expected. This issue occurred when APs were configured with the default MTU value of 1300.	AOS-W 8.5.0.5
AOS-206177	–	Users failed to timeout after an AP reboot and the user entries were retained in the user table although the clients were disconnected few days back. The fix ensures that the user entries are removed from the user table after the clients get disconnected. This issue occurred when the wireless clients were connected using bridge mode to managed devices running AOS-W 8.7.0.0 version.	AOS-W 8.7.0.0
AOS-206178	–	System logs did not display the reason why an AP had shut down. This issue was observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206221	–	APs did not come up during a data center failover. 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.	AOS-W 8.5.0.3
AOS-206355	–	**LLDP** process crashed during zero touch provisioning in Mobility Controller. The issue was observed in switches running ArubaOS 8.2.2.6 and later versions. This issue occurred due to memory corruption. The fix ensures that memory corruption does not occur, and switches work as expected.	AOS-W 8.2.2.6

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206433	–	A few APs failed to send a DNS query to the server to resolve the managed device. As a result, the APs did not come up on the managed device. The fix ensures that the APs send the DNS query to resolve the managed device. This issue was observed in 100 Series and 200 Series access points running ArubaOS 8.5.0.0 or later versions.	AOS-W8.5.0.5
AOS-206452	–	An unknown IP address was displayed for Standby switch in the **Dashboard > Overview > Clients > Wireless Clients** page in the WebUI. The fix ensures that the unknown IP address is not displayed for the wireless clients. This issue occurred when no standby controller was available. This issue was observed in Mobility Master running AOS-W8.6.0.2 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.2
AOS-206496 AOS-210126 AOS-213859 AOS-214883 AOS-214912	–	A few 802.1X clients were unable to connect to an SSID. This issue was observed in APs running AOS-W 8.6.0.5 or later versions. The fix ensures seamless connectivity.	AOS-W 8.6.0.5
AOS-206498 AOS-212922	–	APs running AOS-W 8.5.0.0 or later versions were unable to ping the managed devices. This issue occurred when the APs were configured as Remote APs and were present behind the NAT device. The fix ensures that the APs work as expected.	AOS-W 8.5.0.0
AOS-206517	–	A captive portal username changed after 802.1x reauthentication. The fix ensures that the username does not change after 802.1x reauthentication. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-206537	–	The H flag indicating standby tunnel is not displayed in the output of the show datapath tunnel-table command and this results in a network loop. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206541	–	The **Maintenance > Software Management** page did not display the list of all managed devices that are a part of a cluster. This issue was observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W8.5.0.8
AOS-206577	–	When the **no mtu** command was issued, it returned a validation error. This issue was observed when a Layer-2 IPv6 GRE tunnel was formed between managed devices.	AOS-W 8.7.0.0
AOS-206629 AOS-206636	–	L2TP VPN connection failed on Mac, iOS, and Android clients connected to the managed device. The fix ensures that the managed device works as expected. This issue occurred when: • Clients initiated L2TP connection on random src port instead of the standard src port, 1701. • Clients connected behind a NAT device. This issue was observed in managed devices running ArubaOS 8.4.0.6 or later versions.	AOS-W 8.4.0.6

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206653	–	The **SAPD** process crashes on a managed device and IPv6 APs are stuck in D flag. This issue was observed in CPsec-enabled VPNCs. The fix ensures that the **SAPD** process works as expected.	AOS-W 8.7.0.0
AOS-206689	–	A few users were unable to add a username with a period to local-userdb. The fix ensures that the users are able to add the username. This issue was observed in stand-alone controllers running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206713 AOS-207273 AOS-207332	–	Users were unable to remove a managed device from the L2 connected cluster. The fix ensures that the users are able to remove the managed device. This issue was observed in Mobility Controller Virtual Appliance running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.8
AOS-206725	–	High CPU utilization was observed on Mobility Master when the user inserts a USB modem. This issue was observed in Mobility Masters running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-206765 AOS-208978	–	A few show commands fail to display output. The fix ensures that the show commands display the output. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-206801	–	A managed device running AOS-W 8.2.2.3 or later versions contacts the Activate server more than once during ZTP. This issue was observed in managed devices running ArubaOS 8.2.2.3 or later versions.	AOS-W 8.2.2.3
AOS-206817	–	The **Dashboard > Overview > Wireless Clients** page displayed invalid values for Standby switch. The fix ensures that the WebUI displays the correct values for Standby switch. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-206861	–	An SNMP trap was not generated for a bridge mode user. The fix ensures that the SNMP trap is generated. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-206878	–	The Fing mobile application discovered two connected clients and was unable to isolate them, although deny-inter-user-traffic and deny-inter-user-bridging were enabled. This issue is resolved by configuring deny-inter-user-traffic or deny-inter-user-bridging globally on the firewall, irrespective of VLAN BCMC. This issue was observed in managed devices running ArubaOS 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-206888 AOS-211560 AOS-211565 AOS-214729	–	OAW-AP515 and OAW-AP555 access points running AOS-W 8.7.0.0 or older versions took up to 30 minutes to be operational and join the managed device. This issue occurred when they are provisioned in a native IPv6 deployment and the value of **RA interval** is larger in the network. The fix ensures that OAW-AP515 and OAW-AP555 access points work as expected in native IPv6 deployment.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206888	–	A few APs took up to 30 minutes to be operational and join the managed device, when they were provisioned for the first time in a native IPv6 deployment. This issue was observed in AP-515 and AP-555 access points running AOS-W 8.7.0.0 in a cluster setup.	AOS-W 8.7.0.0
AOS-206890	–	The body field in the **Configuration > Services > Guest Provisioning** page of the WebUI did not allow users to add multiple paragraphs for email messages. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206891	–	A delay was observed in sending the RADIUS interim accounting messages. This issue occurred when the clients roamed between controllers. The fix ensures that there is no delay in sending the RADIUS interim accounting messages. This issue was observed inMobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-206896	–	Some Remote APs running AOS-W 8.6.0.4 or later versions took a log time to failover. The fix ensures that Remote APs work as expected.	AOS-W 8.6.0.4
AOS-206902 AOS-208241	–	An AirGroup user was unable to connect to Sonos speakers. The fix ensures that users can connect to Sonos speakers. This issue was observed in managed devices managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-206907	–	Some AP-303H access points running AOS-W 8.5.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: assert**. The fix ensures that the access points work as expected.	AOS-W 8.5.0.5
AOS-206929	–	The show global-user-table command did not provide an IPv6 based filtering option. This issue was observed in Mobility Masters running AOS-W8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-206930	–	Some Mobility Masters running AOS-W 8.7.0.0 or later versions allowed to configure the same IPv6 address twice. This issue occurred when the user enters the same IPv6 address in a different format.	AOS-W 8.7.0.0
AOS-206998 AOS-208353 AOS-212541	–	A few APs running AOS-W 8.6.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **[Kilchoman] AP555 crash: NOC_error.c:473 NOCError: FATAL ERRORparam0 :zero, param1 :zero, param2 :zero**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.2
AOS-207007	–	Clients were unable to connect to few APs intermittently. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-207011	–	A few AP-325 access points running ArubaOS 8.5.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: TARGET ASSERT DUE TO MORE THAN 5 RECOVERY**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.5.0.5

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207037	–	Stale route entries removed from branch controllers showed up in master controllers. The issue was observed in controllers running AOS-W 6.5.3.3. The fix ensures that the stale entries removed from branch controllers are removed automatically from master controllers.	AOS-W 6.5.3.3
AOS-207039	–	In a few APs running AOS-W 8.7.0.0 Fine Timing Measurement is not set in neighbor report. The fix ensures that Fine Timing Measurement is enabled.	AOS-W 8.7.0.0
AOS-207053	–	A few incorrect MAC addresses in the same subnet were listed in the mesh portal. The fix ensures that the wrong entries of the mesh portal are removed from the mesh link table. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.7
AOS-207056	–	The managed devices in datazone e was unable to forward L2 GRE packets. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-207073	–	An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Fatal exception in interrupt: PC is at dma_cache_maint_page+0x64/0x160, LR is at __dma_page_dev_to_cpu+0x2c/0xe4**. Enhancements to the wireless driver resolved this issue. THis issue was observed in AP-305 access points running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-207157 AOS-208746 AOS-213492 AOS-213612	–	Mobility Master lost the server certificate and hence, the newly added managed devices were unable to download server certificate from the Mobility Master. The fix ensures that the server certificate is always available on the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-207159	–	The **Diagnostics > Tools > AAA Server Test** page incorrectly displayed the Authentication value as failed instead of timeout in the WebUI. The fix ensures that the timeout value is displayed for the Authentication field in the WebUI. This issue occurred while connecting to a server that was down. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.4

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207175 AOS-207961 AOS-208334 AOS-211183 AOS-217736 AOS-215466 AOS-216791	–	A few APs running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: External-WDT-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.4
AOS-207237	–	A few clients were unable to connect to APs running AOS-W 8.6.0.4 or later versions. The fix ensures seamless connectivity. **Duplicates:** AOS-203038, AOS-209048, AOS-210038, AOS-210443, AOS-210641, AOS-210664, AOS-212228, AOS-212388, AOS-213327, AOS-213496, AOS-209237, AOS-209443, AOS-211008, and AOS-216192	AOS-W 8.6.0.4
AOS-207303	–	Users were unable to add a managed device to an existing cluster of managed devices configured with rap-public-ip address. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-207337	–	After upgrading from AOS-W 8.2.x.x to AOS-W 8.5.0.0- FIPS or later versions, a few managed devices were stuck in the **LAST SNAPSHOT** state. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-207358	–	Some APs running AOS-W 8.7.0.0 or later versions logged the error message, **ctrlr not found, ip 0.0.0.0 id (3.57.164.244,5ef0f615,18)**. The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-207397	–	The AirWave graph for some clients displayed zero value. The fix ensures that the correct graph is displayed. This issue occurred when the CL_TX_DATA_BYTES_TRANSMITTED counter and the CL_RX_DATA_BYTES counter were decremented from AMON_STATION_STATS_MESSAG counter, and the wireless clients downloaded huge files from the wired FTP servers. This issue was observed in 7030 controllers running ArubaOS 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-207416	–	The output of the **show whitelist-db rap** and **show ap database long** commands displayed the status of the Remote AP as Provisioned and R-c2 respectively, although the Remote AP was authenticated using the AP authorization profile. The fix ensures that the Remote AP is authenticated in whitelist database and the AP moves to Rc2 authenticated state. This issue was observed in Remote APs connected to stand-alone controllers running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.8

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207458 AOS-205925	–	When the **show ucc client-info** command was issued, a stand-alone switch did not display the UCC client data. The fix ensures that the UCC client data is displayed. This issue was observed in stand-alone switches running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-207492 AOS-210872	–	A few clients were not redirected to the captive portal page. The fix ensures that captive portal works as expected. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-207552	–	A mismatch of MTU value was observed between the AP and the controller. The fix ensures that the MTU value is consistent across the AP and the controller. This issue occurred when the AP was rebooted after setting the default value of the rap-gre-mtu parameter. This issue was observed in APs connected to stand-alone switches running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-207567	–	Wireless clients did not connect to the nearest access points. This issue was observed in access points running AOS-W 8.5.0.4. The fix ensures that the clients automatically connect to the nearest access points.	AOS-W 8.5.0.4
AOS-207619 AOS-210965 AOS-216192	–	A few clients were not redirected to the captive portal page. The fix ensures that captive portal works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.13
AOS-207629	–	A Mobility Master running AOS-W 8.3.0.0-FIPS displayed the PPTP port status as open although FIPS mode disable both the PPTP configuration and PPTP port. The fix ensures that the PPTP port is not open in FIPS mode.	AOS-W 8.3.0.0-FIPS
AOS-207664 AOS-213842 AOS-214256	–	The WebUI login banner text was not displayed after upgrading the managed device to ArubaOS 8.5.0.0 or later versions. The fix ensures that banner text appears after the upgrade.	AOS-W 8.5.0.10
AOS-207664 AOS-213842	–	The login banner text was not displayed after upgrading the managed device to AOS-W 8.5.0.0 or later versions. The fix ensures that the login banner text is displayed after an upgrade.	AOS-W 8.5.0.10
AOS-207692	–	Some managed devices running AOS-W 8.6.0.4 or later versions logged multiple authentication error messages. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.4
AOS-207775 AOS-213087 AOS-215946	–	The **Auth** process crashed on managed devices running AOS-W 8.5.0.9 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.9

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207791	—	The **udbserver** process crashed multiple times on a managed device running AOS-W 8.5.0.8 or later versions. The fix ensures that the managed device works as expected.	AOS-W 8.5.0.8
AOS-207795	—	Users were unable to access the WebUI of the Mobility Master. The fix ensures that users are able to access the WebUI. This issue was observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-207893	—	A client was unable to receive an IP address. The fix ensures that memory utilization in APs is regulated by the creation of a new boot log file at every restart instance of the BLE daemon process. This issue occurred due to high memory utilization in the AP caused by the BLE daemon process. This issue was observed in APs running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-207915	—	A few 500 Series access points running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: BadAddr:ecf47526bb436b6e PC:wlc_mutx_ bw_policy_update+0x156c/0x2938 [wl_v6] Warm-reset.** The fix ensures that the AP works as expected. **Duplicates:** AOS-208119, AOS-209128, AOS-210182, AOS-210217, AOS-211247, AOS-211252, AOS-211715, AOS-211774, AOS-212111, AOS-212235, AOS-212557, AOS-212741, AOS-212930, AOS-212961, AOS-214656, AOS-214965, AOS-215250, OS-215656, AOS-217649, and AOS-217692	AOS-W 8.6.0.4
AOS-207915	—	Some 500 Series access points running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as A**P Reboot reason: BadAddr:ecf47526bb436b6e PC:wlc_mutx_ bw_policy_update+0x156c/0x2938 [wl_v6] Warm-reset.** The fix ensures that the AP works as expected. **Duplicates:** AOS-208119, AOS-209128, AOS-210182, AOS-210217, AOS-211247, AOS-211252, AOS-211715, AOS-211774, AOS-212111, AOS-212235, AOS-212557, AOS-212741, AOS-212930, AOS-212961, AOS-214656, AOS-214965, AOS-215250, AOS-215656, AOS-217649, and AOS-217692	AOS-W 8.6.0.4
AOS-207970	—	A few APs running AOS-W 8.7.0.0 or later versions stopped sending unicast packets after a few configuration changes. The fix ensures that APs continue to send unicast packets.	AOS-W 8.7.0.0
AOS-208030 AOS-208287 AOS-209499	—	A few clients were unable to connect to APs. This issue occurred when EAPOL frames were not sent from the AP. The fix ensures that APs work as expected. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208044 AOS-211207	—	The **stm** process crashed on Mobility Masters running AOS-W 8.7.0.0 or later versions. This issue occurred when AP regulatory configuration was reset. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208044 AOS-211207	—	The **smt** process crashed on Mobility Masters running AOS-W8.7.0.0 or later versions. This issue occurred when AP regulatory configuration was reset. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.7.0.0
AOS-208067 AOS-211569	—	Allowlist database was not getting updated when Clustering was enabled in managed devices. This issue was observed in ArubaOS 8.7.0.0. The fix ensures that allowlist database gets updated when clustering is enabled.	AOS-W 8.7.0.0
AOS-208102 AOS-214040	—	Some APs running AOS-W 8.7.0.0 crashed and rebooted unexpectedly. The log file listed the reason for the event as **Process /aruba/bin/sapd has too many open files (771)**. The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-208113	—	Intermittent data loss was observed for a few clients connected to APs. The fix ensures that APs work as expected. This issue was observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-208193	—	User-based tunneled node and the users were not removed even after a heartbeat failure. The fix ensures that the tunneled node is removed after a heartbeat failure. This issue was observed in standby switches running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.1
AOS-208269 APS-213010	—	Clients experienced poor performance with APs. Also, APs did not prioritize traffic from active stations and hence, stations went to sleep mode. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208337 AOS-209348 AOS-212655 AOS-213442	—	The **airmatch_recv** process crashed on Mobility Controller Virtual Appliances running AOS-W 8.5.0.7 or later versions. The fix ensures that the Mobility Controller Virtual Appliances work as expected.	AOS-W 8.5.0.7
AOS-208420	—	Users were unable to log in to CLI of a switch. This issue occurred when the password had special characters, < and/or >. The fix ensures that users can log in to the CLI of a switch. This issue was observed in switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.5

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208421 AOS-209367 AOS-209509 AOS-209606 AOS-211577 AOS-211772 AOS-211879 AOS-212502	–	A few managed devices running AOS-W 8.5.0.12 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Soft Watchdog reset**. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.12
AOS-208438	–	Captive portal failed in bridge forwarding mode APs running AOS-W 8.7.0.0 or later versions. This issue occurred due to an empty AP netdestination list. The fix ensures that captive portal works in bridge forwarding mode APs.	AOS-W 8.7.0.0
AOS-208483	–	Users failed to timeout after an AP reboot and the user entries were retained in the user table although the clients were disconnected. This issue occurred when the wireless clients connected using bridge mode switched to a VAP terminated on another managed device deployed in a different cluster environment. The fix ensures that the user entries are removed from the user table after the clients get disconnected. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-208492 AOS-208806	–	A few APs logged the **Phony BSSID Detection** error message and detected its own BSSIDs as phony BSSIDs. The fix ensures that the APs work as expected. This issue was observed in Air Monitor APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-208515	–	The radio usage graph in OmniVista 3600 Air Manager got reset to zero. The fix ensures that the radio usage graph does not reset to zero. This issue occurred while downloading large files. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-208553	–	The **Test** button in **Diagnostics > Tools > AAA Server Test** was grayed out for read-only users. The fix ensures that the test button is not grayed out for read-only users. This issue was observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-208557	–	OAW-AP534, OAW-AP535, and OAW-AP555 access points running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **reboot reason: due to Assertion failed! ic->ic_curchan->ic_ieee == dfs->dfs_curchan->dfs_ch_ieee:dfs_process_radar_found_ind.c:961**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.4
AOS-208568	–	The **show ap essid** command displayed incorrect **VLAN(s)** values. The fix ensures that the correct VLAN values are displayed. This issue was observed in managed devices running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208625	–	RADIUS accounting packets did not have location and AP group related details. The fix ensures that location and AP group related details are available in RADIUS accounting packets. This issue was observed in managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-208686	–	The **Wireless call quality** page in the WebUI displayed two different score types without any header. This issue is resolved by changing the **End-to-End** score to **MOS Score** to and the **Wireless-only** and **Controller** score to **UCC** Score. This issue was observed in Mobility Masters running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-208696	–	The **profmgr** process crashes after configuring LACP and the error message, **Module profmgr is busy** is displayed. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208728 AOS-208559	–	Users were unable to change the port configuration status to untrusted. The fix ensures that users are able to change the port configuration status. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208790	–	A few APs running AOS-W 8.5.0.9 or later versions logged the error message**, Unexpected stm (Station management) runtime error at wifi_mgmt_recv_frame, 10284, wifi_mgmt_recv_frame:10284: NULL src-mac, frame type=0, subtype=15**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.9
AOS-208807	–	The CLI displayed the list of expired certificates which were deleted using the WebUI and hence, resulted in configuration failure when new certificates were added. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208854	–	The output of the **show ap vlan-mcast** command did not display any information. The fix ensures that the command output displays the required information. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions	AOS-W 8.3.0.0
AOS-208987	–	Clients stayed in the post auth role in the bridged captive portal even after a session timeout. This issue occurred when the clients were authenticated or deauthenticated before timeout. The fix ensures that the clients are not stuck in the post auth role. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-209069	–	The control plane security configuration, **auto-cert-allowed-addrs** pushed from a Mobility Master to the managed devices was not visible in the **Configuration > System > CPSec** page of the WebUI. The fix ensures that the WebUI displays the control plane security configuration. This issue was observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209086 AOS-216862	–	The **dot1x** module crashed on managed devicesunexpectedly. The fix ensures that the managed devices work as expected. This issue was observed in OAW-4104controllers running AOS-W8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-209130	–	Stale user entries were not removed from the user-table and hence, new users could not connect to the managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209136	–	A few clients were disconnected due to the Tx fail reached maximum error. This issue occurred due to an incorrect state of variables in the AP while peer STA is in power save state, which lead to the packets being sent out when the peer STA was also 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 8.3.0.0 or later versions. The fix ensures that the state of variables in APs power save state machine is updated correctly.	AOS-W 8.3.0.0
AOS-209165	–	The **Configuration > AP Groups** page did not sort the list of AP groups based on when they were created, and hence the newly created AP groups were displayed at the bottom of the table. The fix ensures that the WebUI sorts the list of AP groups. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-209196 AOS-213746	–	Some APs rebooted unexpectedly. The fix ensures that the APs work as expected. The issue occurred when tunnel forwarding mode, **dot11k**, and **WPA3** were enabled in AP. This issue was observed in OAW-AP345 access points running AOS-W8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-209243 AOS-210135	–	Some OAW-AP535 access points running AOS-W 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-209256	–	An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Out of memory**. The fix ensures that APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209273	–	The **Dashboard > Infrastructure** page of the WebUI did not display the data in graphical charts for mesh APs. The fix ensures that the WebUI displays the graphs for mesh APs. This issue was observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-209276	–	**AESCCM Decryption Invalid Replay Co** displayed twice in the output of show datapath crypto counters with different values. The fix ensures that correct value is shown.	AOS-W 8.5.0.10

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209323	–	The **Server Group Match Rules** option for **Internal** server in the **Authentication > Auth Servers** page of the WebUI was not available in Mobility Masters running AOS-W 8.7.0.0 or later versions. The fix ensures that the WebUI displays the **Server Group Match Rules** option for **Internal** server.	AOS-W 8.7.0.0
AOS-209324	–	The **lagm** process crashed while configuring port channels. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.6
AOS-209402	–	A few clients experienced dot1X timeout in split tunnel mode.This issue occurred when multiple wired clients are connected to an AP. The fix ensures that the clients do not experience dot1X timeout. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-209406 AOS-211798 AOS-215512 AOS-215574 AOS-215869	–	The **ISAKMPD** process crashed on managed devicesrunning AOS-W 8.5.0.10 or later versions. The fix ensures that the managed deviceswork as expected.	AOS-W 8.5.0.10
AOS-209533	–	While importing guest entries from CSV file, users were unable to download the summary text file. The fix ensures that users are able to download the summary text file. This issue was observed in stand-alone switches running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-209551	–	A few OAW-RAPs running AOS-W 8.5.0.10 or later versions rebooted unexpectedly. This issue occurred when the **activate whitelist download** command was executed. The fix ensures that the OAW-RAPs work as expected.	AOS-W 8.5.0.10
AOS-209553	–	A few Mobility Controller Virtual Appliances allowed users to log in to the Debug CLI during boot up without requesting for the AOS-W decryption key. The fix ensures that users log in to Debug CLI only after entering the v decryption key. This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-209574 AOS-210108 AOS-211758 AOS-214855	–	Some APs running AOS-W 8.7.0.0 crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: MemLeak: mem low**. The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-209612	–	The value of Tx data bytes transmitted for 5 GHz radio was lower than the actual transmitted value. The fix ensures that the actual values are transmitted for 5 GHz radio. This issue was observed in OAW-AP205 access points running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209626 AOS-215091	–	A few clients experienced connectivity issue. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209640	–	A few clients did not receive IP addresses from the VLAN configured on LLDP-MED network policy profile. The fix ensures that clients receive the IP addresses. This issue was observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-209648	–	A few users were unable to revert the AP blacklist time configuration. This issue is resolved by issuing the **no ap ap blacklist-time** command to restore the inherited or default configuration. This issue was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-209679 AOS-210115	–	The **SAPD** process crashed on APs running AOS-W 8.5.0.10 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-209691	–	Clients were unable to pass traffic with packet size more than 1470. This issue occurred when connected to mesh point APs. The fix ensures that the clients are able to pass traffic. This issue was observed in stand-alone switches running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209701 AOS-215784	–	A few APs did not send ACK packets and users were unable to connect to APs running AOS-W 8.5.0.10 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-209748 AOS-215172 AOS-217181	–	Some users were unable to make configuration changes to the existing RADIUS server profile at the device level. The log file listed the reason for the event as **Reference retrieval error**. The fix ensures that the users are able to make changes to an existing RADIUS server profile. This issue was observed in Mobility Masterrunning AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-209774 AOS-209778	–	The old outer IP address of an AP was displayed in the user table. The fix ensures that the stale entries are remove from the user table. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209774 AOS-209778	–	The old outer IP address of an AP was displayed in the user table. The fix ensures that the stale entries are removed from the user table. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209783	–	After a reload of the Mobility Master, OAW-RAPs and VIA clients with ECDSA Suite B certificates overloaded the **ISAKMPD** process. As a result, the **ISAKMPD** process became unresponsive. The fix ensures that IKE exchanges are throttled at the beginning of the tunnel establishment and it is restricted only to a certain maximum number of exchanges at a time. 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 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209797	–	A Mobility Master Hardware Appliance running AOS-W 8.6.0.4 or later versions intermittently returned high values for SNMP walk for OID **ifOutDiscards**. The fix ensures that the Mobility Master Hardware Appliance does not return incorrect values for SNMP walk for OID **ifOutDiscards**.	AOS-W 8.6.0.4
AOS-209805	–	A few users were not assigned VLANs and hence, they did not receive IP addresses and experienced connectivity issues. This issue occurred when users were connected to MPSK BSSIDs. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-209855 AOS-210214 AOS-211809 AOS-212590 AOS-212823 AOS-214704	–	A few APs running AOS-W 8.7.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-209873	–	The AOS-W 8.6.0.5 syslog guide did not have information about **u-encr-alg=0x1 m-encr-alg=0x1** error message. The syslog reference guide is updated with description for the error message.	AOS-W 8.6.0.5
AOS-209892	–	The output of the **show usb** command did not display the status of the USB port when a OAW-4005 switch was powered on with 802.3af POE power source. The fix ensures that the command output displays the status of the USB port as **External USB port is Disabled as Controller is powered ON with PoE**. This issue was observed in OAW-4005 switches running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-209912	–	A few managed devices failed to filter and drop spoofed ARP responses from the clients that sent ARP response for the IP address that did not belong to the clients. The user entry for the other IP address was present on the managed devices but not in the route cache table. The fix ensures that the managed devices are able to stop ARP spoofing attacks for such clients. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209916	–	A managed device running AOS-W 8.6.0.0 or later versions displayed the **Sos packet processing: bad opcode 0x3a, expects VRRP (hapiSosReceive)** error message. The fix ensures that the managed device works as expected.	AOS-W 8.6.0.0
AOS-209977	–	SNMP query with an incorrect community string failed to record the offending IP address in the trap or log information. The fix ensures that the offending IP address is updated correctly in the trap or log message. This issue was observed in stand-alone switches running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209996	–	A few APs running AOS-W 8.5.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: __bug**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.9
AOS-209998	–	A few users were unable to configure a password for VPN dialer in the **Configuration** > **Roles** > **VPN** page of the WebUI. The fix ensures that the users are able to configure a password for VPN dialer configuration. This issue was observed in managed devices running AOS-W 8.6.0.5-FIPS or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.5-FIPS
AOS-210004 AOS-213784 AOS-216298	–	A server received multiple **GSM radio lookup failed, error(error_htbl_key_not_found)** notifications for all BSSIDs. This issue is resolved by moving the GSM lookup failure logs to user-debug category. This issue was observed in a Mobility Master running AOS-W 8.6.0.5.	AOS-W 8.6.0.5
AOS-210065 AOS-213825	–	A few users were unable to connect to an AP. This issue occurred when AirMatch sent incorrect configurations to the AP. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.10
AOS-210122 AOS-215655	–	Clients were unable to receive the IP addresses from their respective VLANs. The fix ensures that the clients are able to receive the IP addresses. This issue occurred when the clients were connected to a OAW-RAP. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.7.0.0
AOS-210126 AOS-213859 AOS-214883 AOS-214912	–	A few 802.1x clients were unable to connect to an SSID. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-210276	–	The **Activate username** and **Activate password** fields were populated under **Configuration** > **System** > **Whitelist** page in the WebUI of the secondary Mobility Master, though the Activate credentials were not configured in the CLI. The fix ensures that the Activate credentials are not displayed in the WebUI. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-210342	–	The VRRP authentication password was not encrypted in the output of the **show running config** command. The fix ensures that the VRRP authentication password is encrypted in the command output. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210385 AOS-203760	–	A few managed devices running AOS-W 8.8.0.0 displayed the **KERNEL: [40741.546880] denverton-pinctrl INTC3000:00 / gpio gpiochip0: registered chardev handle for line 75** error message unexpectedly. The fix ensures that the managed devices work as expected.	AOS-W 8.8.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210404	–	The **Pending Changes** option did not appear in the WebUI. The fix ensures that the WebUI displays the **Pending Changes** option. This issue occurred when there were too many unsaved nodes and the **show configuration unsaved-nodes** command had an output of more than 1024 characters. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.7
AOS-210416 AOS-210480	–	The **show ap client trail-info** command displayed incorrect VLAN values. The fix ensures that the correct VLAN values are displayed. This issue was observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-210448	–	A few OAW-AP200 Series access points running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. This issue occurred when wireless containment was enabled. Enhancements to the wireless driver resolved the issue.	AOS-W 8.6.0.4
AOS-210481	–	The **Dashboard** > **Infrastructure** > **Clusters** page did not list all the clusters. The fix ensures that the WebUI displays the list of available clusters. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.5
AOS-210482	–	A few managed devices running AOS-W 8.3.0.6 or later versions display the **Invalid set request** error message, while configuring ESSID for a **Beacon Report Request** profile in the WebUI. The fix ensures that the error message does not appear in the WebUI.	AOS-W 8.3.0.6
AOS-210484	–	A few managed devices did not display the 802.11k measurements from clients. The fix ensures that the managed devices display the 802.11k measurements. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.6
AOS-210506	–	Clients were disconnected from the network because some APs changed channels. The fix ensures seamless connectivity. This issue occurred when AirMatch was configured after 48 hours of a failover. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.8
AOS-210529	–	A few users were unable to upgrade the managed device using the WebUI. The fix ensures that the users are able to upgrade the – using the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210638	–	The **ARM** process crashed on managed devices running AOS-W 8.6.0.5 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.5
AOS-210715	–	The **ValidUser** ACL displayed only IPv6 entries even when the PEFNG license was not enabled. The fix ensures that the **ValidUser** ACL displays all valid entries. Scenario: This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.4

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210805	–	The **Traffic Analysis** window in the **Dashboard** > **Overview** > **Wireless Clients** page displayed the **Error retrieving information Please try again later** error message. The fix ensures that the WebUI displays the traffic analysis data. This issue was observed in stand-alone switches and managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-210845 AOS-217214 AOS-217871	–	OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first.** Enhancements to the wireless driver resolved the issue.	AOS-W 8.6.0.6
AOS-210896	–	Hotspot 2.0 IEs were not present in beacons frames. The fix ensures that the Hotspot 2.0 IEs are present in beacons frames. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.0
AOS-210990	–	A few managed devices sent BPDUs when STP was globally disabled. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-210992	–	**Flow Group delete: id not found** error message was displayed after upgrading Mobility Masters to 8.6.0.5. This issue was observed in Mobility Masters running AOS-W 8.6.0.5. The fix ensures that the upgrade is done without error message.	AOS-W 8.6.0.5
AOS-211227	–	Some APs sent beamforming sounding frames during **EAPoL** authentication. The fix ensures that beamforming sounding frames are sent after **EAPoL** authentication. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W8.6.0.5
AOS-211256	–	SFP J8177C/J8177D with part numbers 1990-4606 were not working in switches running AOS-W 8.6.0.3 or later versions. The fix ensures that the switches works as expected.	AOS-W 8.6.0.3
AOS-211324	–	A few iPads were unable to connect to SSIDs. The log file listed the reason for the event as **STA Requesting Association without authentication**. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.8 or later versions. The fix ensures seamless connectivity.	AOS-W 8.5.0.8
AOS-211389	–	A few users were unable to install new evaluation licenses on the Mobility Master running AOS-W 8.5.0.0 or later versions in a Mobility Master-Managed Device topology. The fix ensures that the evaluation licenses are installed successfully on the Mobility Master. This issue occurred due to a corrupt license database entry.	AOS-W 8.5.0.4
AOS-211429	–	The **Authmgr** process generated the **Error ERROR: value too long for type character varying(32)** error message when the TACACS user name exceeded 32 characters. The fix ensures that the managed devices work 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

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-211430	–	The WebUI did not display the list of APs and clients. This issue occurred when VRRP IPv4 / IPv6 dual stack was used to form IPsec tunnel between the Mobility Master and the managed device. The fix ensures that the WebUI lists the APs and clients present in the network. This issue was observed in Mobility Master running AOS-W8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-211452	–	The output of the **show ap ble-database** command did not display the corrupt or incorrect APB. This issue is resolved by displaying the corrupt or incorrect APB (where the BLE MAC address is all zeros) in the output of the **show ap ble-database** command. This issue was observed in managed devices running AOS-W 8.8.0.0	AOS-W 8.8.0.0
AOS-211472	–	Captive portal failed to send mails to guest accounts. This issue occurred when the SMTP server failed to validate the host. This issue was observed in stand-alone controllers running AOS-W 8.7.0.0 or later versions. The fix ensures that Captive portal works seamlessly.	AOS-W 8.7.0.0
AOS-211472	–	Captive portal failed to send mails to guest accounts. This issue occurred when the SMTP server failed to validate the host. The fix ensures that the captive portal works as expected. This issue was observed in stand-alone controllers running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-211476	–	Some APs came up in a restricted mode after upgrading from AOS-W 8.2.2.6 to AOS-W8.6.0.5 or later versions. This issue occurred due to AP LLDP power negotiation interoperability issue with Cisco 9000 switches. The fix ensures that the APs do not come up in restricted mode.	AOS-W 8.6.0.5
AOS-211545 AOS-217654	–	A few APs crashed and rebooted due to **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue was observed in Mobility Masters and managed devices running AOS-W 8.5.0.10 or later versions	AOS-W 8.5.0.10
AOS-211587 AOS-216068	–	High CPU utilization was observed in **udbserver** and **postgres** processes. This issue was observed in managed devices running AOS-W 8.7.1.0. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.0
AOS-211658	–	A few clients were unable to connect to OAW-AP535 access points running AOS-W 8.6.0.5 or later versions in a cluster setup, when WMM and HT configurations were enabled. The log file listed the reason for the event as **Ptk Challenge Failed**. The fix ensures seamless connectivity.	AOS-W 8.6.0.5
AOS-211699 AOS-212564 AOS-212567 AOS-212599 AOS-212604 AOS-215978 AOS-217452	–	A few OAW-AP505 access points running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic by RCU: WARNING: CPU: 3 PID: 3215 at kernel/softirq.c:155local_bh_enable_ip+0xd4/0xe0()**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.5

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-211782	—	Users were unable to delete a policy assigned to a role and the error message, **No Changes Done** was displayed. This issue was observed in Mobility Masters running AOS-W 8.7.0.0 or later versions. The fix ensures that users are able to delete a policy assigned to a role.	AOS-W 8.7.0.0
AOS-211841	—	The **Dashboard > Infrastructure** page of the WebUI displayed the client status as **Unknown**. The fix ensures that the WebUI displays the correct status of clients. This issue was observed in managed devicesrunning AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-211863	—	Some APs did not come up on managed devices running AOS-W 8.6.0.5 or later versions. This issue occured when the forwarding mode was changed to bridge mode and when the name of the ACL reached the maximum size of 64 bytes. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.5
AOS-211878 AOS-214377	—	Some APs failed to come up as OAW-RAPs. This issue occurred when the MTU size was not adjusted automatically. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-212039	—	User debug logging information was not available in the **Configuration > System > Logging > Logging Levels** page of the WebUI. This issue was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions. The fix ensures that the WebUI displays the user debug logging information.	AOS-W8.5.0.10
AOS-212063 AOS-216153	—	Licenses were installed with incorrect dates in Mobility Masters running AOS-W 8.5.0.10 or later versions. The fix ensures that the licenses are installed with valid details.	AOS-W 8.5.0.10
AOS-212123	—	The SNMP trap **wlsxNUserAuthenticationFailed** was not generated upon failed authentication in a termination-enabled dot1X configuration. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions. The fix ensures that the SNMP trap is generated upon failed authentication.	AOS-W 8.0.0.0
AOS-212203 AOS-212560 AOS-213878 AOS-213879	—	Some users experienced poor network performance. This issue occurred due to 2.4G beacon power fluctuation in OAW-AP505 access pints running AOS-W 8.6.0.5 or later versions. The fix ensures optimal network experience.	AOS-W 8.6.0.5
AOS-212255	—	Some APs were stuck in **Not in Progress** state during cluster live upgrade. This issue was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-212423	—	High bandwidth usage was observed on a few clients. The fix ensures optimal bandwidth usage. This issue occurred when AP ports in split tunnel forwarding mode were moved to tunnel forwarding mode. This issue was observed in managed devicesrunning AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212432 AOS-212634 AOS-212958	–	The **Datapath** process crashed on OAW-4750XM switches running AOS-W 8.7.1.0 or later versions. This issue was observed on a cluster when a switchover happened. The fix ensures that the controllers work as expected.	AOS-W 8.7.1.0
AOS-212458 AOS-215059 AOS-215163	–	Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Take care of the TARGET ASSERT first at NOC_error**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP535 access points and OAW-AP555 access points running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-212486 AOS-216471	–	L2TP IP address leak is observed and VLAN pool gets exhausted. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W8.5.0.11, or later versions.	AOS-W 8.5.0.11
AOS-212554	–	VIA connection failed and high ISAKMP CPU usage was observed. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-212568		The **aaa / certmgr / cpsec** security categories in the **Configuration > System > Logging > Logging Levels** page of the WebUI displayed **None** even if values were configured. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. The fix ensures that the WebUI displays the aaa / certmgr / cpsec security categories.	AOS-W 8.0.0.0
AOS-212576	–	Some APs running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly due to a race condition. The log file listed the reason for the event as **Kernel panic - not syncing: rcu_sched detected stalls (pc is at __schedule+0x78/0x360).** The fix ensures that the APs work as expected.	AOS-W 8.6.0.5
AOS-212599 AOS-211699 AOS-212564 AOS-215978 AOS-212567 AOS-217452	–	APs running AOS-W 8.3.0.0 or later versions crashed and reboot unexpectedly. The log files listed the reason for the event as, **Kernel panic - not syncing: jiffies stall (pc is at __schedule+0x78/0x360)**. The fix ensures that the AP works as expected.	AOS-W 8.3.0.0
AOS-212686		Some APs sent high numbers of SAP MTU frames than the configured value. This issue occurred when fragmented GRE packets were exchanged. This issue was observed in APs running AOS-W 8.6.0.6 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.6.0.6
AOS-212707	–	Some Mobility Masters running AOS-W 8.5.0.10 displayed the error message, **Fri Oct 16 23:58:53 2020, 0, 0, 0, 0,0, 0, 0**. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.5.0.10

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212755	–	Some users connecting to OAW-AP505 access points running AOS-W 8.7.0.0 were unable to pass traffic intermittently. The fix ensures that clients are able to pass traffic.	AOS-W 8.7.0.0
AOS-212843	–	802.11r clients in bridge mode were assigned the default role instead of the derived role. This issue was observed in managed devicesrunning AOS-W 8.0.0.0 or later versions. The fix ensures that the clients get the derived role.	AOS-W 8.0.0.0
AOS-212856	–	A few managed devicesrunning AOS-W 8.6.0.2 or later versions displayed a very low **Max/Actual-EIRP value**. The fix ensures that the managed devices display the correct **Max/Actual-EIRP value**.	AOS-W 8.6.0.2
AOS-212861 AOS-215350 AOS-215522 AOS-216305	–	OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first.** The fix ensures that the AP works as expected.	AOS-W 8.6.0.6
AOS-212885 AOS-214735	–	Some OAW-AP345access points were stuck in boot loop after an upgrade. The log file listed the reason for the event as, **BUG in aruba_wlc.c:4527/aruba_radio_update().** This issue was observed in OAW-AP345 access points running AOS-W 8.7.1.0 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.7.1.0
AOS-212935	–	Temporary ACL was still applied to user roles even if the disaster-recovery mode was disabled. This issue occurred when configuration changes in disaster recovery mode were not submitted using the write memory command. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-212973 AOS-216286	–	The **no ipv6 enable** command did not disable the IPv6 feature. The fix ensures that the command disables the IPv6 feature. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-212991	–	The **use-ip-for-calling-station** parameter of the **aaa authentication-server radius** command did not work as expected for VIA clients. This issue was observed in stand-alone switches running AOS-W 8.6.0.6 or later versions. The fix ensures that the command works as expected.	AOS-W 8.6.0.6
AOS-213089	–	Some managed devices running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:30:2)**. The fix ensures that the managed devices work as expected. **Duplicates**: AOS-213044, AOS-213295, AOS-214238, AOS-214429, AOS-214431, AOS-214678, AOS-215123, AOS-215572, and AOS-216951.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213099 AOS-214123 AOS-215367 AOS-216451 AOS-216612 AOS-217647	—	The **dpagent** process crashes on managed devices running AOS-W8.5.0.10 or later versions.The fix ensures that the managed devices work as expected. **Duplicates**:AOS-217721, AOS-217942, AOS-217943, AOS-218405	AOS-W 8.5.0.10
AOS-213115	—	Some managed devices running AOS-W8.5.0.10 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first**. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.10
AOS-213132 AOS-216300	—	Users are unable to upload server certificates in PEM or DER format. This issue was observed in Mobility Master running AOS-W8.6.0.6-FIPS. The fix ensures that the Mobility Masterdevices work as expected.	AOS-W 8.6.0.6
AOS-213191 AOS-217421 AOS-217537	—	**Dashboard > infrastructure > Controllers > Network Map** did not load on Mobility Master running AOS-W 8.6.0.5. The fix ensure that infrastructure map is displayed.	AOS-W 8.6.0.5
AOS-213242 AOS-215607 AOS-218659	—	Some APs did not connect to the network. The fix ensures that the APs work as expected. This issue occurred due to high noise level and channel utilization on the 2.4 GHz band. This issue was observed in OAW-AP535 access points and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-213305 AOS-213310	—	Some OAW-AP515 access points running AOS-W8.7.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **PC is at wlc_nar_dotxstatus+0x88/0x7d8: AOS-200674 instrumentation kicks in (wlc_nar_validate_cubby)**. The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-213308	—	Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **PC is at asap_ap_dev_xmit+0x118/0x4d0**. The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-213309 AOS-213949	—	Some AP-515 access points running AOS-W8.7.0.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at wlc_ratesel_clr_cache+0x2c/0xa0**.The fix ensures that the APs work as expected.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213490 AOS-214916	—	The value of **wlanAPRxDataBytes64** was displayed as 0. The fix ensures that the correct value is displayed. This issue was observed in stand-alone controllers running AOS-W8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-213510	—	The IoT manager did not send the correct configuration to APB. The fix ensures that the IoT feature works as expected. This issue was observed in Mobility Masters running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-213558	—	Users are unable to add a new node to an existing cluster of eight nodes. This issue was observed in managed devices running AOS-W8.5.0.6 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.6
AOS-213614 AOS-206852	—	A managed device running AOS-W8.6.0.2 or later versions sent disconnect-ACK messages using VRRP IPv6 address instead of sending the message using physical IPv6 address. Hence, ClearPass Policy Manager continuously sent disconnect request messages to the same client. The fix ensures that the managed device works as expected.	AOS-W 8.6.0.2
AOS-213856		The **show ap remote debug heartbeat-miss-trace** command displays only UTC time in time field. This issue was observed in managed devicesrunning AOS-W8.7.1.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.0
AOS-213865		The WebUI displays the message, **one or more settings have been overridden at bottling** and displays the older folder name after an override. This issue was observed in Mobility Masters running AOS-W8.5.0.10 or later versions.	AOS-W 8.7.1.0
AOS-213924 AOS-217233	—	The Mobility Controller Virtual Appliance dashboard displayed incorrect VLAN ID details for some wired users. This issue was observed in stand-alone controllers running AOS-W 8.7.0.0 or later versions. The fix ensures that the WebUI displays correnct VLAN IDs.	AOS-W 8.7.0.0
AOS-213941 AOS-215645	—	Some AP-575 access points running AOS-W 8.7.1.0 rebooted unexpectedly. The log file listed the reason for the reboot as **thermal shutdown**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.0
AOS-214099	—	The ACL did not block session traffic to a particular website, when application rules and forwarding rules were used together in a PBR rule. The fix ensures that ACL blocks traffic based on the PBR rule. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-214165 AOS-203374	—	VIA authentication timed out although the server responded without any delay. This issue was observed in OAW-4550controllers running AOS-W8.0.0.0 or later versions. The fix ensures that the VIA authentication works without delay.	AOS-W 8.3.0.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-214243 AOS-215775	–	A managed device running AOS-W 8.5.0.0 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:b0:2)**. The fix ensures that the managed device works as expected. This issue occurred due to a race condition.	AOS-W 8.7.1.0
AOS-214255		Older 802.11b clients are unable connect to a few APs.This issue occurs when VAPs on 2.4 GHz radio are configured with different basic rates and when some of which do not include 802.11b CCK rates. This issue was observed in OAW-AP203R, OAW-AP203RP, OAW-AP203H, and OAW-AP207 access points running AOS-W8.3.0.0 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
AOS-214261		Some clients experienced connectivity issues while roaming. This issue was observed in OAW-AP535access points running AOS-W8.5.0.10 or later versions.The fix ensures seamless connectivity.	AOS-W 8.5.0.10
AOS-214321 AOS-215683	–	Clients are either unable to connect to the AP or are getting disconnected when the **SAPD process** over utilizes memory. This issue was observed in OAW-AP205 access points running AOS-W8.5.0.6 and the client was roaming to new AP. The fix ensures that the wireless clients obtain the IP address from APs as expected.	AOS-W 8.5.0.6
AOS-214529 AOS-192680	–	The RADIUS attributes configured using RADIUS modifier profile were not sent in the RADIUS request for clients during 802.1x authentication.This issue was observed in managed devices running AOS-W8.4.0.0 or later versions.The fix ensures that the attributes from RADIUS modifier profile are sent in RADIUS request for 802.1x clients.	AOS-W 8.5.0.1
AOS-214714	–	A few stand-alone controllers running AOS-W 8.5.0.11 or later versions crashed and rebooted unexpectedly. The crash happened only when DPI was enabled. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the stand-alone controllers work as expected.	AOS-W 8.5.0.11
AOS-214829	–	OAW-AP115 access points running AOS-W8.3.0.0 were unable to connect to a controller. The issue was observed in managed devices running AOS-W8.3.0.0 or later versions. The fix ensures that the APs are authenticated as expected.	AOS-W 8.3.0.0
AOS-214835 AOS-218512	–	It was observed that the data transfer speed in OAW-AP315 access points running AOS-W 8.3.0.0 was less. The issue was observed in managed devicesrunning AOS-W 8.3.0.0 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
AOS-215012 AOS-215567	–	The **ap debug counters** values for **Bootstraps** and **Reboots** did not reset after an upgrade. The fix ensures that the upgrade resets the **Bootstraps** and **Reboots** values. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W8.5.0.11

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-215022		Clients authenticated using wpa3-sae-aes with MAC authentication were disconnected from the network. This issue was observed in managed devices running AOS-W8.5.0.9 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.5.0.9
AOS-215073	–	Few OAW-AP515 access points running AOS-W 8.5.0.8 or later versions crashed unexpectedly and rebooted after several minutes. This issue occurred when many virtual AP configurations are sent from the **SAPD** to **AP-STM** process. The fix ensures that the APs work as expected.	AOS-W 8.5.0.8
AOS-215084 AOS-215085 AOS-215086 AOS-215087 AOS-215088 AOS-215089	–	The **hwMon** process crashed unexpectedly in a few managed devices running AOS-W 8.3.0.3 or later versions in a Mobility Master-Managed Device topology. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.3
AOS-215107 AOS-212656 AOS-212696	–	Users were unable to load custom captive portal page when **Use HTTP for authentication** option was enabled. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions. The fix ensures that the custom captive portal page loads properly.	AOS-W 8.5.0.11
AOS-215576	–	A few managed devices running AOS-W 8.6.0.7 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Nanny rebooted machine - gsmmgr process died (Intent:cause:register 34:86:0:2c)**. This issue occurred due to a memory leak. The fix ensures that the managed devices work as expected. **Duplicates**: AOS-215484, AOS-215550, AOS-216996, AOS-217224, AOS-217226, AOS-217248, AOS-217305, AOS-217431, AOS-217697, AOS-217756, AOS-217901, AOS-217984, AOS-218046, AOS-218072, and AOS-218079	AOS-W 8.6.0.7
AOS-215641 AOS-217628 AOS-217640	–	The **ISAKMPD** process crashes on managed devices running AOS-W8.6.0.0 or later versions in a PSK-RAP setup. **Duplicates**:AOS-215205, AOS-215714, AOS-217268, AOS-215642, AOS-21564, AOS-217362	AOS-W 8.7.1.1
AOS-215774	–	BLE did not work in an AP. This issue occurred because of a wrong firmware on the the AP. This issue is resolved by updating the firmware on the AP. This issue was observed in OAW-AP303P access points running AOS-W 8.6.0.6.	AOS-W 8.6.0.6
AOS-216133	–	Clients were unable to connect to APs on A-band channels. The fix ensures that clients can connect to APs on A-band channels. This issue was observed in APs running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0

Table 7: *Resolved Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216204	—	Some OAW-AP535 access points running AOS-W8.5.0.10 or later versions crashed unexpectedly. The log file listed the reason for the event as, **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**.The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-216205	—	OAW-AP535 access points running AOS-W 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: CPU 0 stall.** The fix ensures that the AP works as expected.	AOS-W 8.5.0.10
AOS-217035	—	APs were down and were unable to connect to the managed device. This issue occurred when UDP traffic was sent without establishing IPsec tunnels. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-217082 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 captive portal authenticates the users. This issue was observed in managed devices running AOS-W8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-217452 AOS-212599	—	Some APs running AOS-W8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: rcu_sched detected stalls by cpu: 2, count: 2**. The fix ensures that the APs work as expected. **Duplicates**: AOS-215978, AOS-211699, AOS-212564, AOS-212567	AOS-W 8.6.0.5

Chapter 6
Known Issues and Limitations

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

Limitations

Following are the limitations observed in this release.

Port-Channel Limitation in OAW-4850 switches

On OAW-4850 switches with all the member ports of each port-channel configured from the same NAE (Network Acceleration Engine), if one of the member ports experiences link flap either due to a network event or a user-driven action, the rest of the port-channels also observe the link flap for less than a second.

Custom Certificate

When AOS-W is downgraded from 8.8.0.0 to 8.7.0.0, an AP retains the custom certificate that was synchronized in AOS-W 8.8.0.0. In AOS-W 8.8.0.0, an AP downloads the custom certificate from a managed device and saves it in its flash memory if a bridge mode SSID is configured. If the managed device is downgraded to AOS-W 8.7.0.0, the AP is also downgraded. The AP that is running AOS-W 8.7.0.0 checks if any custom certificate is saved in its flash memory. If the AP finds a custom certificate saved in its flash memory, it uses the custom certificate. If the AP does not find a custom certificate saved in its flash memory, it generates a new default certificate. If you do not want to use the custom certificate, issue the following command to erase the flash sector:

```
apfcutil -i RAP
```

The AP reboots and generates new default certificate.

Known Issues

Following are the known issues observed in this release.

Table 8: *Known Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-185166	–	An AP image upgrade over TFTP fails when the **serverip** configuration in an AP is set to the VRRP IP address for the VLAN in the switch. This issue is observed in OAW-4850 switches running AOS-W 8.3.0.6. **Workaround**: Configure the **serverip** to the interface IP address for the VLAN.	AOS-W 8.3.0.6
AOS-201205 AOS-215376	–	Some APs are unable to switch partition after a successful upgrade. This issue is observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-209127	–	Internal server timeout is observed during an authentication request. This issue is observed in stand-alone switches with master-redundancy setup using **VRRP** environment, where the stand-alone switches are running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-210383	–	The **Cluster Members** pop-up window under **Dashboard > Infrastructure > Clusters** page does not display any value for **Hostname**, **Role**, and **Reachable** fields in the WebUI. This issue occurs when the user configures IPv6 cluster in the WebUI. This issue is observed in Mobility Masters running AOS-W 8.8.0.0 in a Mobility Master-Managed Device topology.	AOS-W 8.8.0.0
AOS-211070	–	The **Cluster Live Upgrade** process fails on a managed device and displays **Controller x.x.x.x is down** message. This issue occurs due to a mismatch of IP address families between the cluster and the Mobility Master-Managed Device connectivity (both connections needs to use the same version of IP, either IPv4 or IPv6. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions in a Mobility Master-Managed Device topology. **Workaround**: Ensure that the cluster and the Mobility Master-Managed Device connectivity belong to the same IP address family (either IPv4 or IPv6).	AOS-W 8.5.0.10
AOS-211423	–	An ongoing Teams call is terminated and classification for new sessions does not occur. This issue occurs when an third client joins an ongoing video conference call in the Teams. This issue is observed in managed devices running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-211634	–	The **Controller** field is not updated in the WebUI. This issue occurs on cluster-failover during an ongoing Teams call. This issue is observed in managed devices running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-212288	–	Some managed devices are displayed as unknown after the Mobility Master **L2** failover. This issue is observed in Mobility Masters and managed devices running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-212847	–	The **Maintenance > Software Management > Upload AOS image for controller** page of the WebUI does not allow users to upload multiple images subcutaneously. This issue is observed in Mobility Masters running AOS-W 8.8.0.0.	AOS-W 8.8.0.0

Table 8: *Known Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212858	–	The **Maintenance > Software Management > Upload AOS image for controller** page of the WebUI does not allow users to delete multiple images subcutaneously. This issue is observed in Mobility Masters running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-212941	–	The newly configured VLANs are not displayed when the show vlan command is executed. And, after a flash backup restore, the logging was disabled. This issue is observed in managed device running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-213157	–	A Mobility Master fails to perform version check of managed devices during image upgrade process. This issue occurs when the managed devices are running AOS-W 8.7.0.0 or earlier versions. This issue is observed in Mobility Masters running ArubaOS 8.8.0.0 in a cluster setup.	AOS-W 8.8.0.0
AOS-213345	–	The output of the **show ap image-preload status <summary/all/list>** command does not display the list of APs. This issue is observed in managed devices running AOS-W 8.8.0.0 in a cluster setup.	AOS-W 8.8.0.0
AOS-213428	–	The **Upgarademgr** process does not provide FQDN support for image servers. This issue is observed in Mobility Masters running AOS-W 8.8.0.0 version.	AOS-W 8.8.0.0
AOS-214016	–	The **wpa3_sae** process crashes on Mobility Masters running AOS-W 8.8.0.0 version.	AOS-W 8.8.0.0
AOS-215624 AOS-215652	–	Some OAW-AP325 access points are unable to come up on the Managed Device. The log file lists the reason for the event as **Reboot after image upgrade failed.** This issue is observed in OAW-AP325 access points running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-215727 AOS-216896	–	Stale AP entries that were cleared using the **clear gap-db** command prior to the upgrade reappears on the Mobility Master after the upgrade. This issue is observed in Mobility Masters running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-215989	–	A few 802.11ax clients experience a drop in throughput when they connect to multiple 802.11ax OFDMA-enabled APs running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-216926	–	The status of a managed device changes to Config Failure. This issue occurs when the alg-teams-audio app ACL is configured. This issue is observed in managed devices running AOS-W version acl was configured	AOS-W 8.8.0.0

Table 8: *Known Issues in AOS-W 8.8.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218219	—	A Teams call with an external client is not classified and prioritized. This issue is observed in managed devices running AOS-W 8.8.0.0.	AOS-W8.8.0.0
AOS-218578	—	Mobility Master fails to upgrade in a dual stack topology. This issue occurs when two managed devices are connected on a IPv6 network. This issue was observed managed devices running AOS-W bedlore 8.8.0.0.	AOS-W8.7.0.0
AOS-219048	—	An AP does not obtain an IP address from a service AP. This issue occurs when a OAW-AP325 access point uses Wi-Fi Uplink and AP-577 access point as the service AP. This issue is observed in access points running AOS-W 8.8.0.0.	AOS-W 8.8.0.0

Chapter 7
Upgrade Procedure

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

CAUTION

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 75 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 75 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 75 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

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.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 74.

NOTE

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

In the WebUI

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

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

NOTE

The AOS-W image file is digitally signed and is verified using RSA2048 certificates preloaded at the factory. The Mobility 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.

NOTE

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 75 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 75 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 75.
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:

CAUTION

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot Controller after upgrade**.
   d. Click **Upgrade**.

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

   The Mobility 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.