AOS-W 8.6.0.0

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	Updated the **Limitations** section stating no ZTP and multi-version support for OAW-4104 switches.
Revision 03	The following Resolved issues have been added: ■ AOS-184873 ■ AOS-187306 Added OAW-41xx Series Hardware OmniAccess Mobility Controllers in **Supported Platforms** section.
Revision 02	Added description regarding cluster support for OAW-RAPs in the **Features** section.
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

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

For a list of terms, refer Glossary.

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

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

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

802.11mc Fine Timing Measurement

802.11 mc Fine Timing Measurement (responder mode only) can be enabled on 510 Series access points by navigating to **Configuration > System > Profiles > Wireless LAN > Virtual AP > Advanced setting** and enabling the check box **Fine Timing Measurement (802.11mc) Responder Mode.**

Agile Multiband Operation (MBO)

AOS-W provides Agile Multiband support on 802.11ax capable APs. MBO enables the network to utilize the available spectrum efficiently, and helps in optimizing connectivity experience for the end-users. MBO can be enabled using the WebUI or CLI. The following CLI commands were modified to enable MBO and CDC:

- **show ap association**
- **show ap bss-table**
- **wlan ssid-profile**

AP Conversion

A new command, **ap convert**, is introduced to convert OAW-APs or OAW-RAPs to OAW-IAPs and Openconfig APs. You can convert the APs, AP lists, or AP groups using local-flash or local image server options like ftp, tftp, http, https, or scp by copying the downloaded image from Alcatel-Lucent support to the local ftp/tftp/scp server.

```
(host) [mynode] #ap convert
   active
   add
   cancel
   clear-all
   delete
```

Blacklisting

Starting from AOS-W 8.6.0.0, the spoofed deauth blacklist feature is not supported.

BSS Color and BSS Color Switch Count

The Alcatel-Lucent 802.11ax based access points like OAW-AP505, OAW-AP515, OAW-AP534. OAW-AP535, and OAW-AP555 support BSS coloring mechanism and you can set the number of times the BSS color switch announcements are sent in beacons before switching to a new color.

Bulk Configuration of Stand-alone Controllers

AOS-W supports bulk configuration of stand-alone controllers by replacing the configuration files in the stand-alone controllers and rebooting them.

Centralized Licensing for IPv6 Network

AOS-W supports the centralized licensing feature in IPv6 network, where both license servers and license clients contain IPv6 addresses configured on the managed device. The managed device containing IPv4 or IPv6 address acts as the license client and communicates with the license server containing IPv6 address to obtain the available licenses.

ClearPass Policy Manager Support to Whitelist OAW-RAPs

AOS-W provides support for ClearPass Policy Manager to whitelist OAW-RAPs in a cluster environment. You can configure ClearPass Policy Manager as an external server that authenticates OAW-RAPs using the MAC address of OAW-RAPs.

Cluster Support for OAW-RAPs

AOS-W supports up to 12 node clusters for OAW-RAPs. Now, the OAW-RAPs can terminate on a cluster with more than 4 nodes.

Configuration Using APIs

AOS-W supports a config replace API, which is used to configure a node or device with specific configurations. This feature helps automate the configuration based on few configuration files.

Configuring Destination Port for Syslog Server

Starting from AOS-W 8.6.0.0, Users can configure the destination port for syslog server by navigating to **Configuration > System > Logging** in the **Managed Network** node hierarchy.

Configuring both Session and Route ACL

Starting from AOS-W 8.6.0.0, Users can configure both session and route ACL for branch-vpnc tunnel traffic using the **vpn-acl** command.

Custom SIP

AOS-W supports the custom SIP feature. Custom SIP classifies and prioritizes the SIP media traffic that is compliant with SIP protocol but uses non-standard port for SIP signaling.

Default Value of host-ageout-time Parameter

The default value of the Openflow controller's **host-ageout-time** parameter is changed to 3600 seconds.

Execute the following command to view the value of the **ofc host-ageout-time** parameter:

```
(host) [mynode] #show openflow-controller

Openflow-controller
-------------------
Parameter                   Value
---------                   -----
ofc state                   Enabled
ofc host-ageout-time        3600 sec
ofc mode                    passive
ofc certificate-file        none
ofc key-file                none
ofc ca-certificate-file     none
ofc tls                     Disabled
ofc port                    6633
ofc topology-discovery      Disabled
ofc auxiliary-channel-port  6633
```

Deleting Users from Mobility Master

Starting from AOS-W 8.6.0.0, **aaa user delete** command can be executed from the Mobility Master using the **ip-addr<ip-addr> and macaddr <macaddr>** parameters.

Downloading Log Files

Users can download the log files of Flash file system, Startup configuration and Running configuration to their local system by navigating to **Maintenance > Technical Support > Copy files** under **Mobility Master** node hierarchy.

Enabling 802.11mc Fine Timing Measurement

Starting from this release, 802.11mc Fine Timing Measurement can be enabled on 510 Series access points using the CLI command **wlan virtual-ap**.

Enhancements to EST Profile

Starting from AOS-W 8.6.0.0, the following EST enhancements can be configured by the user,

- User name and password for EST authentication.
- Organizational Unit Name.
- Arbitrary levels for EST enrollment and re-enrollment.
- Change the username/password and challenge password fields without de-activating and re-activating the EST profile.

Global AP Table Size

AOS-W supports an increase in **global ap table** size to ensure that the users can view all the APs operating in a dense environment and detect or monitor more number of rogue BSSID entries.

IoT Proxy Server

Starting from AOS-W 8.6.0.0, AOS-W supports the configuration of a proxy server in an IoT transport profile. You can use a proxy server to send IoT data to the final destination when a direct link cannot be established with the server.

IoT Vendor Filter

Starting from AOS-W 8.6.0.0, AOS-W supports the vendor filter that is either a vendor name or vendor ID of the IoT device. You can configure up to five comma separated vendor names, vendor ID, or any combination of vendor name or vendor ID in vendor filter of an IoT transport profile.

IPv6 Support for Mobility Master Redundancy Configuration

AOS-W provides IPv6 support for Mobility Master's Layer-2 and Layer-3 redundancy configuration, as well as establish communication between Mobility Masters and managed devices by using VPNC. This feature allows seamless migration of network infrastructure to IPv6 without compromising the Mobility Master redundancy.

IPv6 Support for Policy-Based Routing

AOS-W provides IPv6 support for next-hop lists in policy-based routing rule.

IPsec Tunnels using GCM ciphers

Starting from AOS-W 8.6.0.0, an IPsec tunnel can be established between managed devices and APs using GCM ciphers. The IPsec tunnel can be established without loading the ECDSA custom certificates. By default, the APs send the GSM cipher algorithm in the IPsec set, along with the current cipher list. New dynamic maps are created on the managed devices to establish the IPsec tunnels with GCM ciphers.

Per- Command Authorization with TACACS+ Servers

Starting from AOS-W 8.6.0.0, AOS-W supports per-command authorization for management users with TACACS+ Servers running on ClearPass Policy Manager. This feature gives flexibility in determining commands to be allowed for each management user at each configuration-node. The allowed and not-allowed commands for each management user can be configured on the TACACS+ servers. The commands executed by the management user will be sent to the TACACS+ server for authorization and only the authorized commands can be executed. Otherwise, the command triggered will be denied.

Enhancements to OAW-AP325 and OAW-AP335 access points

Starting from AOS-W 8.6.0.0, OAW-AP325 and OAW-AP335 access Points can detect LTE-U signals in the WLAN spectrum.

Enhancements to 510 Series access points

The 510 Series APs now support the following features:

- 512 client support
- DL-MU-MIMO
- Spectrum analysis
- BSS Coloring Support

Enhancements to 530 Series and 550 Series access points

The 530 Series and 550 Series APs now support the following features:

- 3G / 4G USB modems
- Wi-Fi Hotspot
- 1024 client support
- Spectrum analysis
- Real Time Protocol Analysis (RTPA) support

Role- Based ACL

Starting from AOS-W 8.6.0.0 Role- Based ACL can now be applied to users residing in different switches by configuring a policy domain group profile.

Session and Route ACL for traffic coming over IPSec Tunnel

Starting from AOS-W 8.6.0.0, session and route ACL can be applied to traffic coming over IPSec tunnel. The command **vpn-acl** configures both session and route ACL for branch-vpnc tunnel. This feature is supported only for hub and spoke topology.

Support for SES-Imagotag Cloud TLS Authentication

AOS-W allows an AP with ESL USB dongle to connect to the SES cloud by using TLS authentication. This allows you to configure and update the ESL through the SES cloud.

Support for Enhanced Open Security and WPA3 in Decrypt-Tunnel Mode

Starting from AOS-W 8.6.0.0, all access points and managed devices support enhanced open security and WPA3 in decrypt tunnel mode.

Support for MySphera Tag

MySphera is a leading provider of BLE-based asset tracking tags and services. When a MySphera BLE tag broadcasts an advertisement, an AP obtains the RSSI information, computes the location of the tag, and relays the location information to a destination server.

Support for AmberBox Sensor

AOS-W supports AmberBox detectors and gateways that connect to a USB port in an AP. The AP relays the traffic from the detector or gateway to the destination server.

Support for New 4G Modem

Starting from AOS-W 8.6.0.0, the Inseego Skyus SC4 USB 4G modem is supported on OAW-RAPs.

Support for Nordic Zigbee USB Dongle

Starting from AOS-W 8.6.0.0, APs which do not have an integrated Zigbee radio, support Nordic nRF52840 Zigbee USB dongle to provide IoT services.

Support for Hanshow USB Dongle

AOS-W supports Hanshow USB dongles. A Hanshow dongle plugs into the USB port of an Alcatel-Lucent AP and transfers electronic shelf label data from computer, server, or cloud to electronic shelf label tags through the AP. The USB port of the AP works as a wired Ethernet port and supports bridge and tunnel modes.

Support for ABB Sensor

AOS-W supports the following ABB sensors and forwards the IoT data from these sensors over Telemetry-HTTPS and Telemetry-websocket server types:

- Motor sensor
- Pump sensor
- Bearing sensor
- Ambient sensor
- ECM drive sensor
- CoMo sensor

Support for Stateful Failover of Roaming Clients

During a UAC failure, hitless failure of high-value application traffic such as voice is supported when the client roams between BSSIDs.

Thermal Shutdown Support in Access Points

The Alcatel-Lucent 530 Series and 550 Series APs support operating temperatures of up to 50°C (indoor) or 60°C (outdoor). Starting from AOS-W 8.6.0.0, these APs are enabled with thermal shutdown feature. The **show ap power-mgmt-statistics** command introduced in AOS-W 8.6.0.0 displays the highest temperature, lowest temperature, and the current temperature of the AP.

Tri-radio support for 550 Series Access points

Starting from AOS-W 8.6.0.0, Tri-Radio mode is supported in 550 Series access points. In Split 5 GHz or tri-radio mode, radio 0 will operate in lower 5 GHz band range scanning channel 36-64, radio 2 will operate in upper 5 GHz band scanning channel 100-165. Radio 1 will operate in full 2.4 GHz band scanning channel 1-13. Tri-radio mode supports the following features,

- ClientMatch
- Station Management
- AirMatch
- SAPD/SAPM
- Spectrum Analysis
- Cluster
- MultiZone
- Mesh
- Controller Datapath Tunnel ID
- Firmware

WebRTC Prioritization

Starting from AOS-W 8.6.0.0, AOS-W supports the WebRTC prioritization feature that prioritizes the media traffic from WebRTC sources. WebRTC prioritization provides better end user experience, dashboard visibility of all WebRTC applications like voice, video, and application sharing, and call quality monitoring for audio calls using upstream and downstream RTP analysis.

WebUI Support for Cluster Members

AOS-W displays a **Cluster Members** pop-up window under **Dashboard > Infrastructure > Clusters** page in the WebUI. The **Cluster Members** pop-up window displays a summary of each cluster member and includes the connection type - L2, L3, or both used by the cluster member.

WebUI Support to Blacklist Clients

Users can manage blacklisted clients in both stand-alone switches and Mobility Masters by using the WebUI. AOS-W now forwards the client blacklist to the database of all the managed device in a Mobility Master-Managed Device topology. As a result, users can blacklist clients in multiple managed devices in the same hierarchy.

WebUI Support to Configure IoT Transport Profile

The AOS-W webUI allows configuration of an IoT transport profile.

Wi-Fi RTLS and BLE Telemetry Streams

Starting from AOS-W 8.6.0.0, the Wi-Fi RTLS and BLE telemetry streams are combined into a single telemetry stream in the IoT transport profile. This optimizes the integration of telemetry streams with third party location engines.

ZTP using DHCPv6 options

AOS-W supports using DHCPv6 options to get master information for zero touch provisioning of the managed devices when the users are unable to use Activate. Option 16 provides the vendor information and the option 17 of the DHCPv6 provides information such as master IPv6 address, VPNC information and so on.

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 8.6.0.0*

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 8.6.0.0*

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
MC-VA-xxx Virtual OmniAccess Mobility Controllers	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 8.6.0.0*

AP Family	AP Model
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
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303
OAW-AP303H Series	OAW-AP303H

Table 5: *Supported AP Platforms in AOS-W 8.6.0.0*

AP Family	AP Model
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
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP387	OAW-AP387
500 Series	OAW-AP504, OAW-AP505
510 Series	OAW-AP514, OAW-AP515
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555
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_72905

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-125897 AOS-155697 AOS-187598 AOS-189036 AOS-192082 AOS-192723 AOS-192731 AOS-192734	151952 191568	When a managed device rebooted, APs and clients rebooted without IP addresses and other fields. The fix ensures no fields are missing when clients come up after a reboot. This issue was observed in managed devices running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-128004 AOS-128971 AOS-132396 AOS-132895 AOS-133089 AOS-136197 AOS-191835	154915 156084 160639 161262 161499 165351	A few APs crashed and rebooted unexpectedly when a wireless client tried to establish a connection to its BSS ID. The fix ensures that the APs work as expected. This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-128555	155631	A memory leak was found as a result of using a script to query the Dashboard in managed devices running AOS-W 8.3.0.0. The fix ensures that the managed device work as expected. This issue occurred when certain Monitoring Dashboard queries were run either using a script or the WebUI, where memory relating to the query filter strings were not freed.	AOS-W 8.3.0.0
AOS-131325 AOS-146748	159222 179137	The number of clients displayed in the active-standby IP field on the Mobility Master dashboard was incorrect. This issue occurred due to a cluster failover causing race condition. The fix ensures that the dashboard displays the correct values. This issue was observed in Mobility Master running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-131364 AOS-186846	159267	The **isakmpd** process in switches crashed unexpectedly. This issue occurred when simultaneous re-keys were triggered between the switches that had multiple site-to-site tunnels established between them. The fix ensures that the **isakmpd** process does not crash and the switches work as expected. This issue was observed in OAW-4450, OAW-4750, and OAW-4750XM switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-137885	167418	A managed device rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed device works as expected. This issue occurred when DPI was disabled. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions in a master-local topology. **Duplicates:** **New IDs:** AOS-137994, AOS-138825, AOS-139619, AOS-140506, AOS-140640, AOS-142059, AOS-142131, AOS-142374, AOS-142436, AOS-142459, AOS-142938, AOS-142941, AOS-143251, AOS-143359, AOS-143490, AOS-143812, AOS-144011, AOS-144031, AOS-144595, AOS-144997, AOS-145474, AOS-146676, AOS-146869, AOS-147106, AOS-147108, AOS-150112, AOS-150425, AOS-151192, AOS-154648, AOS-158202, AOS-189735, AOS-192533. **Old IDs:** 167550, 168626, 169681, 170922, 171101, 172951, 173031, 173338, 173414, 173443, 174062, 174068, 174472, 174613, 174798, 175219, 175480, 175502, 176206, 176793, 177432, 179043, 179301, 179768, 179770, 183956, 184356, 185389, 190064, 195103.	AOS-W 8.2.0.0
AOS-140223	170522	Some APs rebooted unexpectedly at various locations due to a random memory corruption. The fix ensures that the APs do not crash. This issue was observed in APs running AOS-W 8.0.0.0 or later versions. **New IDs:** AOS-137992, AOS-139067, AOS-139068, AOS-139236, AOS-139954, AOS-139996, AOS-140035, AOS-140405, AOS-140440, AOS-142709, AOS-140498, AOS-142702, AOS-140699, AOS-140727, AOS-142269, AOS-140917, AOS-142069, AOS-142008, AOS-142011, AOS-142066, AOS-142715, AOS-142843, AOS-142869, AOS-142909, AOS-143020, AOS-143118, AOS-143163, AOS-143385, AOS-143430, AOS-143438, AOS-143819, AOS-143961, AOS-144314, AOS-145172, AOS-145450, AOS-145451, AOS-146659, AOS-147731, AOS-148278, AOS-150376, AOS-150999, AOS-155130, AOS-155131, AOS-155134, AOS-175738, AOS-176812, AOS-177001, AOS-177068, AOS-177105, AOS-177236, AOS-177239, AOS-178067, AOS-190731 **Old IDs:** 167229, 167548, 167831, 167864, 168537, 168658, 168972, 168973, 169050, 169078, 169199, 169563, 169712, 170137, 170202, 170252, 170431, 170786, 170823, 170824, 170834, 170914, 170948, 171126, 171189, 171231, 171499, 171697, 171919, 171935, 172894, 172897, 172932, 172958, 172961, 173211, 173333, 173497, 173770, 173777, 173786, 173942, 173970, 174021, 174120, 174124, 174171, 174296, 174360, 174642, 174710, 174720, 175226, 175415, 175860, 177020, 177405, 177406, 178484, 179023, 179701, 180755, 181551, 184299, 185146, 190707, 190708, 190712	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-140453 AOS-140742 AOS-140942 AOS-145285 AOS-147285 AOS-154327 AOS-182833 AOS-187546	170839 171247 171529 177178 180034 189649	The output of the **show ap monitor ap-list** command displayed corrupt SSID information for an AP. The fix ensures that the AP drops the corrupt packets. This issue occurred when the AP tried to process some corrupt packets. This issue was observed on OAW-AP325 access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-140512 AOS-185844 AOS-187810	170929	A managed device failed to boot up during the **Initializing CFGM** stage of the initial setup. The fix ensures that the managed device works as expected. This issue was observed managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-140986 AOS-185962	171594	The log files of a managed device listed the **authmgr [3425]: <522125> <3425> <WARN> |authmgr| Could not create/find bandwidth-contract for user, return code (-11)** warning message. The fix ensures that the warning message is not displayed. This issue occurred when a bandwidth contract was not allocated to the user if the user was assigned a role which did not have a bandwidth contract configured. This issue was observed in managed devices running AOS-W 8.3.0.0.	AOS-W 8.2.0.2
AOS-141387 AOS-186364	172109	The AP driver log listed the **vap-0 AP PS: AID=4342056 select next response** error message. This issue is resolved by removing the debug log messages in the AP driver. This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-142627 AOS-189127	173673	The **Dashboard** page in the WebUI of a Mobility Master showed incorrect status of the moved managed devices. This issue occurred when the device **default-node** parameter was configured in the CLI and managed devices were deleted in the WebUI. The fix ensures that the **Dashboard** page displays the correct status of the moved managed devices. This issue was observed in Mobility Masters running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-141647 AOS-143919 AOS-146338 AOS-187192	172019 172464 175355 178584	A Mobility Master displayed high CPU utilization. This issue is resolved by allowing clients to choose non-ECDH-based ciphers. High mode includes only ECDHE and DHE ciphers, medium mode includes only DHE and RSA ciphers, and low mode includes only RSA ciphers. This issue occurred when the Web Server accepted ECDH-based ciphers proposed by a client. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-142968 AOS-143134 AOS-144431 AOS-145646 AOS-146413 AOS-148222 AOS-152443 AOS-158329 AOS-177195 AOS-177687 AOS-178219 AOS-187690 AOS-187691	174100 174320 175992 177665 178689 181469 187116 195288 173924 176293 179464	An AP did not support fast recovery. The fix ensures that the AP works as expected. This issue was observed in OAW-AP303H, OAW-AP305, OAW-AP315, OAW-AP325, and OAW-AP335 access points running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-143514 AOS-143768 AOS-184333	174823 175163	The **Authentication** process crashed unexpectedly. This issue occurred when the aaa test-server verbose command was executed. The fix ensures that the **Authentication** process works as expected. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-144527 AOS-187683	176124	When a write erased managed device was loaded with AOS-W 8.4.0.0 software using ZTP, the managed device was automatically downgraded to a version that was present in Activate. The fix ensures that the ZTP based automatic upgrade feature upgrades the device depending on the provisioning response from Activate and will ignore the mandatory upgrade only if the version in the Activate is same as that of the managed device. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-144684 AOS-184346	176339	Log files on few managed devices contained incorrect or garbled ESSID and BSSID values. The fix ensures that these incorrect messages are not generated. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
AOS-145854 AOS-186448 AOS-186600 AOS-185757	177936	The WebUI and CLI did not allow a user to change an expired WebUI certificate on a Mobility Master running AOS-W 8.2.1.0. The log file listed the **Error: server certificate <certificate-name> not found in path /sc** error message. The fix ensures that the WebUI and CLI allow a user to successfully change the expired WebUI certificate with a new one on the Mobility Master. This issue occurred while uploading a certificate.	AOS-W 8.2.1.0
AOS-146118	178291	The **dir** CLI command did not contain some basic options like sorting by date, name, size, and filtering by keyword. The fix ensures that the missing options are available in the command. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-146236 AOS-146760 AOS-153009 AOS-153097 AOS-153713 AOS-153714 AOS-178929 AOS-180416 AOS-185034 AOS-186200 AOS-187344 AOS-187509 AOS-191018	178445 179150 187925 188032 188837 188838 182020 189319	An AP running AOS-W 8.2.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt: PC is at dma_cache_maint_page LR is at __dma_page_dev_to_cpu**. Enhancements to the wireless driver resolved the issue.	AOS-W 8.2.0.0
AOS-146331 AOS-183502 AOS-184796 AOS-185200 AOS-189634 AOS-192923	178574	A few managed devices running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. This issue occurred due to datapath crash. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.0
AOS-146670 AOS-152310 AOS-157311 AOS-182295 AOS-184295 AOS-187138	179034 186931 193759	Clients experience poor performance with OAW-AP300 Series access points. Enhancements to the wireless driver has resolved this issue. The issue occurred in OAW-AP300 Series access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-146680 AOS-189368	179047	An AP crashed unexpectedly. The log file listed the reason for this event as **PC is at wlc_apps_bss_ps_off_done+0x54/0x118 [wl] and LR is at wlc_mbss_shm_ssid_upd+0x2f8/0x330 [wl]**. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP345 access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-146916 AOS-193067	179360	A managed device displayed the **Module L2TP is busy. Please try later** error message and did not provide an L2TP IP address. The fix ensures that the managed device provides an L2TP IP address and works as expected. This issue occurred when the **show vpdn l2tp local pool** command was executed. This issue was observed in managed devices running AOS-W 8.0.0.0.	AOS-W 8.0.0.0
AOS-147018 AOS-186071	179516	An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: softlockup: hung tasks**. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP203H access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-147151 AOS-192908	179828	A few managed devices running AOS-W 8.3.0.8 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout**. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.8
AOS-147232 AOS-158495 AOS-184142	179942 195511	A client was unable to send or receive traffic to or from an AP. The fix ensures that the AP sends a PAPI message to the UAC and the clients are able to send or receive traffic to or from the AP. This issue occurred when the station management process in an AP sent a PAPI message to the AAC instead of the UAC. This issue was observed in a cluster topology running AOS-W 8.2.1.0 with 802.11r enabled.	AOS-W 8.2.1.0
AOS-147511 AOS-186853	180406	A client received IPv6 router advertisements randomly from different VLANs. The fix ensures that the client receives router advertisement on its derived vlan. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
AOS-147695 AOS-157682	180700 194359	The **profmgr** process in a managed device crashed unexpectedly. This issue occurred when the node name for current working node was renamed using WebUI and a **cd** command was executed. The fix ensures that the **profmgr** process works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-148349 AOS-184288 AOS-187591 AOS-188218	181630	The **OpenFlow** profile was enabled automatically in a managed device immediately after the managed device was upgraded. This issue occured when **OpenFlow** was disabled on the managed device prior to its upgrade. The fix ensures that the **OpenFlow** profile is not automatically enabled after an upgrade. This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-148450 AOS-193798	181773	A few managed devices running AOS-W 8.2.1.0 or later versions rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed devices work as expected.	AOS-W 8.2.1.0
AOS-148529 AOS-191978	181872	A few clients connected to managed devices were unable to access internet. This issue occurred when the client traffic received incorrect Source NAT when IP Nat Inside feature was enabled on interface VLAN that was configured with PBR. This issue was observed in managed devices running AOS-W 8.4.0.4 in a Mobility Master-Managed Device topology.	AOS-W 8.4.0.4
AOS-148642 AOS-156454 AOS-157236 AOS-158502 AOS-158643 AOS-158515 AOS-187647 AOS-190258	195534 192618 193666 195518 195534	The **Postgres** process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. This issue was observed in OAW-4550 switches running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-149092	182612	Clients were unable to resolve ARP requests because the AP memory utilization was high, which led to drop in client traffic. The fix ensures that the clients are able to resolve the ARP requests. This issue was observed in access points running AOS-W 8.3.0.0. **Duplicates** **New IDs** - AOS-147186, AOS-152832, AOS-153857, AOS-155657, AOS-155875, AOS-187974, AOS-157746, AOS-182979, AOS-184932, AOS-186102, AOS-186390, AOS-187381, AOS-188113, AOS-193558, **Old IDs** - 179873, 187691, 189031, 191516, 191814	AOS-W 8.3.0.0
AOS-149433 AOS-154112 AOS-155617 AOS-157342 AOS-158217 AOS-192100	183072 189384 191463 193798 195126	The **datapath** process in a managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. The fix ensures that the managed device processes the FTP traffic and works as expected. This issue occured when a client sent FTP traffic and NAT was applied. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-149543	183200	During upgrade process, the image files were left on the flash drive and the user was unable to upgrade the AOS-W image. The fix ensures that the user is able to upgrade the AOS-W image. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-149841 AOS-152895 AOS-153975 AOS-154406 AOS-154483 AOS-154558 AOS-154973 AOS-155411 AOS-155695 AOS-155710 AOS-156409 AOS-157916 AOS-158259 AOS-183215 AOS-183376 AOS-185652 AOS-186768 AOS-191074 AOS-195052 AOS-195058	183580 187760 189185 189741 189841 189944 190491 191119 191565 191582 192564 194698 195184	A few OAW-AP300 Series access points running AOS-W 8.2.1.1 or later versions crashed and rebooted unexpectedly. The log file listed the reason for this event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.2.1.1
AOS-150245 AOS-188486	184120	A client was redirected to the hostname configured in the captive portal profile and a blank page was displayed in the browser. This issue occurred when the captive portal login page was configured as an FQDN host. This issue is resolved by adding a netdestination entry for the captive portal host. This issue was observed in managed devices running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-150414 AOS-186954	184344	A few APs crashed and rebooted unexpectedly. The log file listed the reason for this event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT**. Enhancements to the wireless driver resolved this issue. This issue occurred because of a bit corruption of the memory. This issue was observed in OAW-AP300 Series, OAW-AP310 Series, and OAW-AP320 Series access points running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1
AOS-150496 AOS-150883 AOS-158128 AOS-188358 AOS-191464	184454 184972 195001	Incorrect SNMPv3 authentication and privacy password were sent to managed devices from the Mobility Master when the managed device running AOS-W 8.2.1.1 or later versions either entered or returned from disaster recover mode. This issue occurred because the **ip ospf message-digest-key** got erased and the SNMPv3 authentication and privacy password were decrypted multiple times. The fix ensures that the SNMPv3 authentication and privacy password does not get decrypted multiple times.	AOS-W 8.2.1.1

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151110 AOS-155015 AOS-180155 AOS-182098 AOS-190683	185286 187984 190542	A radio experienced a high number of resets in APs. Enhancements to the wireless driver resolved this issue. This issue occurred when the APs were in Air Monitor mode. This issue was observed in OAW-AP335 access points running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-151652 AOS-186197	186018	Mobility Master sent a large number of authorization requests to the ClearPass Policy Manager for AirGroup users. This issue occurred as the IPv6 addresses were aging out. The fix ensures that the IPV6 addresses do not age out early. This issue was observed in Mobility Masters running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1
AOS-151855 AOS-187347 AOS-190052	186274	Users were unable to delete an existing management server that was already configured in the Mobility Master running AOS-W 8.2.0.0 or later versions. 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.	AOS-W 8.2.0.0
AOS-152326 AOS-183140 AOS-187297 AOS-187406 AOS-187549	186957	The beacon displayed the country code information intermittently for 5 GHz non-DFS channel when 802.11h was enabled in the radio profile. The fix ensures to broadcast a country code after checking the status of the 802.11h Virtual AP to determine if the country code needs to be broadcasted. This issue was observed in 510 Series access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-152750 AOS-186035	187572	A few managed devices, running AOS-W 8.2.2.0 or later versions, sent OSPF LSA with '00' in LSA checksum field which caused upstream routers to log OSPF errors. With the fix, the managed devices send OSPF LSA with calculated checksum. This issue occurred when the managed devices established OSPF neighbor relationship with routers other than the Alcatel-Lucent routers.	AOS-W 8.2.2.0
AOS-153085	188019	Users were unable to delete the **default-amp** management server profile from both Mobility Masters and managed devices. The issue is resolved by rebooting the managed devices so that the users can delete the management server configuration profile. This issue was observed in managed devices running AOS-W 8.2.1.1 in a Mobility Master-Managed Device topology.	AOS-W 8.2.1.1
AOS-153087	188021	A managed device running AOS-W 8.3.0.0 generated the following console error **|snmp| An internal system error has occurred at file ../unix/aruba_main.c function snmpRequestProcessing line 704 error Cannot send snmp response**. The fix ensures that the managed device works as expected.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-153533 AOS-179571 AOS-181276 AOS-181402 AOS-184537 AOS-190563 AOS-191120	188590 185520 192894 193585	A few APs running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: Rebooting the AP because of FW ASSERT (0x009C5997)**. As a result, incorrect memory corruption was detected during fast recovery process of the APs. Enhancements to the wireless driver resolved this issue.	AOS-W 8.3.0.7
AOS-153618 AOS-156944 AOS-184269 AOS-186423 AOS-185202 AOS-187798 AOS-188970 AOS-190361 AOS-193281	188700 193277	A few APs were unable to join a cluster and rebooted with the **unable to contact switch: HELLO-TIMEOUT** error message. The fix ensures that the APs are able to join the cluster. This issue occurred when the cluster leader received a Deactivate event from DDS of a different managed device that was a previous leader. This issue was observed in managed devices running AOS-W 8.3.0.6.	AOS-W 8.3.0.6
AOS-153876 AOS-155448 AOS-186866	184901	The **Licensing** tab under **Configuration** > **System** page of the WebUI displayed incorrect count of license usage. The fix ensures that the correct license count is displayed. This issue was observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-153842 AOS-185358	189015	Some APs were unable to connect to the 2.5 GHz or the 5 GHz radio. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP320 Series access points running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-153938	189134	Some APs did not handle VLAN tagged packets. The fix ensures that the APs work as expected. This issue occurred when the VLAN packets were forwarded to uplink switches without processing and were interpreted as negative packets by the uplink switches. This issue was observed in OAW-AP303H access points running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-154191	189490	Some APs running AOS-W 8.3.0.0 sent AMON messages such as CL_HT_MODE with incorrect values displaying 0, 9, and 255. This issue occurred because SAPM did not provide radio profiles for Mesh. The fix ensures that the SAPM process provides radio profiles for mesh APs.	AOS-W 8.3.0.0
AOS-154735 AOS-187277	190181	An AP crashed and rebooted unexpectedly. The log files listed the reason for this event as **kernel panic: softlockup: hung tasks**. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP203H access points running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-154809	190272	PPPoE stopped working on a OAW-RAP running AOS-W 8.2.1.1. The fix ensures that PPPoE works as expected on the OAW-RAP. This issue occurred while provisioning a OAW-RAP using ZTP.	AOS-W 8.2.1.1
AOS-154908 AOS-185189 AOS-187222 AOS-187252 AOS-187519 AOS-188153	190396	The console logs of an AP showed the standby IP address as 0.0.0.0. During a failover, the AP lost connectivity with the standby managed device and it did not come up. The fix ensures that the AP failover occurs when the standby managed device is up and the AP obtains the correct IP address of the standby managed device. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AOS-W 8.3.0.1
AOS-154994 AOS-183903	190518	When the client device set an authentication frame after it was already authenticated, its association status was cleared but an incorrect error message- **Requested authentication algorithm not supported** was displayed. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-155081 AOS-188336	190642	Post configuration changes, if Iterator was not reset after handling auth servers list in gdata, values of **show configuration committed** and **show configuration effective** commands were different. This issue is resolved by resetting the iterator to zero after processing auth server list in gdata. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-155114	190678	A user role under an ACL did not work as any other session ACL. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.2.1.0.	AOS-W 8.2.1.0
AOS-155127 AOS-185571 AOS-186648	190702	Some users were unable to access the login page during captive portal authentication on the managed devices running AOS-W 8.3.0.0 or later versions in a cluster setup. The fix ensures that the captive portal authentication login page is displayed. This issue occurred when AP datapath sent HTTP requests to the AAC instead of the UAC in Split-Tunnel forwarding mode.	AOS-W 8.3.0.0
AOS-155232 AOS-158451 AOS-186843 AOS-187407	190863 195457	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Take care of the HOST ASSERT first**. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP315 access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-155267	190912	The **show datapath bridge ap-name** command and **show ap mesh debug forwarding-table ap-name** command were running in to an infinite loop and displayed **Warning: Not enough memory to complete this operation** error message. The fix ensures that the managed devices work as expected. This issue occurred when the AP was configured as OAW-RAP with PPPoE enabled. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-155632 AOS-157337 AOS-157417 AOS-158610	191489 193793 193945 195645	Mobility Masterr crashed and rebooted unexpectedly. The log file listed the reason for the event as **Control Processor Kernel Panic** This issue occurred when IP options caused the Datapath process to crash . Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-4x50 Seriesswitchesrunning AOS-W 8.2.0.0 or later versions. **Duplicates:** AOS-184786, AOS-186151, AOS-187156, AOS-187576, AOS-187752, AOS-187880, AOS-189198, AOS-189439, AOS-191458, AOS-191603, AOS-192748, AOS-193261, AOS-193272, AOS-193491, AOS-193997.	AOS-W 8.2.0.0
AOS-155667 AOS-182789 AOS-185224 AOS-186048 AOS-186473 AOS-188296 AOS-190743 AOS-191883 AOS-191900	191528	A few OAW-RAPs 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 OAW-RAPs work as expected.	AOS-W 8.3.0.0
AOS-155715 AOS-194512	191588	A mismatch of quiet period was observed between OAW-AP335 and OAW-AP345 access points running AOS-W 8.3.0.7 in a Mobility Master-Managed Device topology. Enhancements to the wireless driver resolved this issue.	AOS-W 8.3.0.7
AOS-155780	191686	A VIA client did not connect to a VIA server. The fix ensures that the VIA client is able to connect to the VIA server. This issue occurred when the VIA client was connected wirelessly to the same managed device on which the VIA VPN terminated. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-155801	191726	SNMP walk performed from AirWave did not produce correct results. The fix ensures that the SNMP walk produces the correct result. This issue was observed in managed devices running AOS-W 8.3.0.3.	AOS-W 8.3.0.3.
AOS-155976	191945	Users were unable to provision an AP using the CLI command, **provision-ap** and an error message, Internal error was displayed. This issue occurred when an IPv6 interface did not exist between the Mobility Master and managed devices but one existed between the managed devices and the APs. The fix ensures that the users are able to provision an AP. This issue was observed in managed devices running AOS-W 8.3.0.3 or later versions.	AOS-W 8.3.0.3

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-156080 AOS-182758 AOS-190590 AOS-191121 AOS-191286 AOS-193632 AOS-193733	192112	A managed device showed Skype error messages in the HTTPD logs and dropped XML messages that were meant for UCM. The visibility of Skype for Business call records were missing from the WebUI. The fix ensures that the managed device works as expected and does not drop the XML messages that are meant for UCM. This issue was observed in managed devices running AOS-W 8.2.2.2.	AOS-W 8.2.2.2
AOS-156104 AOS-156587 AOS-178581 AOS-180782 AOS-186801	192143 192814 180455 191142	OAW-AP207 access points running AOS-W 8.2.2.0 or later versions rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.2.2.0
AOS-156223	192294	The BSSID of few APs were wrongly classified after configuration of IDS AP classification rule profile on OAW-4650 switches running AOS-W 8.3.0.0 or later versions. The fix ensures that the APs are properly classified with the active IDS AP classification rule configuration.	AOS-W 8.3.0.0
AOS-156244 AOS-187898	192323	Managed devices sent syslog packets with invalid facility levels. This issue is resolved by implementing a local logging facility. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-156610 AOS-157949 AOS-187850 AOS-188197	192852 194755	A Mobility Master running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **mcellsolverstart process error**. The fix ensures that the Mobility Master does not crash when the database contains invalid timezone string but logs the error message. This issue occurred because of an invalid timezone string.	AOS-W 8.3.0.0
AOS-156727 AOS-156728 AOS-156834 AOS-158306 AOS-189954 AOS-191486	193015 193016 193152 195249	The **Cluster manager** process crashed in a managed device unexpectedly. The log files listed the reason for this event as **Module Cluster Manager Process is busy. Please try later**. The fix ensures that the managed device works as expected. This issue occurred because the **lc-cluster exclude-vlan** string had more than 256 characters, that led to memory corruption. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions in a cluster setup.	AOS-W 8.2.2.0
AOS-156838 AOS-186859	193158	A few users were unable to reprovision an AP. This issue is resolved by keeping the original characters and not converting them to a different format. This issue occurred when a special character in a German keypad was used in the AP name. This issue was observed in APs connected to managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.2.1

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-156840 AOS-157049	193160 193416	The CLI Command, **halt** did not work on theMobility Master. This issue occurred as the init process was killed when the halt command was executed. The fix ensures that the command works as expected. This issue was observed in Mobility Master running AOS-W 8.3.0.4 or later versions.	AOS-W 8.3.0.4
AOS-156854 AOS-183152 AOS-186773 AOS-186847	188356	Clients reconnected to the AP frequently as the effective rates and advertised rates were not the same. Enhancements to the wireless driver resolved this issue. This issue was observed in 510 Series access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-157005 AOS-185233 AOS-185351 AOS-186096 AOS-186796	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. Enhancements to the wireless driver resolved this issue. This issue was observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-157008	193558	The output of the **show ap bss table** command displayed incorrect MTU value for a OAW-RAP as the AP MTU report packet was single encrypted. The fix ensures that the MTU report packet is not dropped by the managed device and the output of the **show ap bss table** command displays the correct MTU value. This issue occurred when the default value of the **rap-gremtu** parameter was changed to a new value using the **ap systemprofile <profile_name>** command. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-157011	193362	The output of **Show datapath papi counters** command displayed invalid tunnel endpoint information. The fix ensures that the **Show datapath papi counters** command displays the correct information. This issue was observed in Mobility Master running AOS-W 8.3.0.3.	AOS-W 8.3.0.3
AOS-157144	193538	The **Station Management** process crashed continuously in a stand-alone switch running AOS-W 8.4.0.0 or later versions. The fix ensures that the switch works as expected. This issue occurred when a stand-alone switch running any AOS-W 8.x version was converted to managed node using the **write erase** command, and then the switch was upgraded to AOS-W 8.4.0.0 version and rebooted in the managed node. After that, the switch was again converted to stand-alone mode using **write erase** command.	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-157162 AOS-184508 AOS-187102	193561	An AP was unable to form a UAC tunnel with a managed device after a failover. The log file listed the following reasons for the issue as: Dynamic BSS tunnel could not be setup Denied; AP not found in STM The fix ensures that the AP forms UAC tunnel with the managed device. This issue occurred when the AP channel updates were not registered with the STM process. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-157492	194064	VRRP authentication failed in a managed device. The fix ensures successful authentication. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
AOS-157767 AOS-155877 AOS-184056 AOS-187322	191816	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20)**. The fix ensures that the managed device works as expected. This issue was observed in OAW-40xx Series and OAW-4x50 Seriesswitches running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-157823 AOS-185568	194561	A few 802.1X clients were displayed with an IP address instead of a user name in the **Managed Network > Dashboard > Overview > Clients** page of the WebUI. The fix ensures that the WebUI displays correct information about the 802.1X clients. This issue was observed in stand-alone switches running AOS-W 8.3.0.3 or later versions.	AOS-W 8.3.0.3
AOS-157979	194788	A memory leak was found in both **arci-cli-helper** and **STM** processes as a result of using a script to query the controller Monitoring Dashboard. The fix ensures that there is no memory leak. This issue occurred when certain Monitoring Dashboard queries were run either using a script or the WebUI, where memory relating to the query **filter** strings were not freed. This issue was observed in controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-158180 AOS-158565	195080 195592	The licenses within the AP licensing pool were consumed every time the mesh point was rebooted or was disconnected from its parent. The fix ensures that the license count does not get exhausted. This issue was observed in APs in mesh portal and mesh point mode running AOS-W 8.2.0.0 or later versions. **Duplicates**: AOS-182719, AOS-183629, AOS-184955, AOS-185312, AOS-185342, AOS-185428, AOS-187858.	AOS-W 8.2.0.0
AOS-158506 AOS-185418	195522	Some managed devices did not renew wired clients after idle-timeout. The fix ensures that the wired clients remain connected to the managed devices. This issue occurred when the DHCP packets were not treated as traffic, removing the wired clients from the user tables. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-158618	195656	The status of the AP is displayed as **DOWN** in the WebUI but displayed as UP when the **show ap database** command was executed. The fix ensures that the status of the AP is displayed correctly in the WebUI and CLI. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions. **Duplicates:** **New IDs:** AOS-146683, AOS-158210, AOS-150880, AOS-147450, AOS-129107, AOS-147384, AOS-147743, AOS-147347. **Old IDs:** 179056, 180149, 180324, 180214, 180774, 184967, 195656, 195117, 156245.	AOS-W 8.2.0.0
AOS-158646 AOS-188596 AOS-189023 AOS-191439 AOS-193368 AOS-195912	195687	The **datapath** process crashed multiple times in a OAW-4750XM switch running AOS-W 8.4.0.3 or later versions. The log file listed the reason for the event as **Datapath Timeout**. The fix ensures that the switch works as expected. This issue occurred because of a null pointer access.	AOS-W 8.4.0.3
AOS-158656	195704	The password in the **Active** configuration was displayed in clear text in the log files when the **show log all | include phonehome** command was executed. The fix ensures that the active password is not displayed when the command is executed. This issue was observed in Mobility Master running AOS-W 8.3.0.6.	AOS-W 8.3.0.6
AOS-181708	194675	The output of the **show ap allowed-channels country-code DE** command displayed restricted WLAN channel range of 149-165 in the allowed list of channels of OAW-AP325 access points running AOS-W 8.3.0.3 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.3.0.3
AOS-181925	195713	The **Dashboard > Access Points** page of the Mobility Master WebUI did not display updated information of an AP that is displayed as UP on the managed device. The fix ensures that the correct information of the AP is displayed on the Mobility Master WebUI. This issue was observed in Mobility Masters running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1
AOS-182294	—	When the **show ip route** command was executed, IPsec route table displayed IP route entries although the IPsec map configuration was disabled. The fix ensures that the stand-alone controller works as expected. This issue occurred after the stand-alone controller was rebooted. This issue was observed in stand-alone controllers running AOS-W 8.2.2.3 or later versions.	AOS-W 8.2.2.3
AOS-182652 AOS-188650	—	A managed device crashed and rebooted unexpectedly. The log files listed the reason for this event as **sos_stats_type_tnl_stats_global_display**. The fix ensures that the managed device works as expected. This issue occurred while trying to bring up APs and clients on the managed device. This issue was observed in OAW-4850 switches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-182970 AOS-185867	—	The output of the **backup flash** command from an SSH session displayed the **Please wait while we take the flash backup...Error backing up DBs** error message. The fix ensures that this error message is not displayed. This issue was observed in OAW-4104 switches running AOS-W 8.5.0.0	AOS-W 8.5.0.0
AOS-183123	—	The **%** symbol was not displayed for **cluster client threshold values** in **Configuration > System > Profiles > Cluster** page of the WebUI. This issue was observed in managed devices running AOS-W 8.5.0.0 in a cluster setup.	AOS-W 8.5.0.0
AOS-183148 AOS-183454 AOS-183782 AOS-184700 AOS-185163 AOS-186657 AOS-187148 AOS-191694	—	A few APs running AOS-W 8.0.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot reason: fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.0.0.0
AOS-183244 AOS-185673	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **FW assert at tbd.c:39**. The fix ensures that the AP works as expected. This issue occurred while enabling or disabling 802.11k profile. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-183549 AOS-184354 AOS-189719 AOS-194323	—	Managed devices, running AOS-W 8.3.0.0 in a cluster setup, crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.0
AOS-183508 AOS-186447	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Warm reset**. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP345 access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.6
AOS-183626	—	The CLI allowed configurations on the managed device when the **configuration-purge-pending-config** command was executed, even though previously entered commands were not committed. The fix ensures that the command works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-183669 AOS-190457 AOS-192089 AOS-194012 AOS-193792	—	The system LED blinked with a green light after a OAW-RAP connected to the managed device and booted up. The fix ensures that the system LED blinks with red light when the OAW-RAP boots up. This issue was observed in OAW-RAPs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.4.0.0
AOS-183723 AOS-187678	—	The SSL handshake for POST failed for clients performing captive portal authentication on a managed device. This issue occurred when TLS 1.2 was enabled in Web Server profile within the SSL protocol. The fix ensures that the managed device works as expected .This issue was observed in managed devices running AOS-W 8.2.0.0-FIPS or later versions in a Mobility Master- Managed Device topology.	AOS-W 8.2.0.0
AOS-183740	—	A few clients were unable to connect to APs intermittently. The fix ensures that the clients are able to connect to the APs seamlessly. This issue occurred because the GRE rule was incorrectly updated with a non-gateway MAC address. This issue was observed in APs running AOS-W 8.3.0.4.	AOS-W 8.3.0.4
AOS-183883 AOS-183989 AOS-193747	—	A few APs were marked as **Down** and were inactive. The fix ensures that the managed devices accept the messages from the APs and the APs are able to connect to the managed devices seamlessly. This issue occurred because the managed devices running AOS-W 8.3.0.0 or later versions dropped AP-READY message from APs.	AOS-W 8.3.0.0
AOS-183887 AOS-186573	—	The user-table entries got deleted when a client roamed between APs. The fix ensures that the entries do not get deleted. This issue occurred when a client was associated with captive portal SSID. This issue was observed in APs running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.2.4
AOS-183962 AOS-184518 AOS-187753	—	IKE Overlay routes for client traffic were missing from the VPN Concentrator and the managed device. Hence, the managed device got disconnected from the Mobility Master. The fix ensures that the IKE Overlay routes are available and the connection is restored between the managed device and the Mobility Master. This issue was observed in OAW-4650 and OAW-4008 managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-183998 AOS-183999	—	A few users were unable to configure the PPPoE password while provisioning a OAW-RAP in the **Configuration > Access Points > Remote APs** page in the WebUI. This issue occurred because the **Retype password** field for PPPoE was missing from the Uplink option in the provisioning page in the WebUI. The fix ensures that the user is able to configure the PPPoE password while provisioning a OAW-RAP. This issue was observed in OAW-RAPs running AOS-W 8.3.0.6.	AOS-W 8.3.0.6

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-184051	—	Mobility Master sent NTP sync packets every 15 seconds to the NTP server. This issue occurred due to upstream reachability that triggered sync packets from the Mobility Master. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Master running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-184135	—	A few users were unable to download applications from Google Play Store. This issue occurred when the YouTube application is blocked. The fix ensures that the users are able to download the applications from Google Play Store.This issue was observed in stand-alone controllers running AOS-W 8.4.0.0.	AOS-W 8.4.0.0
AOS-184265 AOS-184964 AOS-187616	—	A Mobility Master displayed **Name-server already exists** error message when more than one DNS server was added under **Configuration > System > General > Domain Name System** tab in the WebUI. The fix ensures that this error message is not displayed and more than one DNS servers can be added. This issue occurred due to an error in API response for **ipv6_domain_lookup**. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-184289	—	SNMP traps or syslog error messages were not generated when the VLAN probe failed on the managed devices running AOS-W 8.2.2.0 or later versions in a cluster setup. The fix ensures that syslog messages are generated as expected.	AOS-W 8.2.2.0
AOS-184302 AOS-186325 AOS-185500 AOS-188413 AOS-188648 AOS-189366 AOS-192566	—	Multiple **sapd** processes crashed on a managed device running AOS-W 8.3.0.6 or later versions. Enhancements to the wireless driver resolved this issue.	AOS-W 8.3.0.6
AOS-184365 AOS-188342	—	A managed device brought up in a full-setup mode got stuck during the boot up process and displayed the **Waiting for IP** error message. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2
AOS-184441	—	The output of the **show boot history** command displayed incorrect user information in the **Reboot Cause** message. However, the correct information was logged in the **Controller Reboot initiated** message before the reload. The fix ensures that the **Reboot Cause** message displays the appropriate information. This issue occurred because the managed device incorrectly used the current user information who had logged in and executed the **show boot history** command for the **Reboot Cause** message. This issue was not limited to any specific switch model or AOS-W version.	AOS-W 8.3.0.4

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-184474 AOS-186793 AOS-186872 AOS-186971 AOS-189390 AOS-190362 AOS-192337 AOS-194239 AOS-194677 AOS-195037	—	An AP 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. This issue was observed in OAW-AP300 Series access points running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-184519	—	A user was 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-184545 AOS-186523 AOS-187213	—	A few OAW-AP303H access points running AOS-W 8.2.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: softlockup: hung tasks**. Reducing the batch size to 64 resolved this issue. This issue occurred when the APs processed large batch files that led to lock stall detection.	AOS-W 8.2.0.0
AOS-184701	—	The active-standby IP field on the Mobility Master dashboard displayed incorrect number of clients. This issue occured due to a cluster failover causing race condition. The fix ensures that the number of clients are displayed correctly. This issue was observed in Mobility Masters running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-184705 AOS-186108	—	Some clients were unable to send and receive data traffic. The fix ensures that the clients send and receive data traffic. This issue occurred when the client experienced inter-band roaming in both bridge and decrypt-tunnel forward modes. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-184707 AOS-185647	—	A few OAW-RAPs running AOS-W 8.2.1.0 or later versions failed to come up on the managed device after reboot of the APs, and received the same inner IP which had already been assigned to other OAW-RAPs. The fix ensures that the OAW-RAPs boot up successfully with new inner IP addresses. This issue occurred because most of the OAW-RAP whitelist database entries were removed from the Mobility Master.	AOS-W 8.2.1.0
AOS-184787 AOS-185944 AOS-185948	—	The **authentication** process crashed in a stand-alone switch due to memory corruption. The fix ensures that the switch works as expected. This issue was observed in OAW-4750 and OAW-4750XM switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-184851 AOS-187529 AOS-190376	—	The **login-fcgi** process crashed unexpectedly in OAW-4850 switches running AOS-W 8.4.0.0 or later versions. This issue is resolved by increasing the array size to 128K for processing request parameters. This issue occurred when HTTP requests larger than 8k were processed that led to a segmentation fault.	AOS-W 8.4.0.0
AOS-184870	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **AP process crash (core file: panic-dump.ME203-19AP1167.2019-03-11_00-51-53)**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-184912	—	The output of the **show ap arm client-match summary advanced** command did not display the success percentage for its parameters. The fix ensures that the success percentage details are displayed for its parameters. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-184947 AOS-192737	—	The jitter and health score data was missing from the **Dashboard > Infrastructure > Uplink > Health** page in the WebUI of a Mobility Master running AOS-W 8.4.0.4. The fix ensures that the jitter and health score details are available in the WebUI.	AOS-W 8.4.0.4
AOS-184957	194208	User-derivation rules were missing in the CLI but the same was available in the WebUI. This issue occurred when the switch was migrated from a 6.x to 8.x topology. The fix ensures that the user-derivation rules are present in the Command Line Interface. This issue was observed in Mobility Master running AOS-W 8.3.0.0 or later versions	AOS-W 8.3.0.0
AOS-189696	—	The **isakmp** process crashed on a managed device when RAP whitelist-db entries were added from the Mobility Master. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.0 in a cluster setup.	AOS-W 8.5.0.0
AOS-185089	—	Unable to setup an IPsec tunnel because Mobility Masters were using port 500 instead of port 4500 to form L3 redundancy. The fix ensures that the IKE connection initiates on port, 4500. This issue occurred as IKE started negotiating on port 500. This issue was observed in Mobility Masters running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-185184	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Kernel panic; BUG: soft lockup - CPU#0 stuck**. Enhancements to the wireless driver resolved this issue. This issue was observed in 530 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185197 AOS-188490 AOS-189847	—	Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20).** The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Master running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-185259 AOS-186237 AOS-188214	—	All Radios displayed poor channel quality in **Dashboard > Overview > Radios > CHANNEL QUALITY** page in the WebUI. The fix ensures that the correct channel quality is displayed. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185327	—	The **show ap debug radio stats** command displayed incorrect values of **Rx Time** percentage. The fix ensures that the command displays the correct values. This issue was observed in Mobility Master running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185597	—	An AP crashed and rebooted unexpectedly. The log files listed the reason for this event as **WLAN FW exception at wal_ba_tx_sm()**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP555 and 530 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185822	—	A few APs were beaconing without any connected clients, and displaying **wl1: PHYTX error and plcp 057c 0000 || 01cb 0000 0000 || 0000 0000 || 00** error messages. The fix ensures that the AP works as expected. This issue was observed in 510 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185894	—	A few APs set the TID of downlink multicast traffic to 0. Enhancements to the wireless driver resolved this issue. This issue occurred when the AP was operating in tunnel mode. This issue was observed in OAW-AP555 access points running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-186095	—	A few APs lost association and reconnected back immediately. Enhancements to the wireless resolved this issue. This issue occurred due to a beacon drift. This issue was observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185602 AOS-187149 AOS-188372 AOS-189992 AOS-191622 AOS-192188	—	A few APs consumed more licenses than the actual number of APs that were up on the network because S-AAC (standby) mesh AP consumed Active AP licenses. This issue occurred when virtual AP was enabled in the mesh point connected to the mesh portal in a cluster setup. The fix ensures that the standby mesh APs do not consume Active APs' licenses. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185696	—	A few APs stopped responding to data frames and could not decode BA packets from the STAs causing packet drop. Enhancements to the wireless driver resolved this issue. This issue was observed in 530 Series Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185833 AOS-186094	—	A few APs crashed unexpectedly. The log file listed the reason for this event as **ar_wal_vdev.c:2528 Assertion;Thread ID : 0x0000005e;PC : 0x4b0c9de8**. Enhancements to the wireless driver resolved the issue. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-185920 AOS-185921	—	A managed device rebooted unexpectedly. The log file listed the reason for this event as **Nanny Rebooted Machine – fpapps process died and crashed on pubsub, cfgm, syslogdwrap, aaa and nanny module**. The fix ensures that the managed device works as expected. This issue occurred due to a memory leak. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-185932	—	A few clients deleted block acknowledge agreement leading to ping timeouts. Enhancements to the wireless driver resolved this issue. This issue occurred randomly when clients were still connected. On re-negotiation, the traffic resumed normally. This issue was observed in 550 Series access points running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-185937	—	An AP crashed and rebooted unexpectedly. The log files listed the reason for this event as **whal_recv_ recovery.c:606 Assertion RX_ HW_WDOG_HANG failedparam0 :zero, param1 :zero, param2 :zero**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP555 and 530 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-185977 AOS-190735	—	Heartbeats were missed randomly in a cluster setup. The fix ensures that the managed devices works as expected. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-186009 AOS-189072	—	The AP database displayed **F** flag after successful 802.1x authentication. The fix ensures that the AP works as expected. This issue was observed in OAW-AP303H access points running AOS-W 8.3.0.3 or later versions.	AOS-W 8.3.0.3
AOS-186052	—	A few APs witnessed TX mute when a radio reset burst occurred. The fix ensures that the AP works as expected. This issue occurred due to a reset in the G radio that was triggered due to an interference in the AP's operating channel. This issue was observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-186076 AOS-187464 AOS-187884 AOS-189850 AOS-191866 AOS-192125 AOS-192310 AOS-193177 AOS-193387 AOS-193581 AOS-194218 AOS-194312 AOS-194434	—	The STM process in a managed device that is part of a cluster setup crashed unexpectedly. This issue occured when the memory that was allocated for some clients was not released after these clients disconnected from their UAC in a cluster. The fix ensures that the STM process does not crash. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.2

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-186111	—	The price update of ESLs failed unexpectedly. This issue is resolved by optimizing the **COEX** method between WiFi radio and ESL radio. This issue occurred when the SES-imagotag's Electronic Shelf Label (ESL) system stopped responding after running for a long time. This issue was observed in OAW-AP300 Series, OAW-AP303H Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP340 Series, and 510 Series access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-186113	—	A few mesh wired APs did not work as expected when the DHCP packet had a VLAN tag. The fix ensures that the mesh wired APs work in bridge trunk mode. This issue was observed in APs running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-186133	—	A few managed devices displayed abnormally high multicast traffic in **Performance Summary > All Radios** monitoring page. The fix ensures that the managed device works as expected. This issue was observed in OAW-AP320 Series access points running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-186144	—	A managed devices is unable to enable Tunnel Keepalive automatically, even after configuring Tunnel Heartbeat Interval & Tunnel Heartbeat Retries. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.0 in a master-local topology.	AOS-W 8.5.0.0
AOS-186146	—	A few APs were acknowledging upstream frames though the radio was turned off. Enhancements to the wireless driver resolved this issue. This issue was observed in 530 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-186184	—	The **Configuration > Access Points** page in the WebUI did not display the SNMP System Location. The fix ensures that SNMP System Location is displayed in the WebUI. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-186207	—	The **Unexpected HCM runtime error at hcm_gsm_update_section_ip_probe 167 Failed to update section for probe IP 10.120.128.1 src_intf 0 probe default, error error_htbl_key_not_found** error message was displayed in the log file of a Mobility Master running AOS-W 8.4.0.1 or later versions. The fix ensures that the Mobility Master works as expected.	AOS-W 8.4.0.1
AOS-186233 AOS-186360 AOS-191178	—	The **Authentication** module in managed devices running AOS-W 8.4.0.0 or later versions in a Mobility Master-Managed Device topology crashed unexpectedly. The fix ensures that the managed device works as expected.	AOS-W 8.4.0.0
AOS-186303 AOS-187388 AOS-188301	—	A few OAW-RAPs rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: Fatal exception on PC is at netdev_run_todo+0x290/0x2b4**. The fix ensures that OAW-RAPs work as expected. This issue was observed in OAW-AP305 access points running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-186304 AOS-190135	—	Users were unable to connect to the OAW-RAP over IPv6 network in a managed device because the AP was waiting to receive AP regulatory domain information from the managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.6.	AOS-W 8.3.0.6
AOS-186379	—	IPv4 session table output was missing in tech support logs. The fix ensures that the IPv4 session table outputs are available in the tech support log. This issue as observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-186386 AOS-186556	—	A few clients failed to obtain the IPv6 address from the external DHCPv6 servers when the **bc-mc optimization** parameter was enabled using the **interface vlan <vlan>** command. 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-186388	—	A few clients were unable to connect to 5 GHz channel of OAW-AP325 access points running AOS-W 8.3.0.0 or later versions. The fix ensures that the clients are able to connect to the APs. This issue occurred during high availability deployment of APs.	AOS-W 8.3.0.0
AOS-186526	—	The **profmgr** process in a Mobility Master crashed unexpectedly. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.4.0.0.	AOS-W 8.4.0.0
AOS-186558	—	A few clients were unable to connect after reboot of the OAW-4550 switch running AOS-W 8.2.0.0 or later versions. The fix ensures that the clients are able to connect to the stand-alone switch. This issue occurred because the GRE tunnel was not established after reboot of the stand-alone switch. .	AOS-W 8.2.0.0
AOS-186796 AOS-186921	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. Enhancements to the wireless driver resolved this issue. This issue was observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-186774	—	When the show memory cfgm command was executed, a large memory allocation was displayed in the output. The fix ensures that there is no memory leak. This issue was observed in managed devices running AOS-W 8.3.0.6.	AOS-W 8.3.0.6
AOS-186860	—	RADIUS authentication requests were sent in the IP address of the managed device running AOS-W 8.4.0.1, although they were configured to go through the loopback IP. The fix ensures that the RADIUS authentication requests were sent through the loopback IP.	AOS-W 8.4.0.1

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-186884	—	The POE status of an AP was displayed as **POE AF** even though 25.5 W of power was allocated to the AP through LLDP. This issue is resolved by changing the output of the **show ap debug system-status ap-name** command and associating the power supply status with the overall AP power status. The overall AP power status is derived from the results of the physical layer classification and the data link classification. For APs that have a single Ethernet port, a line with title **HW POE Status** is added. This issue was observed in APs running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-186953 AOS-188141 AOS-188641	—	A few clients faced connectivity issues when they did not receive DHCP packets in an Open SSID or EAPOL packets in 802.1X SSID. The fix ensures that the clients are able to connect to the network. This issue occurred due to a mismatch between tunnel IDs and virtual AP interface within the AP datapath. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.0 or later versions in a cluster setup.	AOS-W 8.5.0.0
AOS-186969	—	The **Acct-Authentic radius** attribute was not sent from the managed device when the managed device was upgraded to AOS-W 8.4.0.2. The fix ensures that the managed device works as expected.	AOS-W 8.4.0.2
AOS-186979	—	A few APs running AOS-W 8.3.0.6 or later versions were unable to reboot automatically after an uplink or WAN link status change. The fix ensures that the APs work as expected.	AOS-W 8.3.0.6
AOS-186985	—	A large number of **warning: ClientCursor::yield can't unlock b/c of recursive lock ns: site1.pathloss_history** error messages were displayed in the log files of mongo database on the Mobility Master. The fix ensures that the error messages do not appear in the log files. This issue occurred when the Mobility Master created corrupt dump file of the AirMatch database. This issue was observed in Mobility Masters running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-187036	—	A few APs running AOS-W 8.3.0.0 or later versions were stuck in an upgrade state and were unable to boot up. The fix ensures that the APs work as expected. This issue occured due to AP image mismatch detected by the managed devices.	AOS-W 8.3.0.0
AOS-187041	—	A FIPS-enabled ClearPass Policy Manager server failed to establish an SSH session with the Mobility Master. This issue is resolved by adding support for Diffie-Hellman-Group14-SHA256 in Mobility Masters. This issue occurred when a Mobility Master offered only Diffie-Hellman-Group14-SHA1 keys instead of Diffie-Hellman- Group14-SHA256 keys. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions in both FIPS and non- FIPS mode.	AOS-W 8.2.0.0
AOS-187044	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Critical process /aruba/bin/rapper [pid1336] DIED, process marked as RESTART**. The fix ensures that the AP works as expected. This issue was observed in OAW-AP365 access points running AOS-W 8.3.0.3 or later versions.	AOS-W 8.3.0.3

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-187086	—	Traffic from wired phones were unable to reach the call server via uplink VLAN 4092. The fix ensures that the managed device egresses the traffic from the wired phones. This issue occurred when lower priority uplink was used as higher priority next-hop. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-187087	—	A few APs rebooted frequently. The log files listed the reason for this event as **BUGFailureAt:net/core/skbuff.c:1609/consume_skb()! Warmreset**. Enhancements to the wireless driver resolved this issue. This issue occurred when the APs were in AM mode. This issue was observed in 510 Series access points running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-187113 AOS-187451	—	A few APs were using 40MHz channels on 2.4 GHz instead of 20 MHz. The fix ensures that the channel is switched back to 20 Mhz. This issue occurred because in 2.4 GHz, the channels are always scanned in 40 MHz but if the scan channel and home channel share the same control channel, channel is switched back to the configured channel after scan. This issue was observed in 510 Series access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-187114	—	The **Pending Changes** page displayed additional changes when the user configured a new policy rule under **Configuration > Roles & Policies > Policies** page in the WebUI. The fix ensures that unnecessary changes are not displayed in the **Pending Changes** page in the WebUI. This issue was observed when the user configured a new rule for an existing policy under the **Policies** page and clicked the **Submit** button. This issue was observed in Mobility Masters running AOS-W 8.3.0.4.	AOS-W 8.3.0.4
AOS-187115 AOS-190146	—	The application name in the policy configuration was incorrect in the **Configuration > Roles & Policies > Policies > <Policy name>** page in the WebUI. The fix ensures that the correct application name is displayed in the WebUI. This issue occurred when the WebUI was accessed for the first time. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-187171	—	A few split tunnel clients got disconnected frequently. The log files listed the reason for the event as **Denied; Ageout**. The fix ensures that the clients do not get disconnected. 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-187328	—	A configuration failure error occurred on managed devices when a deprecated SNMP trap was pushed from the Mobility Master to the managed devices. However, the SNMP trap was not part of the **show snmp trap-list** command and the SNMP process validation failed but the **profile manager** process did not perform the validation. This issue is resolved by adding a validation check for SNMP names in the **profile manager** process. This issue was observed in managed devices and stand-alone switches running AOS-W 8.2.2.3.	AOS-W 8.2.2.3

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-187331 AOS-188142 AOS-188540 AOS-189356	—	An AP was unable to detect the nearby AP list. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP515 access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-187337	—	The WebUI allowed user to access pages which were inaccessible to administrators. This issue is resolved by providing access only to the authorized pages and removing access privileges to unauthorized pages. This issue was observed in managed device running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-187341	—	The panic list file command listed operating system files. This issue is resolved by removing the obsolete panic command from the CLI. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-187356	—	An AP randomly stopped transmitting 5 GHz beacons and affected the network. The fix ensures that the AP works as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-187361 AOS-188746 AOS-190163	—	The **LMS preemption** process failed when NAT was applied to the primary LMS IP address in APs. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.0
AOS-187422 AOS-189258	—	The output of **show log all** and **show audit-trail** commands displayed the unencrypted password entered for non-profile commands such as **aaa test-server** command. The fix ensures that the passwords are displayed in asterisks as intended. This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.3.0.5.	AOS-W 8.3.0.5
AOS-187479 AOS-188428	—	The authentication server configuration details were not forwarded from the primary Mobility Master to the secondary Mobility Master in Layer-3 redundancy configuration. The fix ensures that the authentication server configuration details are forwarded correctly. This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-187510	—	A managed device running AOS-W 8.4.0.2 or later versions crashed and rebooted because the 802.1X processes crashed after a cluster live upgrade on the managed device. The fix ensures that the managed device works as expected.	AOS-W 8.4.0.2
AOS-187568	—	After an upgrade, the clients were unable to get an IP address as the session ACL for authenticated role was missing from the managed device running AOS-W 8.4.0.0 or later versions. The fix ensures that the clients are able to get an IP address.	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-187692	—	OAW-RAP3WN and OAW-AP135 running AOS-W 8.3.0.0, provisioned as a OAW-RAP crashed frequently with an **Out of memory** error. This issue occurred because a large number of http requests were sent the APs. This issue is resolved by limiting the number of requests sent to the AP.	AOS-W 8.3.0.0
AOS-187726	—	The output of the **show ap debug radio-stats** command displayed incorrect Rx frames counter. The fix ensures that the correct number of Rx frames are displayed in the command output. This issue was observed in OAW-AP325 access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-187750	—	A few APs were unable to discover the nearby AP list. This issue is resolved by increasing the dwell time of the DFS channels to 60 ms. This issue occurred because the dwell time of the DFS channels were set to 20 ms. This issue was observed in 510 Series access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-187834	—	APs were not sending Port VLAN IDs in an LLDP packet although the **native-vlan-id** parameter is set using **ap system-profile** command. The fix ensures that the APs send a Port VLAN ID with a value other than 0. This issue was observed in access points running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.4
AOS-187906	—	The AP image mismatch logs were classified as debugging logs instead of error logs. The fix ensures that the AP works as expected. This issue was observed in APs running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-188008	—	Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event listed as **kernel panic: Intent:cause:register 12:86:e0:2**. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions. **Duplicates** **New IDs:** AOS-150036, AOS-104286, AOS-126139, AOS-131894, AOS-137958, AOS-139171, AOS-139271, AOS-139328, AOS-139499, AOS-139557, AOS-139982, AOS-140021, AOS-140167, AOS-140370, AOS-140533, AOS-140534, AOS-140804, AOS-141875, AOS-142000, AOS-142561, AOS-142578, AOS-142701, AOS-142918, AOS-143300, AOS-143320, AOS-143489, AOS-143617, AOS-143759, AOS-143796, AOS-143913, AOS-144081, AOS-144787, AOS-145368, AOS-146152, AOS-146411, AOS-146746, AOS-158323. **Old IDs:** 183858, 125335, 152333,159970, 167506, 169114,169246, 169314, 169523, 169596,170181, 170238, 170446, 170740, 170956, 170957, 171337, 172736,172884,173586,173613,173769,174036,174531, 174553, 174797,174968, 175153, 175197, 175349, 175566,176496, 177293, 178339, 178864, 179135, 195282.	AOS-W 8.2.0.0
AOS-188073	—	The **Max Negotiated Tx Rate** was incorrect after changing the **vht-support-mcs** and **supported-mcs-set** values. The fix ensures that the correct values are displayed. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-188170	—	The Common Name of captive portal certificate was changed from the company's domain name to **securelogin.arubanetworks.com** after upgrading the managed device. The fix ensures that when the switch certificate expires, the captive portal certificate does not get replaced by the default certificates. This issue occurred when a custom certificate used for switch certificate expired and the captive portal certificate got replaced with the default certificate. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-188285	—	Mesh portal rebooted continuously because the **wpa_hex_key** value exceeded more than 132 bytes string in the **ap mesh-recovery-profile cluster <cluster_id> wpa-hexkey <wpa_hex_key>** command. The log files listed the reason for the event as **AP rebooted Tue Jun 11 10:40:01 CDT 2019; Critical process /aruba/bin/meshd [pid 2450] DIED, process marked as RESTART**. This issue is resolved by using **mesh-recovery-generate** command to get a qualified hex-key.	AOS-W 8.3.0.7
AOS-188429	—	Client was unable to login to the managed device after upgrading the AOS-W version to AOS-W 8.5.0.0. The fix ensures that the managed devices work as expected.	
AOS-188467	—	The AMON messages from a peer cluster displayed **wrong value for cl_cluster_incompatible_reason** error messages because the incompatible reason was not reset after an incompatibility with a peer cluster member was resolved and the cluster was re-formed. The fix ensures that incompatible reason is reset to zero when the cluster is re-formed after resolving incompatibility. This issue was observed in managed devices running AOS-W 8.3.0.6 in a cluster topology.	AOS-W 8.3.0.6
AOS-188437 AOS-149344 AOS-155500	182960 191229	Mobility Master displayed the **tar crashError tar'ing(1). May have run out of space** error message. This issue occurred when a user executed the tar crash command to generate the crash.tar file. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-188485 AOS-193638	—	The **<ofald 237504> <ERRS> |AP 32438@172.16.4.151 ofald| |sdn| ERRS ofald_datapath_msg_recv_cb:274 Invalid message type 126** error message was displayed every second in APs. The fix ensures that these spurious messages do not come through. This issue was observed in APs running AOS-W 8.4.0.0-FIPS in a Mobility Master-Managed Device topology.	AOS-W 8.4.0.0
AOS-188470	—	PPPoE did not work when a OAW-RAP was provisioned using ZTP and the **Either ping is disabled on AP's uplink router or there are issues with AP's uplink connectivity** error was displayed. The fix ensures that if the AP is a PPPoE AP, the AP does not reboot after checking for the IP address in the PPPoE server. This issue was observed in OAW-AP203R access points running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-188478	—	The OAW-RAP whitelist file did not contain the first MAC address entry. This issue occurred when the user runs the **show whitelist-db rap export-css <filename>** command to export the OAW-RAP whitelist file to the switch directory. The fix ensures that the OAW-RAP whitelist file is exported successfully. This issue was observed in stand-alone switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.5
AOS-188505	—	The **wlanAPWiredPortRxBytes** and **wlanAPWiredPortTxBytes** displayed incorrect values when an SNMP walk was performed using the **IPNetMonitorX** tool. The fix ensures that the correct values are displayed. This issue occurred when: the client generated more traffic. the counters increased beyond 32-bit. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-188594	—	The **datapath** process in a switch crashed unexpectedly when the data traffic that was sent from the switch to the VPN Concentrator (VPNC) was not fully compressed. The fix ensures that the **datapath** process does not crash and the switch works as expected. This issue was observed in OAW-4450 switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-188597	—	A managed device failed to send User-ID update to Palo Alto Network even though the managed device successfully established HTTPS connection to Palo Alto Network firewall. This issue is resolved by providing the missing key-name for the key-attribute in the User-ID PAN-API message. This issue occurred because of a missing key-name for the key-attribute in the User-ID PAN-API message. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-188649 AOS-183922 AOS-147702	180722	High memory utilization was observed and the **show memory debug** command did not include the memory available column. The fix ensures proper memory utilization and the command **show memory debug** will display the memory available field. This issue was observed in Mobility Master running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
AOS-188664 AOS-194339	—	The output of the **show airmatch debug static-radios** command did not display AP related information. This issue is resolved by issuing the **show airmatch debug reporting-radio mac <MAC address>** command. This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-188971 AOS-189146	—	Split tunnel clients got disconnected frequently when the split-tunnel had more than one IP address (IPv4 and IPv6) and the client got deauthenticated even if one of the IP addresses were actively sending or receiving traffic. The log files listed the reason for the event as **Denied; Ageout**. The fix ensures that the split tunnel clients do not get disconnected. This issue was observed in a stand-alone switch running AOS-W 8.4.0.1 or later versions.	AOS-W 8.4.0.1

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-189152 AOS-191781	—	Although redundancy was disabled in the **lc-cluster profile**, some APs appear are appearing with standby tunnels on the switch. As a result, the **show lc-cluster load distribution ap command** returned incorrect ap count. The fix ensures that APs do not get a standby switch assigned when redundancy is disabled. This issue was observed in access points running AOS-W 8.4.0.4.	AOS-W 8.4.0.4
AOS-189160	—	A few APs running AOS-W 8.3.0.4 or later versions rebooted unexpectedly. The log files listed the reason for this event as **Critical process /aruba/bin/rapper [pid 7933] DIED, process marked as RESTART**. The fix ensures that the APs work as expected.	AOS-W 8.3.0.4
AOS-189189 AOS-191358	—	A few users were unable to establish a VPN connection with the managed device or VPNC using AnyConnect application. The fix ensures that the AnyConnect application is able to establish the VPN connection. This issue occurred when IP Compression was enabled on the managed device or VPNC. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-188830 AOS-190051 AOS-194626	—	Some configurations were lost when an L2 switchover occurred in a Mobility Master. The fix ensures that the Mobility Master works as expected. This issue was observed in a Mobility Master running AOS-W 8.5.0.2.	AOS-W 8.5.0.2
AOS-189008	—	An AP showed a high RSSI value. This issue is resolved by enhancing the wireless driver to show the correct RSSI value. The issue occurred when low power was used on the AP radio. This issue was observed in OAW-AP515 access points running AOS-W 8.4.0.3 or later versions.	AOS-W 8.4.0.3
AOS-189194	—	The 5 GHz and 2.4 GHz antenna values were swapped after AP provisioning rules configuration is committed in the **Configuration > Access Points > Provisioning Rules** page of the WebUI. This issue occurred when the user selected the **Set Antenna Gain for Dual Band mode option** from the Actions drop-down list and entered the **5 GHz and 2.4 GHz** field values in the WebUI. The fix ensure that the values are displayed correctly in the WebUI. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.4.0.3 or later versions.	AOS-W 8.4.0.3
AOS-189300 AOS-192761	—	A few managed devices crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed devices work as expected. This issue occurred when the site-to-site IPsec tunnel was disconnected on the managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-189392 AOS-190057 AOS-192234	—	An AP used the wrong PoE status. Enhancement to the wireless driver resolved this issue. This issue occurred when the external switch granted grater power to the AP via LLDP negotiation, and the AP detected the power as invalid. This issue was observed in 510 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-189420	—	Clients declined the IP addresses and were unable to connect to the managed device. The fix ensures that the clients are able to connect to the managed device. This issue occurred because the managed device sent an ARP request to the client's mac address. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	
AOS-189429	—	XSS allowed client-supplied data from malicious users to execute commands in users' web browser. The fix ensures that the XSS does not allow data supplied from malicious users to execute commands in the users' web browsers. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-189471	—	A few clients were unable to connect to APs that are configured with LACP and have allowed band of 5 GHz. The fix ensures that clients connect to APs seamlessly. This issue was observed in OAW-AP335 access points running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-189478	—	The IPv6 multicast stream did not pass to clients when the VAP forward mode was set to d-tunnel. The fix ensures that the AP works as expected. This issue was observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-189504 AOS-189181	—	The **Configuration > Interfaces > Ports** page in the WebUI displayed the **Expecting string of length 1 to 32** error message in the **Allowed VLANs** field. The output of the **interface port-channel** command also displayed the same error message. This issue occurred when the trunk allowed VLAN was added from either WebUI or CLI, due to which trusted VLANs beyond 32 characters could not be added. The issue is resolved by increasing the string length of the trusted VLAN to 255 characters. This issue was observed in Mobility Master running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
AOS-189551	—	Port Based Tunnel (PBT) client traffic from different ports of the same switch was not broadcasted across multiple CPUs and a single CPU was used for client traffic. The fix ensures that the switch is able to broadcast PBT to multiple CPUs. This issue was observed in OAW-4850 switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-189625 AOS-192000 AOS-191733	—	A few switches crashed and rebooted unexpectedly when DPI was enabled on the switches. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the switches work as expected. This issue was observed in OAW-4750 and OAW-4750XM switches running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-189721	—	Datapath process crashed in a managed device. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed device works as expected. This issue was observed in OAW-4550 switches running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-189750	—	Modified EIRP values were not visible on the managed device's **Configuration > AP Groups > AP group name > Radio> Basic** page of the WebUI. The fix ensures that the correct EIRP value is displayed in the WebUI pages of both Mobility Master and managed device. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-189757	—	The Captive Portal redirection did not work when the client **http GET** packet contained files with .png or .gif format. The fix ensures that files with .png or .gif format are not included. This issue is observed in managed devices running AOS-W 8.4.0.2.	AOS-W 8.4.0.2
AOS-189768	—	IPv6 users did not receive route advertisements and hence faced connectivity issues. The fix ensures that the users receive the route advertisement. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
AOS-189782	—	A user was unable to perform SSO with ClearPass Policy Manager and had to enter the username and password manually. The fix ensures that the SSO works correctly with ClearPass Policy Manager. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-189802 AOS-190543	—	The Google Chromecast service stopped responding unexpectedly in OAW-AP303H access points running AOS-W 8.2.2.0 or later versions in a stand-alone switch. The issue is resolved by converting the OAW-APs to OAW-RAPs. This issue occurred when the Google ChromeCast device and the guest wireless client were connected to the same AP in bridge mode SSID.	AOS-W 8.4.0.1
AOS-189977	—	Managed Device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2)**The fix ensures that the managed device works as expected. This issue was observed inmanaged devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-189986	—	A few users were unable to configure the WPA passphrase and received the **Fields does not match** error message under **Security** tab in the **Configuration > WLANs > New WLAN** page in the WebUI. The fix ensures that the users are able to configure the WPA passphrase. This issue occurred when the users added an extra space at the end of the WPA passphrase. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-190071 AOS-190372	—	A few users were unable to access the websites when WebCC was enabled on the user role. This issue occured in a Per User Tunnel Node (PUTN) setup when the VLAN of user role was in trunk mode. The fix ensures that users can access websites seamlessly. This issue was observed in OAW-4005 switches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-190084 AOS-189945	—	A fatal error message was displayed when there was mismatch between the AOS-W versions of a Mobility Master and managed device. Changes to the log levels resolved this issue. This issue was observed in managed devices running AOS-W 8.3.0.0 or later.	AOS-W 8.3.0.0
AOS-190231 AOS-193796	—	The **tar crash** command failed to generate the **crash1.tar** file. The fix ensures that the crash file is generated. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-190184 AOS-190241 AOS-190347 AOS-190405 AOS-190468 AOS-190487 AOS-190776	—	The database synchronization failed between primary and secondary Mobility Masters in L3 redundancy. The fix ensures that the L3 redundancy works as expected. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-190478	—	The **WARN |fpapps| Duplicate MAP_ADD from IKE for default-ha-ipsecmap** syslog messages were generated on managed devices running AOS-W 8.3.0.0 or later versions in a cluster setup. The syslog messages were displayed only when the logging level of type information was enabled. The fix ensures that the syslog messages are not displayed.	AOS-W 8.3.0.7
AOS-190633 AOS-191480	—	A few clients connected to APs through bridge mode SSID were unable to obtain IP address or forward traffic. Also, the APs crashed and rebooted unexpectedly when the **show ap debug acl-table ap-name <ap-name>** command was executed. The fix ensures that the APs work as expected and the clients are able to connect to them. This issue was observed in OAW-AP215 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-190927 AOS-192132	—	A Mobility Master become unresponsive and had to be power cycled. The fix ensures that the Mobility Master works as expected. This issue occured because the core files present in tmpfs were not getting copied to the process's crash directory. This issue was observed in a Mobility Master running AOS-W 8.4.0.4	AOS-W 8.4.0.4
AOS-190930	—	The AP crashed, after a new cluster node was added. The fix ensures that the APs work as expected. This issue is observed in AOS-W 8.4.0.4.	AOS-W 8.4.0.4
AOS-191019 AOS-193042	—	A few OAW-AP345 access points running AOS-W 8.3.0.7 crashed and rebooted unexpectedly. The log files listed the reason for the event as **AP Reboot reason: Warm-reset**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.3.0.7
AOS-191025		A few devices dropped the DHCPv6 solicit packet sent by APs. The fix ensures that the AP adds AP MAC address in link-layer address in the client identifier field. This issues occured because APs sent DHCPv6 solicit message with "00:00:00:00:00:00" link-layer address instead of MAC address. This issue is observed in OAW-AP320 Series access points running AOS-W 8.5.0.1.	AOS-W 8.5.0.1

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191035	—	When the user attempted to enable redundancy, an error message was displayed - **VRRP IP or VLAN cannot be changed when cluster group-membership is enabled. Disable cluster group-membership on all nodes and try again**. The fix ensures that the error message does not appear. This issue was observed in managed devices running AOS-W 8.4.0.4.	AOS-W 8.4.0.4
AOS-191080 AOS-193211	—	The **STM** process crashed continuously on a OAW-4650 switch and users were unable to connect to the network. This issue was due to a corrupt channel in the tunneled node manager. The fix ensures that the **STM** process crash does not re-occur. This issue was observed in OAW-4650 switches running AOS-W 8.4.0.2.	AOS-W 8.4.0.2.
AOS-191112	—	A few data packets were lost when the packets were forwarded using AP Packet Capture. The fix ensures that the APs work as expected. This issue occurred when the APs were in Air Monitor mode. This issue was observed in OAW-AP325 and OAW-AP335 access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-191116	—	APs on pure-UAC had missing Radio/EIRP information for random APs when the **`show ap active`** command was issued. This issue is resolved by adding a **Cluster Role** column in the output of **`show ap active`** command. This issue was observed in APs connected to pure-UACs running AOS-W 8.3.0.4.	AOS-W 8.3.0.4
AOS-191195	—	A few devices dropped the DHCPv6 solicit packet sent by APs. This issue occurred when APs sent DHCPv6 solicit message with "00:00:00:00:00:00" link-layer address instead of MAC address. The fix ensures that the AP adds AP MAC address in link-layer address in the client identifier field. This issue was observed in OAW-AP320 Series access points running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-191261	—	Wireless clients were unable to connect to the network due to mac-user entries leak. The fix ensures that the clients are able to connect to the network. This issue was observed in managed devices running AOS-W 8.3.0.5 or later versions.	AOS-W 8.3.0.5
AOS-191292 AOS-193191	—	Managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2)**. The fix ensures that the managed device works as expected. This issue occurred because of high rate of ARP packets on VLAN 50. This issue was observed in managed devices running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-191378	—	ESI did not provide load balancing of traffic between two servers. The fix ensures that the traffic is balanced between the two servers. This issue was observed in managed devices running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-191997 AOS-157544 AOS-192527	—	Licenses were missing after a switch rebooted, due to database corruption, which is caused by power outages. The fix ensures that the licenses are not lost when a switch is rebooted. This issue was observed in switches running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191675	—	Some clients experienced packet loss, when they attempted to reach the destination with route-cache entry marked as inactive. The fix ensures that inactive route-cache entry is not created and a bandwidth contract is used for IP packets with errors, to avoid flooding the Captive Portal. This issue was observed in managed devices running AOS-W 8.3.0.3 or later versions.	AOS-W 8.3.0.3
AOS-191752	—	Some APs were not being reclassified though the classification rules were modified using the **ids ap-classificationrule** command. This issue was observed when the AP classifications were changed using ids-rules, but the old classification rules were not changing. The fix ensures that the APs get reclassified. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-191820	—	The output of the **show datapath dns-cache counter** command did not display any information. The fix ensures that the command output displays the required DNS cache statistics. This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-191962	—	OAW-AP315 and OAW-AP365 access points running AOS-W 8.4.0.4 or later version were unable to connect to the managed device when CPsec was enabled. The fix ensures that the access points are able to connect to the managed device	AOS-W 8.4.0.4
AOS-192542	—	The BSSID MTU value in data zone reverted back to the previous value after the AP was rebooted. The fix ensures that the BSSID MTU value can be changed successfully using the **ap system-profile** command. This issue was observed in APs running AOS-W 8.5.0.1.	AOS-W 8.5.0.1
AOS-192568 AOS-192736	—	A few clients were unable to connect to APs even though High-Efficiency was disabled on all the SSID profiles of the APs. Enhancements to the wireless driver resolved the issue. This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.1
AOS-192711	—	The load balancing between two RADIUS servers failed on a managed device. The fix ensures that the load is balanced equally between both the servers. This issue occurred because the authentication requests were not distributed equally between both the RADIUS servers. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.1
AOS-192841	—	The **Station Management** process crashed on a managed device running AOS-W 8.3.0.1 or later versions and the APs were unable to communicate with the managed device. The fix ensures that the managed devices work as expected.	AOS-W 8.0.0.0
AOS-192857	—	The **fw_visibility** process crashed in a 4-node cluster after an upgrade. The fix ensures the cluster works as expected after an upgrade. This issue was observed in switches running AOS-W 8.0.0.0.	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193083	—	Cluster upgrade failed on a 2 node cluster because the AP platform capacity of the managed device was only 4 and the hash table size was calculated as zero. The fix ensures that the hash table size is set to 1, which ensures a successful hash table creation. This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-193103	—	Incorrect captive portal redirect URLwas observed because of corrupt ap-mac address. The fix ensures that the correct ap-mac address is used in the captive portal redirect URL. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-193115	—	The **impystart** process crashed on a Mobility Master Virtual Appliance. The fix ensures that the **impystart** process does not crash and works as expected. This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.4.0.4.	AOS-W 8.4.0.4
AOS-193188	—	The **Reclassify Detected Radios** pop-up window displayed action commands for a specific SSID in the **Dashboard > Security > Detected Radios** page of the WebUI. The fix ensures that the action commands are not visible on the **Reclassify Detected Radios** pop-up window. This issue occurred when apostrophe and quotation were added to the ESSID of a OAW-4550 switch running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.1
AOS-193661 AOS-193696	—	The output of several commands related to OAW-AP535 access points displayed **Module AM is busy. Please try later.** or **Module AP STM is busy. Please try later.** messages. The fix ensures that the error messages are not displayed for the commands. This issue was observed in OAW-AP535 access points running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.2
AOS-193705	—	In a cluster setup, the **authentication** process crashed in a OAW-4750 managed device running AOS-W 8.4.0.0 because the managed device ran out of virtual address space. This issue is resolved by increasing the virtual address space in the managed device.	AOS-W 8.4.0.0
AOS-193879	—	A DHCP broadcast sent from UBT 1.0 or 2.0 client did not reach the other UBT 2.0 clients that are on the same VLAN in a managed device running AOS-W 8.3.0.0 or later versions. The fix ensures that the DHCP broadcast is sent to the correct client and the managed device works as expected.	AOS-W 8.3.0.0
AOS-194082 AOS-196092	—	A few APs running AOS-W 8.6.0.0 crashed and rebooted unexpectedly. The log files listed the reason for the event as **BadPtr:00000006 PC:wlc_keymgmt_wsec+0x28/0xa4 [wl_v6] Warm-reset**. Enhancements to the wireless driver resolved this issue.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-194560	—	Users were able to upload the Bulk Edit configuration file from the **Configuration > Tasks > Bulk configuration upload** page in the WebUI. The fix ensures that the Bulk Edit configuration file is not editable from the secondary Mobility Master in Layer-3 redundancy, and the **Bulkedit commands not permitted on L3 Secondary** pop-up message is displayed in the WebUI. This issue was observed in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-185812	—	User traffic in tunneled node dropped when web-cc was enabled. The fix ensures that the user traffic is not dropped. This issue was observed in Mobility Master running AOS-W 8.3.0.0 or later versions	AOS-W 8.3.0.0
AOS-183914	—	Some Skype users were unable to join conference calls. This issue occurred when ALG was enabled and the PBR was configured to forward all traffic from clients to VPNC. . The fix ensures that the Skype users are able to connect and join conferences seamlessly. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-186380	—	The **show datapath session dhcp-perf** and **show datapath session perf** commands had extra white spaces in the output and the output looked corrupted. The fix ensures that the output is displayed properly in the CLI. This issue was observed in Mobility Master running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-193960	—	The **show ap debug radio-stats** command did not display the channel utilization value. The fix ensures that the command works as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.5 or later versions.	AOS-W 8.3.0.5
AOS-183468 AOS-183550 AOS-183551 AOS-184610 AOS-194037 AOS-186877 AOS-186916	—	Managed Device crashed and rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2**). This issue occurred because OpenFlow from the managed device was sending all ARP packets to the Mobility Master. This issue is resolved by optimizing the ARP data that is sent to Mobility Master. This issue was observed in Mobility Master running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-186863 AOS-186374	—	Mobility Master crashed and rebooted unexpectedly. The log file listed the event for the as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Master running AOS-W 8.2.2.3 or later versions.	AOS-W 8.2.2.3
AOS-186440	—	The static IP address was not validated in the setup dialog. The fix ensures that the static IP address is validated. This issue was observed inmanaged devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-186411	—	Users were unable to remove a VLAN from port channel trunk. This issue was observed inMobility Master running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-184873 AOS-187032	—	A few clients got disconnected from the AP randomly. The fix ensures that the clients stay connected to the network. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
AOS-187306 AOS-150599	184591	Kernel Coredump was broken in a Mobility Master. This issue was observed in Mobility Master running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0

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

Limitations

Following are the limitations observed in this release.

OAW-AP555 Mesh Portal Limitation

The OAW-AP555 access points operating as a mesh portal reboot automatically when **split-5ghz-mode** is enabled.

Incorrect Sub-Parameter Names in Masteripv6 command

The following sub-parameter names under **ipsec-custom-cert** and **ipsec-custom-cert** parameters of **masteripv6** command are incorrect:

- **interface-c**
- **vlan-c**
- **fqdn-c**
- **interface-f**
- **vlan-f**
- **fqdn-f**

IoT

The **telemetry** profile gets added in a managed device when **ap-grp** is configured in the profile. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.

No IPv6 Support for Mini-Setup Provisioning Mode

The provisioning of managed devices using IPv6 address is currently not supported in a mini-setup mode.

No Support for FQDN over IPv6 Network

The FQDN support for IPv6 address is currently not available in full setup provisioning mode for managed devices.

No ZTP Support for IPv6 in Activate Server

Zero Touch Provisioning for IPv6 using Activate server is currently not supported.

No ZTP and Multi-version Support for OAW-4104 switches

Zero Touch Provisioning and multi-version support for OAW-4104 switches are currently not supported.

It is recommended to have the Mobility Master and managed device running the same AOS-W version.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-108176	130121	A user cannot search for AP group, AP MAC address, AP name, state, or certificate type in the whitelist database. This issue is observed in managed devices running AOS-W 8.0.0.0.	AOS-W 8.0.0.0
AOS-124045	149416	Users are unable to configure the Wireless Intrusion Prevention System policies using the **Configuration > Tasks > Define Wireless Intrusion Protection (WIP) policy** page in the WebUI. This issue is observed when the user disables the WIPS policy intrusion detections using the wizard in the WebUI. This issue is observed in APs running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-137488	166937	The **AirGroup** process stops responding unexpectedly. This issue occurs when an AirGroup profile is changed in a managed device with mDNS servers and users. This issue is observed in managed devices running AOS-W 8.2.0.0.	AOS-W 8.2.0.0
AOS-138719	168501	APs crash unexpectedly when using Suite-B algorithm to enrol certificates using EST. This issue occurs when the AP platforms do not support enrollment of Suite-B certificates like ECDSA-256, ECDSA-384 using EST. This issue is observed in OAW-AP135, OAW-AP325 and OAW-AP334 access points running AOS-W 8.2.00 or later versions.	AOS-W 8.2.0.0
AOS-139460	169472	The CLI command **show datapath error counters** does not display the error counters. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-140817	171368	The multi-user upstream performance with MU-MIMO clients is low. This issue occurs because of Rx packet drop, This issue is observed in access points running AOS-W 8.3.0.0.	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-149536	183192	Unable to check the ASP connection status of the standby Mobility Master from the **Mobility Master > Configuration > Licenses > Aruba Support Portal (ASP)** page in the WebUI. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions. **Workaround**: View the standbyMobility Master ASP connection status using CLI, **show asp status standby** command in the active Mobility Master.	AOS-W 8.4.0.0
AOS-149550	183213	ASP account information is not displayed in the **Mobility Master > Configuration > System > General > Aruba Support Portal page** in the WebUI. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions. **Workaround:** View the ASP account information by executing the command, **show asp account-info**.	AOS-W 8.4.0.0
AOS-149713	183430	User is unable to move from external licensing server mode to ASP mode automatically without manually enabling the ASP profile. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-146549	178875	When a custom app is added or deleted, the **malloc_pages: sos_malloc_dpi failed : processorid : 8, pdata load error -5** error is displayed because the memory reduces each time an AppRF configuration change is made. This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** Restart the managed devices.	AOS-W 8.3.0.0
AOS-148793	182224	The license successfully claimed message is not displayed in the **Mobility Master > Configuration > Licensing > License Inventory** page in the WebUI. This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-149291	182885	The aggregate number of VIA licenses count and managed node hierarchy information is not displayed in the **Mobility Master > Configuration > Licensing > License Inventory** page in the WebUI. This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-149537	183193	User is unable to use the **Enter** key to sign in from the **Signin to ASP** popup window after entering the correct credentials. This issue is observed in Mobility Master running AOS-W8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-150173	184030	The cumulative count of licenses allocated and installed from both active and standby Mobility Masters is not displayed once the active Mobility Master comes up after a failover. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions. **Workaround:** To view the cumulative count of licenses allocated and installed from both active and standby Mobility Masters, navigate to **Mobility Master > Configuration > License > License Inventory** tab and click **update now link**, once the Mobility Master comes up after failover.	AOS-W 8.4.0.0
AOS-152326	186957	An AP does not display the country capabilities IE in beacon and probe response packets. This issue observed in access points AOS-W 8.4.0.0.	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-152380	187033	The **Usage** page under **Dashboard > Overview > Wireless Clients** in the WebUI does not display the transmitted and received throughput data (bps) for PUTN clients. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-153409	188429	A total of 16 capacity licenses are allowed per allocation attempt, with a maximum of 4 per type. A validation message for the same is not displayed when the count exceeds 16. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions. **Workaround:** Allocate licenses according to the limits.	AOS-W 8.4.0.0
AOS-153567	188639	The **Access Points** page under **Managed Network > Dashboard** becomes unresponsive and does not display any information. This issue occurs when the OmniAccess Mobility Controller WebUI is accessed using the Firefox browser. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.4.0.0 or later versions **Workaround:** Switch to Google Chrome browser.	AOS-W 8.4.0.0
AOS-154517	189885	A Mobility Master does not use the password configured in the upgrade profile. This issue is observed in Mobility Master running AOS-W 8.4.0.0. or later versions.	AOS-W 8.4.0.0
AOS-154540	189921	The **Age** column under **Dashboard > Overview > Wired Clients** table, and the **Tunneled Switches** table under **Dashboard > Infrastructure** display incorrect values. This issue occurs when there is no NTP synchronization between the devices. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions. **Workaround:** Perform an NTP synchronization across all connected Mobility Masters and managed devices.	AOS-W 8.4.0.0
AOS-155745	191638	Clients do not receive the multicast packets as the IPv6 streaming is not working as expected. This issue occurs when there are clients on two different nodes acting as source and destination. This issue is observed in a cluster where MLD proxy is enabled and the managed devices are running AOS-W 8.4.0.0.	AOS-W 8.4.0.0.
AOS-156585	192812	A per user tunneled-node client is unable to receive stream when the User Anchor Controller (UAC) fails over twice. This issue occurs when two per user tunneled-node clients with different VLANs are requesting for the same stream and the **no-vlan** parameter is enabled on the per user tunneled-node clients. This issue is observed in managed devices running AOS-W 8.4.0.0.	AOS-W 8.4.0.0
AOS-156896	193225	The Tunneled clients column under **Dashboard > Infrastructure > Tunneled Switches** table displays incorrect tunneled clients information. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-156957	193297	The Tunneled Switches table under **Dashboard > Infrastructure > Access Devices** displays zero **Tunneled Clients** for IPv6 tunnels between Mobility Master and managed device. This issue is observed in Mobility Master running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-179895	186918	Air time fairness feature is not functional although the value of the **shaping-policy** parameter is set to **default-access**. This issue is observed in 510 Series access points running AOS-W 8.4.0.0.	AOS-W 8.4.0.0
AOS-183317 AOS-186033	—	An AP detects multiple false radars on channel 100, with type ID 255. This issue is observed in 530 Series access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-183878	—	The total load percentage of managed devices are not displayed in the logs although more APs are added to the managed devices. This issue is observed in managed devices running AOS-W 8.5.0.0 in a cluster setup.	AOS-W 8.5.0.0
AOS-184342	—	An AP does not support mcs0-mcs15 rates for video multicast rate optimization. This issue is observed 510 Series access points running AOS-W 8.4.0.0.	AOS-W 8.4.0.0
AOS-184834	—	The AP and client entries are not displaying zero although the managed device is disabled or shut down. This issue is observed in managed devices running AOS-W 8.5.0.0 in a cluster setup.	AOS-W 8.5.0.0
AOS-185680	—	The panic dump of an AP is incomplete or truncated. This issue is observed in access points running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-185707	—	An AP crashes unexpectedly. The log file lists the reason for the crash as **watchdog bite received from wcss software**. This issue is observed in access points running AOS-W 8.5.0.0.	AOS-W 8.5.0.0
AOS-185779	—	The log file of an AP shows the **txerr mac 0240 phy 8280 0000 0200 tst 3131 dur 0056** error. This issue is observed in access points running AOS-W 8.5.0.2.	AOS-W 8.5.0.2
AOS-186503	—	The CLI command **show ap bss-table** displays the details of eth1 even when wired-ap is configured on eth1 and the same is the uplink of the AP. This issue is observed in OAW-AP225, OAW-AP325, OAW-AP515, OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-187556	—	A user cannot enroll an AP with an EST server. This issue is observed in OAW-AP100 Series and OAW-AP130 Series access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-188368	—	A PBR rule is not applied to a VIA user role that has upper case characters. This issue is observed in Mobility Master running AOS-W 8.5.0.0 FIPS and a managed device running AOS-W 8.3.0.6 FIPS image.	AOS-W 8.5.0.0-FIPS

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-188438	—	WLAN clients who are not in the same subnet as Mobility Master are unable to reach the VRRP IP of the Mobility Master. This issue is observed inMobility Master running AOS-W 8.6.0.0. **Workaround:** Configure reverse route to the client subnet over the Mobility Master- Managed Device tunnel.	AOS-W 8.6.0.0
AOS-189074	—	A gigabitethernet interface of a managed device does not accept LACP configuration. This issue is observed in managed devices running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-189227	—	The **datapath** process in a Mobility Controller Virtual Appliance crashes unexpectedly when the OAW-RAPs with wired users connected fail over to Backup LMS IP. This issue occurs when the wired user VLAN is same as the switch VLAN of the Mobility Controller Virtual Appliance. This issue is observed in Mobility Controller Virtual Appliance running AOS-W 8.5.0.0 or later versions. **Workaround:** Ensure that the wired user VLAN and controller VLAN of the Mobility Controller Virtual Appliance are configured with different values.	AOS-W 8.5.0.0
AOS-189230	—	The CLI command **show log errorlog** displays the error log, **Process /aruba/bin/hostapd [pid 2038] died: exited with 0x0.** This issue occurs when the mesh recovery mode works as the mesh point mode in OAW-AP535 and OAW-AP555 access points. This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-189426	—	A user cannot configure a managed device using a PC. This issue occurs when a PC is connected to the gigabitethernet port 0/0/0 of a managed device and the setup wizard is used for configuration. This issue is observed in managed devices running AOS-W 8.4.0.0.	AOS-W 8.4.0.0
AOS-189604	—	A few APs with CPsec enabled are not responding and are stuck with D flag (dirty mode) in an IPv6 cluster when VRRP IPv6 address is configured and CPsec is enabled. As a result, the AP goes into D flag mode due to incorrect port selection in the SAPD process. This issue is observed in APs running AOS-W 8.5.0.0 or later versions in a cluster setup. **Workaround:** Disable the VRRP IPv6 address.	AOS-W 8.5.0.0
AOS-189952	—	The **mDNS** process in a managed device crashes unexpectedly. This issue occurs when AirGroup is enabled in an island topology and a client roams across islands. This issue is observed in managed devices running AOS-W 8.2.2.6.	AOS-W 8.2.2.6
AOS-190056	—	OWE enabled Virtual AP does not send deauthentication frames when OWE transition is disabled. This issue is observed in OAW-AP225 and OAW-AP515 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-190149	—	The CLI command **show license-pool-profile-root** displays incorrect status of licenses. This issue is observed in Mobility Master running AOS-W 8.6.0.0.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-190287	—	Huge latency is observed for TX data frames to 11ac clients when VHT TxBF and VHT MU TxBF are enabled. This issue is observed in 530 Series and 550 Series access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-190442	—	A mesh point works in 40M mode although 80M mode is enabled. This issue occurs when the mesh-ht-profile is changed from 80/VHT disable to 80/VHT enable. This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-190764	—	The CLI command **show database synchronize** displays incorrect value for L3 redundancy counters. This issue is observed in Mobility Master running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-190996	—	The CLI command **show ap mesh debug provisioned-clusters** displays ***** Error ***** for mesh recovery cluster encryption. This issue is observed in OAW-AP504 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-191031	—	802.11 ax clients experience poor MU-MIMO performance. This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-191192	—	A user cannot delete deviceClassfilter all from an IoT transport profile. This issue occurs when a deviceClassFilter is not empty. This issue is observed in managed devices running AOS-W 8.6.0.0. **Workaround:** A user cannot delete deviceClassFilter all in the middle of editing an IoT transport profile. Issue the **write memory** command and then issue the **no deviceclassfilter all** command.	AOS-W 8.6.0.0
AOS-191295	—	The output of the **show ap remote debug mgmt-frames** command does not display the 11k BTM-response action frames. This issue occurs when the forwarding mode set to tunnel mode. This issue is observed in 530 Series access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-191323	—	A user cannot move a managed device with LACP configuration to a different point in an hierarchy. This issue is observed in managed devices running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-191761	—	An AP loads configuration in loops. This issue occurs when the speed of the eth0 port is modified to a fixed value with STP enabled on the peer port of the switch. This issue is observed in access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-191784	—	The **BLE relay** process drops a message that is intended for a managed device. This issue is observed in managed devices running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-191796	—	An access point reboots unexpectedly. This issue occurs when core dump and panic dump are generated even when fast recovery mode is enabled. This issue is observed in OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-192077	—	The output of the **show running-config | include uplink** command does not display the uplinks that are configured as backup links. This issue is observed in managed devices running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-192271	—	A user cannot autoassociate based on AP group. This issue is observed in access points running AOS-W 8.6.0.0. **Workaround:** Use AP name for autoassociation.	AOS-W 8.6.0.0
AOS-192364	—	The output of the **show ap database** command displays the **Switch role changed; reload required.** error message. This issue is observed after reboot of the **CFGM** process in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-192449	—	A managed device running AOS-W 8.6.0.0 does not establish IPv6 tunnel with the secondary Mobility Master when the authentication methods are different in Layer-3 redundancy configuration. This issue is observed during a failover when the primary Mobility Master goes down, and the managed device tries to communicate with the secondary Mobility Master using certificate-based authentication instead of PSK authentication.	AOS-W 8.6.0.0
AOS-192640	—	The output of the **show license-usage** command does not display the used licenses list in a stand-alone mobility controller running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-192662	—	The CLI command **show ap monitor** displays lesser number of AP neighbors. This issue is observed in OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-192827	—	The CLI command **show ap debug driver-log** displays the error log, **wlan: [1506:E:CFR] tgt_cfr_init_pdev: 107: Error occurred with exit code -22.** This issue is observed in tri-radio enabled OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-193104	—	AP Tx stalled for few seconds as AP is unable to drain packets in PS Queue while in 0x8 Block_Datafifo state. This issue is observed in 550 Series access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-193255 AOS-193646	—	Users are unable to configure the VPNC details of a managed device from the **Configuration > Controller** page in the **Managed Network** node hierarchy of the WebUI. This issue occurs due to the absence of **via VPN Concentrator** field in the WebUI. This issue is observed in managed devices running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-193889	—	A few APs are unable to pass higher transmission data of MCS 11 to Samsung Galaxy S10e clients. This issue is observed in OAW-AP515 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-194053	—	An AP is stuck in **IL** state although an AP license is available. This issue is observed in access points running AOS-W 8.0.0.0.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-194299	—	The output of the **show license serv** command displays the ACR license used as -1 on the secondary Mobility Master. This issue occurs because the license manager is getting incorrect ACR license usage from the authentication process. This issue is observed in Mobility Master running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-194302	—	Advanced cryptography (ACR) license consumption does not become zero when the ACR license feature is disabled. This issue is observed in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-195135	—	Users are unable to delete the IPv6 AP database entries on a managed device by using the **clear gap lms-ip6 <ipv6 address>** command. This issue is observed in managed devices running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-195146	—	Allowed vlan does not work when wired-ap is enabled with the ports set to trunk mode. This issue is observed in 530 Series and 550 Series access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-196582	—	EST re-enrollment fails on access points. This issue occurs when access points, configured with arbitrary label in the EST profile, are upgraded to AOS-W 8.6.0.0. This issue is observed in access points running AOS-W 8.6.0.0. **NOTE:** This issue gets auto-recovered when the EST certificate expires on the APs and during the auto-recovery the EST parameters are also downloaded from the managed device when the APs are rebooted. If you do not want to wait until the EST certificate expires, the following workaround is recommended: **Workaround:** Disable the EST profile before upgrade and enable it after the upgrade.	AOS-W 8.6.0.0
AOS-192738	—	The Mobility Master list in the WebUI incorrectly displays the mac address of the primary standby Mobility Master for the secondary Mobility Master. This issue is observed inMobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-195281	—	The **mdns** process crashes on a Mobility Master Virtual Appliance running AOS-W 8.6.0.0. The log file lists the reason for the event as **split_tunnel_discover_vlan ()**.	AOS-W 8.6.0.0
AOS-195570	—	AP is unable to decode the beamforming sounding frames from the clients resulting in BFD Failure and no MU transmissions to MU Capable clients. This issue is observed in 550 Series access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-195669	—	An AP sends traffic in SU mode although MU mode is enabled. This issue is observed in access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-195831	—	The secondary active Mobility Master does not delete the MAC entries, though the secondary standby Mobility Master is deleted from an ESXI server. This issue is observed in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-195604	—	Peak single-client top line throughput are not maintained with certain High Efficiency 802.11ax clients with MU-MIMO and OFDMA enabled. This issue is observed in OAW-AP555 access points running AOS-WS 8.6.0.0.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.6.0.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195902	—	The output of the **show crypto ipsec sa** command displays **T2** flag instead of **UT2** flag when IPv6 address is used in Layer-3 redundancy. This issue occurs because the managed devices use only 500 port in IPv6 connections. This issue is observed in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-195982	—	OAW-4104 managed devices running AOS-W 8.6.0.0 are unable to reach the secondary Mobility Master after multiple L3 switch overs.	AOS-W 8.6.0.0
AOS-196195	—	Users are unable to change the configuration details from IPv4 to IPv6 and vice-versa under the **Master Redundancy** accordion in **Configuration > Redundancy > L2 Redundancy** page of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-196211	—	The **Configuration > Controller** page in the WebUI does not display any information when users enable **Enable l3 redundancy**. This issue is observed in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-196212	—	Users are unable to add the VPN peer MAC entries in the **VPN concentrator peers** table under **Configuration > Controller** page in the WebUI. This issue occurs when the users click **+** to add the VPN peer MAC entries in the **VPN concentrator peers** table. This issue is observed in Mobility Masters running AOS-W 8.6.0.0.	AOS-W 8.6.0.0

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

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

Topics in this chapter include:

Migrating from AOS-W 6.x to AOS-W 8.x

Use the interactive migration tool provided on the customer support site to migrate any AOS-W 6.x deployments to one of the following AOS-W 8.x deployments:

- Master-Local setup to Mobility Master
- All-Master setup to Mobility Master
- Master-Local setup to Master switch Mode in AOS-W 8.x
- Stand-alone switch running AOS-W 8.x

For more information, refer to the *AOS-W 8.x Migration Guide*.

Licenses are not migrated by the migration tool from any of the devices to Mobility Master. However, the licenses are preserved when migrating to AOS-W 8.x Master switch Mode or stand-alone switches. For more information on license migration, refer the *Alcatel-Lucent Mobility Master Licensing Guide*.

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 72 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
- **Flash backups:** Use the procedures described in Backing up Critical Data on page 72 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 72 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

From the Mobility 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 71.

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 72 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 72 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 72.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

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

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

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

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

In the CLI

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

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

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

   or

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

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

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

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

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

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.