AOS-W 8.5.0.0

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	■ Added **AOS-157396** as a Resolved Issue . ■ Added a limitation regarding captive portal in the **Known Issues** section. ■ Updated the description of **AOS-155389** under **Known Issues** section.
Revision 03	Removed **AOS-185867** from **Known Issues** section, and **AOS-155092** from **Resolved Issues** section.
Revision 02	Added content for bug **AOS-183745** as a limitation.
Revision 01	Initial release.

Use the following links to navigate to the corresponding topics:

- New Features and Enhancements on page 9 describes the new features and enhancements introduced in this release.
- Supported Platforms on page 16 describes the hardware platforms supported in this release.
- Regulatory Updates on page 19 lists the regulatory updates in this release.
- Resolved Issues on page 20 lists the issues resolved in this release.
- Known Issues and Limitations on page 47 lists the issues identified in this release.
- Upgrade Procedure on page 55 describes the procedures for upgrading your WLAN network to the latest AOS-W version.

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

Important Points Before Upgrading to AOS-W 8.5.0.0

DPI classification is not initialized after a switch is upgraded from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W 8.5.0.0. The affected platforms are OAW-4x50 Series switches.

An additional reboot of the affected platform is required to initialize DPI classification.

To check the status of DPI classification after upgrading an affected platform from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W, 8.5.0.0, issue the **show firewall | include dpi** command. In the following example, DPI classification is disabled:

```
(host) #show firewall | include dpi
DPI Classification      Disabled [Cfg: enabled, PEF license: installed]
```

If DPI classification is enabled, further action is not needed. However, if DP classification is disabled, issue the **show datapath utilization** and check if the DPI classification CPUs are initialized. In the following example, the DPI classification CPUs are disabled:

```
(host) #show datapath utilization

Datapath CPU Allocation Summary
Slow Path (SP) : 1,  Slow Path Gateway (SPGW) : 1
Fast Path (FP) : 17,  Fast Path Gateway (FPGW) : 1
DPI : 0, Crypto (CRYP) : 0
Slow Path Spare (SPSPARE) : 0
```

If the DPI classification CPUs are not initialized, reboot the affected platform by:

- Issuing the **reload** command.
- Power cycling the switch.

Related Documents

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

- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W Migration Guide*
- *AOS-W API Guide*
- *Alcatel-Lucent Mobility Master Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent Mobility Master Hardware Appliance Installation Guide*

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 and later on Windows 7, Windows 8, Windows 10 and Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

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/or enhancements introduced in AOS-W 8.5.0.0.

AP Platform

530 Series Campus Access Points

The Alcatel-Lucent530 Series campus APs (OAW-AP534, and OAW-AP535) are high-performance, multi-radio wireless devices that can be deployed in either switch-based or switch-less network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with 4x4 MIMO radios, while also supporting legacy 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Wired Ethernet ports located on the back of the 530 Series campus APs are used to connect the device to the wired networking infrastructure (wired speeds up to 5 Gbps are supported by both ports) and to provide POE power (802.3at class 4 or 802.3bt class 5) to the device. These APs also support 802.11w standard in tunnel mode with WPA3 security mode.

In addition to both the Wi-Fi radios, the 530 Series campus APs are equipped with Bluetooth Low Energy (BLE) radio that provide the following capabilities:

- Location beacon applications
- IoT gateway applications

For complete technical details refer *530 Series Campus APs Datasheet*. For installation instructions, refer *Alcatel-Lucent530 Series Campus APs Installation Guide*.

550 Series Campus Access Points

The Alcatel-Lucent550 Series campus APs (OAW-AP555) are high-performance, multi-radio wireless devices that can be deployed in either switch-based or switch-less network environments. These APs deliver high-performance concurrent 2.4 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with 4x4 MIMO radio and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with 8x8 MIMO radio, while also supporting legacy 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services. These APs also support 802.11w standard in tunnel mode with WPA3 security mode.

Wired Ethernet ports located on the back of the 550 Series campus APs are used to connect the device to the wired networking infrastructure (wired speeds up to 5 Gbps are supported by both ports) and to provide POE power (802.3at class 4 or 802.3bt class 5) to the device.

In addition to both the Wi-Fi radios, 550 Series campus APs are equipped with Bluetooth Low Energy (BLE) radio that provide the following capabilities:

- Location beacon applications
- IoT gateway applications

For complete technical details refer *550 Series Campus APs Datasheet*. For installation instructions, refer *550 Series Campus Access Points Installation Guide*.

Enhancements to 510 Series Campus Access Points

The Alcatel-Lucent 510 Series campus APs now support the following features:

- Orthogonal Frequency Division Multiple Access (OFDMA)
- ClientMatch
- Cellular modem support
- Hotspot
- Mesh

For complete technical details refer *510 Series Access Points Datasheet*. For installation instructions, refer *510 Series Access Points Installation Guide*.

Enhancements to Management Frame Protection

The management frame protection parameters in the SSID profile cannot be configured for WPA3 opmodes in the command-line interface, they are set automatically based on the opmode. Hence, the descriptions of these parameters are enhanced to indicate that they are configurable only for WPA2 opmodes.

Mute AP Radio

Starting from this release, the rf dot11a-radio-profile and rf dot11g-radio-profile commands include the am-tx-mute parameter. Enable the amtx-mute parameter to prevent an AP that operates in the AM or spectrum mode from creating spurious transmissions during AP boot. By default, the am-tx-mute is disabled.

Support for New 4G Modems

Starting from AOS-W 8.5.0.0, the following 4G modems are supported on OAW-RAPs:

- ZTE MF823 4G modem
- Huawei E8372 4G modem
- Huawei K5160 4G modem

WIDS Containment Enhancements

Air Monitor now sends tarpit or deauthentication containment frames for rogue APs and prevents clients from associating with rogue APs to mitigate possible security threats in a wireless network.

switch Platform

Support for 4G Modems on OAW-40xx Series switches

Starting from AOS-W 8.5.0.0, the following 4G modems are supported on OAW-40xx Series switches:

- ZTE MF823 4G modem
- Huawei E8372 4G modem
- Huawei K5160 4G modem

Authentication

Support for 256-bit Encryption with WPA3 Enterprise in non-CNSA Mode

AOS-W supports 256-bit encryption with WPA3 enterprise in non-CNSA mode.

Support for WPA3 and Enhanced-Open Security Enhancements on OAW-AP534, OAW-AP535, and OAW-AP555 Access Points

The OAW-AP534, OAW-AP535, and OAW-AP555 access points support the WPA3 (including the optional CNSA mode) and the optional enhanced-open security enhancements as specified in the certification programs of Wi-Fi Alliance.

802.11ax capability on ClientMatch

Starting from this release, any 802.11ax capable STAs can be matched with 802.11ax capable radios dynamically resulting in better throughput and spectral efficiency. 802.11ax clients are best compatible with 802.11ax capable radios, resulting in better throughput and spectral efficiency. When an 802.11ax client is associated with a lower radio, ClientMatch pushes the client to the best compatible 802.11ax radio for advanced capabilities. Though STA is in good health, and is 802.11ax capable, it still sometimes connects to lower radios. ClientMatch finds a potential 802.11ax radio on the same band and the client moves to the new 802.11ax radio. The **rf arm-profile** command has been modified to include the **cm-he-min-signal** parameter.

BLE

Alcatel-Lucent Sensor Value

An AP classifies and parses the content of advertisement and scan response frames and reports the BLE telemetry to subscribers.

BluConsole

AOS-W supports iOS BluConsole mobile application that allows a user to access the serial console of an AP over BLE.

Before establishing a BLE connection, the BluConsole mobile application requests user permission to pair with an AP. Bonding is not performed until the user allows permission. User is requested permission every time the BluConsole mobile application connects to an AP.

BLE Functionality

BLE functionality is enabled on AOS-W OAW-AP203H Series, OAW-AP203R Series, OAW-AP210 Series/OAW-AP 220 Series (external USB-based BLE radio), OAW-AP207 Series, OAW-AP300 Series, 510 Series, 530 Series and 550 Series FIPS APs.

Branch Office

Support for Wi-Fi Uplink

The AOS-W Uplink Manager supports Wi-Fi uplink that provides connectivity of an AP running AOS-W to an external wireless network or a managed device by using a third-party AP, such as a Mi-Fi device. This requires the Alcatel-Lucent AP running AOS-W to work as a standard Wi-Fi client.

switch-Datapath

Enhanced Visibility for Application and Datapath Health

Starting with AOS-W 8.5.0.0, the following list of new AMON messages are introduced to determine and assess the datapath CPU utilization and health.

- AMON_SOS_RES_UTIL_MESSAGE
- AMON_SOS_CPU_UTIL_STATS_MESSAGE
- AMON_SOS_DEBUG_DMA_MESSAGE
- AMON_SOS_BWM_MESSAGE
- AMON_SOS_MAINT_CNTR_MESSAGE
- AMON_SOS_CNTR_DESC_MESSAGE
- AMON_SOS_CNTR_VAL_MESSAGE

Cluster

Optimizing Cluster Load Balancing Thresholds

When any new managed device, including the managed device that comes up after a failover, is added to an existing cluster, it is considered for load balancing and accordingly, APs and clients are moved to balance the load in the cluster.

The load balancing thresholds are optimized to the following:

- **Active client rebalance threshold:** This threshold is set to 20%.
- **Standby client rebalance threshold:** This threshold is set to 40%.
- **Active AP rebalance threshold:** This threshold is set to 20%.
- **Active AP rebalance count:** The active AP rebalance count is set to 50.

- **AP total load balance threshold:** The total load balance threshold is set to 40%.

VRRP ID and Passphrase

Cluster allows users to set the starting value of VRRP ID and passphrase for a virtual IP in the cluster profile to avoid VRRP conflict in CoA. That is, Cluster VRRP members will be assigned consecutive VRRP IDs starting from the value configured.

Following parameters can be set by the user in the cluster configuration profile:

- Specify the starting VRRP ID
- Specify the VRRP passphrase for securing the VRRP session

DHCP Option 82

DHCP Option 82 Sub-option 5

DHCP option 82 sub-option 5 can be used to relay non-routeable guest network users into corporate network to obtain IP addresses.

GRE Tunnels

Configuring Tunnel Keepalives

GRE tunnel will now support ICMP based health-check feature to monitor the status of WAN reachability from remote uplink.

IoT

Reporting Sensor Values

Some sensor values are reported periodically to the configured server. The reporting interval is configured in the IoT transport profile. However, some sensor values are reported immediately without waiting for the next reporting interval. For example, events based on intrusion, fire, water level, and so on are reported immediately.

Support for Favendo Sensors

AOS-W supports Favendo sensors to provide IoT-based location services. The BLE relay process in Alcatel-Lucent AP handles telemetry streams to servers that provide location services.

Support for HanVit Sensors

AOS-W supports HanVit sensors to provide IoT-based location services. The BLE relay process in Alcatel-Lucent AP handles telemetry streams to servers that provide location services.

Support for Zigbee 802.15.4 SoluM USB Dongle

AOS-W supports Zigbee 802.15.4 SoluM USB dongles. A SoluM Zigbee 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.

IPv6

IPv6 Support for Dynamic Authorization

For configuring RFC-3576 RADIUS server, the managed device now supports IPv6 address based DAC for disconnect, session timeout, and CoA message requests, and identifies user sessions based on the user's IPv6 address.

Remote Access Points

EST Enrollment

Remote Access Points will use the Corporate DNS server to resolve DNS requests for EST enrollment.

Spectrum Analysis

Support for Spectrum Analysis on 530 Series and 550 Series Access Points

The 530 Series and 550 Series access points support spectrum analysis in both spectrum monitor and hybrid modes.

WebUI

Configuring AP Image Preload

Starting from this release, AP Image Preload can be configured by navigating to **Maintenance > Software Management** in the **Managed Network** node hierarchy.

Configuring Mobility Master Layer-3 Redundancy

Mobility Master Layer-3 redundancy can be configured by navigating to **Configuration > Redundancy >L3 Redundancy** in the **Mobility Master** node hierarchy.

Configuring Radio Resource Profile

Starting from this release, the radio resource 802.11k profile can configured by navigating to **Configuration > System > Profiles > All Profiles > Wireless LAN > 802.11k** in the **Managed Network** node hierarchy.

Configuration Support for MultiZone

MultiZone can now be configured using the WebUI by navigating to **Configuration > AP Groups > AP Group Name > MultiZone** in the **Managed Network** node hierarchy.

VIA VPN Client Authentication

The VIA connection profile now supports **EAP-GTC** authentication option that can be configured by navigating to **Configuration > System > Profiles > All Profiles > Other Profiles > VIA Connection** in the **Managed Network** node hierarchy.

WebUI Session ID

WebUI Session ID will contain a mix of uppercase, lowercase letters and numbers to prevent unauthorized intrusion into a pre-authenticated user session through brute-force attack.

WLAN SSID Profile

WLAN Ageout Refresh Direction

The refresh direction of an SSID profile for a client is bidirectional by default. Starting from AOS-W 8.5.0.0, the ageout refresh direction of SSID profile can be configured to use either bidirectional, receive-only, or transmit-only data frames.

This chapter describes the platforms supported in AOS-W 8.5.0.0.

Mobility Master Platforms

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

Table 3: *Supported Mobility Master Platforms in AOS-W 8.5.0.0*

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 AOS-W release:

Table 4: *Supported OmniAccess Mobility Controller Platforms in AOS-W 8.5.0.0*

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
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 AOS-W release:

Table 5: *Supported AP Platforms in AOS-W 8.5.0.0*

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
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325

Table 5: *Supported AP Platforms in AOS-W 8.5.0.0*

AP Family	AP Model
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
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

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 default DRT file version is part of AOS-W 8.5.0.0:

- DRT-1.0_70076

Chapter 5
Resolved Issues

This chapter describes the issues resolved in AOS-W 8.5.0.0.

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-127536 AOS-136297 AOS-136925 AOS-137646 AOS-182194	154286 165482 166256 167120	**Symptom:** Clients lost wireless connectivity randomly. As a result, buffer allocation failure increased. The fix ensures that the wireless connectivity to the clients is steady and connected at all times. **Scenario:** This issue was observed in APs running AOS-W 8.0.0.0 or later versions in a master-standby topology.	switch-Datapath	All platforms	AOS-W 8.0.0.0
AOS-129107 AOS-146556 AOS-146683 AOS-147450 AOS-147541 AOS-147618 AOS-147743 AOS-148047 AOS-148154 AOS-150880 AOS-158210 AOS-158618	156245 179056 180324 180464 180594 180774 181215 181366 183219 184967 195117 195656	**Symptom:** The status of an AP was displayed as **DOWN** in the WebUI but displayed as **UP** when the **show ap database long** command was executed. The fix ensures that the status of the AP is displayed correctly in the WebUI and command-line interface. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.0.	AP Platform	All platforms	AOS-W 8.4.0.0
AOS-136651	165908	**Symptom:** A Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Control Processor Kernel Panic**. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred because of a softlock. This issue was observed in Mobility Masters running AOS-W 8.1.0.2 or later versions. **New Duplicates:** AOS-185700, AOS-185346, AOS-183067, AOS-182050, AOS-158026, , AOS-156881, AOS-156569, AOS-153358, AOS-152641, AOS-152535, AOS-152349, AOS-151349, AOS-149849, AOS-148015, AOS-147717, AOS-147592, AOS-146130, AOS-145643, AOS-145491, AOS-145264, AOS-143656, AOS-143582, AOS-143172, AOS-143136, , AOS-142405, AOS-140614, AOS-140008, AOS-157396 **Old Duplicates:** , 170224, 171074, 171396, 173372, 174322, 174370, 174917, 175009, 177151, 177457, 177662, 178307, 180558, 180741, 181173, 183588, 185596, 186993, 187232, 187418, 188367, 193202, 193903 and 194859	switch-Platform	All platforms	AOS-W 8.1.0.2

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-136899 AOS-138540 AOS-144429 AOS-144507 AOS-185841	166228 168270 175990 176096	**Symptom:** The **mDNS** process in a managed device was unresponsive and the managed device showed high CPU utilization. The fix ensures that the **mDNS** process works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0.	AirGroup	All platforms	AOS-W 8.0.0.0
AOS-137345 AOS-156729	166773 193017	**Symptom:** The **profmgr** process in a Mobility Master crashed unexpectedly. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred when the device configuration settings were replaced with new configuration settings. This issue was observed in Mobility Masters running AOS-W 8.0.1.0 or later versions.	Configuration	All platforms	AOS-W 8.0.1.0
AOS-138525 AOS-182893	168251	**Symptom:** The WebUI displayed the details of a standby switch even when the redundancy configuration on the active Mobility Master was deleted. The fix ensures that the WebUI does not display the details of the deleted switch. **Scenario:** This issue occurred when the master-redundancy configuration was removed completely from either the command-line interface or the WebUI. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	Configuration	All platforms	AOS-W 8.2.0.0
AOS-138677	168457	**Symptom:** The license count in **Mobility Master > Licenses page** page of the WebUI did not reflect the ACR license usage. The fix ensures that the WebUI reflects the license count. **Scenario:** This issue occured when the license count was not communicated to the applications running on Standby Mobility Master. This issue was observed in Mobility Master running AOS-W 8.2.0.0 or later versions.	Licensing	All platforms	AOS-W 8.2.0.0
AOS-140742 AOS-148350	170839 177178 180034 189649	**Symptom:** The output of the **show ap monitor ap-list** command displayed corrupt SSID information for an AP. The fix ensures that the AP does not process the corrupt packets and displays the correct SSID. **Scenario:** This issue occurred when the AP tried to process some corrupt packets. This issue was observed in OAW-AP325 access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP325 access points	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-140806 AOS-157745	171339 194445	**Symptom:** A managed device rebooted with the initial device configuration although the updated configuration was available in the Mobility Master. The fix ensures that the managed device is updated with the configuration changes in the Mobility Master. **Scenario:** This issue was observed in managed devices running AOS-W 8.1.0.4 or later versions in a Mobility Master-Managed Device topology in a multi-version deployment.	Configuration	All platforms	AOS-W 8.1.0.4
AOS-141552 AOS-150776 AOS-155236	172339 184826 190869	**Symptom:** Active APs were not displayed in the **Dashboard > Access Points** page in the WebUI. The fix ensures that the active APs are displayed in the WebUI. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.3 or later versions.	Configuration	All platforms	AOS-W 8.3.0.3
AOS-143093 AOS-157338	174267 193794	**Symptom:** A VIA client was unable to establish VPN tunnel with the managed device. The log file listed the reason for the event as **Dropping VPN session because we have exceeded the VPN license-limit of 4096**. This issue is resolved by not incrementing the VPN license count for VPN tunnels. **Scenario:** This issue occurred when the VPN license was incorrectly incremented. This issue was observed in managed devices running AOS-W 8.0.0.0.	IPsec	All platforms	AOS-W 8.0.0.0
AOS-143134 AOS-158329	173924 174100 174320 175992 176293 177665 178689 179464 181469 187116	**Symptom:** An AP did not support fast recovery. This issue is resolved by adding support for fast recovery in the AP. **Scenario:** 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.	AP-Wireless	OAW-AP303H, OAW-AP305, OAW-AP315, OAW-AP325 , and OAW-AP335 access points	AOS-W 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-144329 AOS-152686 AOS-157335	175881 187479 193791	**Symptom:** The **datapath** process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when the IPv6 header length was not considered during IPv6 packet reassembly. This issue was observed in managed devices running AOS-W 8.2.2.3.	switch-Datapath	All platforms	AOS-W 8.2.2.3
AOS-145323 AOS-156161	177236 192313	**Symptom:** Incorrect user count was displayed when the **show global_user_table** command was executed. However, the correct user count was displayed in the WebUI dashboard. The fix ensures that the correct user count is displayed. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.3.0.0
AOS-145737 AOS-183813	177788	**Symptom:** A client experienced a slow network or network connectivity issue although the number of sessions in the AP did not reach the maximum value. The fix ensures that clients get a better network experience. **Scenario:** This issue was observed in OAW-AP315 access points running AOS-W 8.0.0.0.	AP Datapath	OAW-AP315 access points	AOS-W 8.0.0.0
AOS-146144 AOS-152880 AOS-154088 AOS-155582 AOS-156758 AOS-157371	178324 187744 189352 191419 193052 193868	**Symptom:** APs were rebooting randomly. The log files for the event listed the reason as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when EIRP table was not sent to the AP when either 2G or 5G channel list was empty. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AP regulatory	All platforms	AOS-W 8.3.0.0
AOS-146322 AOS-148352 AOS-151203 AOS-151296 AOS-151376 AOS-151817 AOS-153999 AOS-155288 AOS-157690 AOS-157995 AOS-184617	178564 181633 185403 185528 185629 186229 189219 190944 194367 194811	**Symptom:** A Mobility Master Virtual appliance crashed unexpectedly due to a memory corruption. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.1.0.0 or later versions.	Logging	All platforms	AOS-W 8.1.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146331 AOS-183502 AOS-184796 AOS-185200	178574	**Symptom:** The **datapath** process in a switch crashed and rebooted unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in OAW-4850 switches running AOS-W 8.3.0.0 or later versions.	switch Datapath	OAW-4850 switches	AOS-W 8.3.0.0
AOS-146612 AOS-146617	178963 178968	**Symptom:** A client got deauthenticated by an AP after the channel was changed from non-DFS channel to DFS channel. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP345 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP345 access points	AOS-W 8.3.0.0
AOS-146616 AOS-147492	178967 180383	**Symptom:** A client was deauthenticated unexpectedly. The log file listed the reason for the event as **UAC down**. This issue is resolved by allowing the AP to send the initial hello message to the UAC three times. **Scenario:** This issue occurred when the response from a UAC to an AP for the initial hello message did not reach the AP. This issue was observed in managed devices running AOS-W 8.2.1.0 in a cluster topology.	Station Management	All platforms	AOS-W 8.2.1.0
AOS-146624 AOS-155236	178976 190869	**Symptom:** Active APs were not displayed in the **Dashboard > Access Points** page in the WebUI. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.3 or later versions.	Configuration	All platforms	AOS-W 8.3.0.3
AOS-146670 AOS-157311 AOS-182295	179034 193759	**Symptom:** Clients experience poor performance with OAW-AP300 Series access points. Enhancements to the wireless driver has resolved this issue. **Scenario:** The issue occured in OAW-AP300 Series access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.0.0.0
AOS-147036 AOS-155499 AOS-158129 AOS-158444	179623 191227 195002 195448	**Symptom:** A Mobility Master crashed and rebooted unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20).** The fix ensures that the Mobility Master works as expected. **Scenario:** This issue occurred because of a race condition while upgrading the hardware caches. This issue was observed in Mobility Master running AOS-W 8.4.0.0 or later versions.	switch Datapath	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-147039 AOS-156717	179627 193004	**Symptom:** The **FPAPPs** process was stuck in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when the initial full-setup wizard was used to switch a OAW-4450 switch that was running in stand-alone mode to a managed device and an invalid netmask was added. This issue was observed in OAW-4450 switches running AOS-W 8.2.1.0.	L2 Forwarding	OAW-4450 switches	AOS-W 8.2.1.0
AOS-147120	179786	**Symptom:** A managed device denied Wi-Fi calling when the deny_ amat_internal netdestination ACL was added above the voip-applications-acl ACL. This issue is resolved by adding the AppRF-based ACL before any deny ACL. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.2.	UCC	All platforms	AOS-W 8.2.0.2
AOS-147186 AOS-152832 AOS-153857 AOS-155657 AOS-155875 AOS-157746 AOS-182979 AOS-184932 AOS-184932	179873 182372 182612 187365 187691 189031 189590 189886 191516 191806 191814 192933 194228 194446 195207 195472	**Symptom:** Clients were unable to resolve ARP requests. The fix ensures that the clients are able to resolve ARP requests. **Scenario:** This issue occurred because the AP memory utilization rate was high, leading to drop in client traffic. This issue was observed in access points running AOS-W 8.3.0.0.	AP Datapath	All platforms	AOS-W 8.3.0.0
AOS-147232 AOS-158495 AOS-184142	179942 195511	**Symptom:** 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 User Anchor Controller (UAC) and the clients are able to send or receive traffic to or from the AP. **Scenario:** This issue occurred when the station management process in an AP sent a PAPI message to the AP Anchor Controller (AAC) instead of the UAC. This issue was observed in a cluster topology running AOS-W 8.2.1.0 with 802.11r enabled.	Station Management	All platforms	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-147511	180406	**Symptom:** A client received IPv6 router advertisements randomly from different VLANs. The fix ensures that the client receives router advertisement on its derived vlan. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	IPv6	All platforms	AOS-W 8.2.1.0
AOS-147702 AOS-182669 AOS-183922	180722	**Symptom:** A switch displayed high memory utilization. This issue is resolved by displaying the correct memory utilization and available memory. **Scenario:** This issue occurred when a switch displayed a lower value for available memory than free memory. This issue was observed in OAW-4010 switches running AOS-W 8.2.1.0	switch-Platform	All platforms	AOS-W 8.2.1.0
AOS-148264 AOS-153070 AOS-155566 AOS-183668	181536 188000 191385	**Symptom:** APs were not broadcasting SSID and multiple radio resets were observed. The fix ensures that the ARM or AirMatch changes the channel immediately after a radar notification is received. **Scenario:** This issue occurred as the ARM or AirMatch unable to change the channel when a radar notification was received. This issue was observed in access points running AOS-W 8.2.0.0 or later versions.	ARM	All platforms	AOS-W 8.2.0.0
AOS-148675 AOS-158300	182073 195240	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT: rcRateFind+229;ratectrl_11ac.c:2394.** Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred while the driver tried to parse the opcode notification from a client that is not yet associated to the AP. This issue was observed in OAW-AP305 and OAW-AP315 access points running AOS-W 8.2.1.0 or later versions.	AP-Wireless	OAW-AP305 and OAW-AP315 access points	AOS-W 8.2.1.0
AOS-149092 AOS-157746	182612 194446	**Symptom:** A client was unable to resolve ARP requests. The fix ensures that the clients are able to resolve ARP requests. **Scenario:** This issue occurred because the AP memory utilization rate was high, leading to drop in client traffic. This issue was observed in access points running AOS-W 8.3.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-149433 AOS-155617 AOS-154112 AOS-157342	183072 189384 191463 193798	**Symptom:** A managed device 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 a managed device processes the FTP traffic and works as expected. **Scenario:** This issue occurred when FTP traffic was sent to a managed device. This issue was observed in managed devices running AOS-W 8.3.0.5.	switch-Datapath	All platforms	AOS-W 8.3.0.5
AOS-149983 AOS-153622	183788 188706	**Symptom:** Some APs that were listed in the output of the **show ap database** command were not displayed in the WebUI. The fix ensures that the correct list of APs is listed in the output of the **show ap database** command and the WebUI. **Scenario:** This issue occured when: ■ an AP was deleted on the Mobility Master because of a conflict between GSM add or delete events coming from two different managed device that are cluster members. ■ an AP was deleted by a managed device that is not the active managed device for that AP. This issue was observed managed devices running AOS-W 8.3.0.0 in a cluster topology.	AP-Platform	All platforms	AOS-W 8.3.0.0
AOS-150041 AOS-154398	183866 189730	**Symptom:** A client did not connect to the SSID after the managed device was upgraded from AOS-W 8.0.0.0. The fix ensures that the country code is added to the beacon frames for the 2.5 GHz radio. For the 5 GHz radio, enable 802.11k so that the country code information is present in the beacon frames of SSIDs that are broadcasted using the non-DFS channels. **Scenario:** This issue occurred because the country code information was not in the beacon frames. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	switch-Platform	All platforms	AOS-W 8.0.0.0
AOS-151275	185499	**Symptom:** Managed devices at the branch office are unable to receive IP address from the branch uplink pool. The fix ensures that the managed devices receive IP address from the branch uplink pool. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions.	IPsec	All platforms	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-149433 AOS-154112 AOS-155617 AOS-157342 AOS-158217	189384 183072 191463 193798 195126	**Symptom:** The datapath process in a managed device crashed and rebooted unexpectedly. The fix ensures that the datapath process works as expected. **Scenario:** This issue occured when a client sends FTP traffic and NAT is applied. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	DPI	All platforms	AOS-W 8.3.0.0
AOS-150797	184849	**Symptom:** Clients were unable to make or receive calls. A **Network busy** error message is displayed. The fix ensures that the clients are able to make or receive calls. **Scenario:** This issue occurred when WMM was disabled on the managed device. This issue is observed in OAW-AP315 access points running AOS-W 8.2.1.1.	WMM	OAW-AP315 access points	AOS-W 8.2.1.1
AOS-151880 AOS-155002 AOS-179663	186310 190526 185931	**Symptom:** An AP sent multicast traffic to clients at a lower rate. This issue is resolved by updating the rate table entry for the multicast traffic to the correct rate. **Scenario:** This issue occurred when **bcmc-optimization** was enabled and DMO was disabled. This issue was observed in OAW-AP303P and OAW-AP515 access points running AOS-W 8.4.0.0.	AP-Wireless	OAW-AP303P and OAW-AP515 access points	AOS-W 8.4.0.0
AOS-152427 AOS-153919	187098 189112	**Symptom:** A Mobility Master recorded high CPU utilization rate and affected services. This issue is resolved by optimizing the DNS lookup. **Scenario:** This issue occurred when a large number of netdestinations with name-based entries were configured on a Mobility Master. These netdestination names were resolved to the DNS IP address which in turn retained the firewall DNS names and led to high CPU utilization. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.0.0.0
AOS-153169 AOS-184045 AOS-184530	188130	**Symptom:** AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: softlockup: hung tasks**. The fix ensures that only 32 packets are processed in one batch. **Scenario:** This issue occurred because the firewall processed too many packets in one batch. This issue was observed in OAW-AP303H access points running AOS-W 8.3.0.1 or later versions.	AP Datapath	OAW-AP303H access points	AOS-W 8.3.0.1

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-153188 AOS-183906	188152	**Symptom:** The AP_INFO AMON message of an AP provided incorrect and outdated information on **opmode**, **ap_model**, **ap_uptime**, and **lms_ip** parameters. The issue was resolved by not forwarding AMON messages on the UAC. **Scenario:** This issue was observed in OAW-AP345 access points running AOS-W 8.3.0.0 or later versions.	AP-Platform	OAW-AP345 access points	AOS-W 8.3.0.0
AOS-153348 AOS-156975 AOS-182581	188356 193317	**Symptom:** Clients reconnected to the AP frequently as the effective rates and advertised rates were not the same. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in 510 Series access points running AOS-W 8.4.0.0 or later versions.	AP-Wireless	510 Series access points	AOS-W 8.4.0.0
AOS-153533 AOS-179571 AOS-181276 AOS-181402 AOS-184537	188590 185520 192894 193585	**Symptom:** Incorrect memory corruption was detected during fast recovery process of an AP. Enhancements to wireless driver resolved the issue. **Scenario:** This issue occurred when an AP crashed and rebooted unexpectedly due to a kernel panic. This issue was observed in OAW-AP305 access points running AOS-W 8.3.0.0 or later versions	AP-Wireless	OAW-AP305 access points	AOS-W 8.3.0.0
AOS-153839	189012	**Symptom:** License synchronizing message, **Status: Error, License syncing is already in progress, please try later**, was displayed as an error instead of a warning or an information. The fix ensures that the status is displayed as **Status: License syncing is already in progress, please try later** instead of an error. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.4.0.0.	Licensing	All platforms	AOS-W 8.4.0.0
AOS-153844	189017	**Symptom:** 802.11b clients were unable to pass traffic. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP305 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP305 access points	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154188 AOS-154532 AOS-154830 AOS-154935 AOS-155110 AOS-155535 AOS-155852 AOS-155931 AOS-155938 AOS-155940 AOS-155941 AOS-156258 AOS-156922 AOS-156934 AOS-156984 AOS-157656	189486 189904 190298 190450 190674 191271 191783 191880 191887 191889 191890 192340 193253 193265 193327 194309	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2**). The fix ensures that the managed device works as expected. **Scenario:** This issue occurred in a cluster setup when an IPv6 client initiated and stopped multiple FTP transfers. This issue was observed in OAW-4x50 Series controllers running AOS-W 8.3.0.2 or later versions.	switch-Datapath	OAW-4x50 Series switches	AOS-W 8.3.0.2
AOS-154221 AOS-158240	189523 191049	**Symptom:** An AP that terminated on a managed device with CPsec enabled did not come up after a cluster failover. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when a cluster failover message timed out in the AP after a cluster failover. This issue was observed in access points running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0
AOS-154324	189646	**Symptom:** The Fing mobile application discovered a connected client although the deny-inter-user-traffic and deny-inter-user-bridging was enabled. This issue is resolved by denying ARP packet request when BCMC optimization is enabled and untrusting both the ingress and egress traffic when either deny-inter-user-traffic or deny-inter-user-bridging is enabled. **Scenario:** This issue occurred when BCMC optimization was enabled in a managed device and the Fing mobile application sent an ARP packet to all the IP addresses in a subnet. This issue was observed in managed devices running AOS-W 8.0.0.0	Multicast	All platforms	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154564 AOS-155770 AOS-156549	189952 192768 191667	**Symptom:** The **SNMP** process crashed on a switch unexpectedly. The fix ensures that the **SNMP** process works as expected. **Scenario:** This issue was observed in OAW-4650 series switch running AOS-W 8.2.1.1 or later versions.	SNMP	All platforms	AOS-W 8.2.1.1
AOS-154665	190094	**Symptom:** A client connected to an AP displayed low signal strength. The fix ensures that an error message is displayed where it confirms that the Front End Module (FEM) is defective. **Scenario:** This issue occurred in OAW-AP340 Series access points running AOS-W 8.3.0.3 or later versions.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.3
AOS-154735	190181	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: softlockup: hung tasks**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP203H access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP203H access points	AOS-W 8.3.0.0
AOS-154973 AOS-155578	190491 191415	**Symptom:** APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: Fatal exception at worker_thread+0x1ec/0x3f8**. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP303H and OAW-AP305 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP303H and OAW-AP305 access points	AOS-W 8.2.0.0
AOS-155015 AOS-182098	190542	**Symptom:** A radio experienced a high number of resets in APs. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the APs were in Air Monitor mode. This issue was observed in OAW-AP335 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP335 access points	AOS-W 8.3.0.0
AOS-155272 AOS-157838	190922 194576	**Symptom:** A managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred because of authentication failure. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155570 AOS-157636 AOS-182455	191405 194286	**Symptom:** A switch returned error message: **Country Code file creation failed** when saving configuration. The fix ensures that the switch works as expected. **Scenario:** This issue occured during the initial setup of the switch because of an attempt to create the country code file in a directory that did not exist. This issue was observed in switches running AOS-W 8.4.0.0 or later versions.	switch-Platform	All platforms	AOS-W 8.4.0.0
AOS-155627 AOS-155881	191480 191822	**Symptom:** Mesh APs did not have licenses and the log files displayed a no mesh license error message on the managed device. The **show license client-table** command output also displayed an incorrect value for used licenses. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0
AOS-157075	193445	**Symptom:** A user was unable to view the list of AirGroup servers in the WebUI. The fix ensures that the list of AirGroup servers is available in the WebUI. **Scenario:** This issue occurred when a client connected to an AP and moved to another AP. This issue was observed in OAW-4750 switches running AOS-W 8.2.0.0 or later versions.	AirGroup	OAW-4750 switches	AOS-W 8.2.0.0
AOS-157767 AOS-155877 AOS-184056	191816	**Symptom:** 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. **Scenario:** This issue was observed in OAW-40xx Series and OAW-4x50 Series switches running AOS-W 8.2.2.0 or later versions.	switch-Platform	OAW-40xx Series and OAW-4x50 Series switches	AOS-W 8.2.2.0
AOS-155987 AOS-157010	191958 193361	**Symptom:** The **ap_name** field appeared blank in **reporting_radio**, **radio_history**, and **ap_info collection** parameters. The fix ensures that the correct **ap_name** field is displayed. **Scenario:** This issue was observed in APs running AOS-W 8.3.0.3 or later versions.	AirMatch	All platforms	AOS-W 8.3.0.3

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156079	192111	**Symptom:** The **Disassociation Timer** value of 802.11v BSS Transition Management Request was incorrect. The fix ensures that the **Disassociation Timer** value is set to the default value of 100. **Scenario:** This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.4.0.0 or later versions.	ARM	All platforms	AOS-W 8.4.0.0
AOS-156080 AOS-182758	192112	**Symptom:** 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. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.2.	Web Server	All platforms	AOS-W 8.2.2.2
AOS-156104 AOS-156587 AOS-178581 AOS-180782	192143 192814 180455 191142	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP207 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP207 access points	AOS-W 8.3.0.0
AOS-156162 AOS-158131	192223 195005	**Symptom:** Managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **dds process died**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when the pre-shared key was not configured while enabling HA with state sync feature. This issue was observed in managed devices running AOS-W 8.3.0.3 or later versions.	HA-Lite	All platforms	AOS-W 8.3.0.3
AOS-156267 AOS-158169	192349 195066	**Symptom:** The **mDNS** process in a managed device consumed more memory than the typical threshold limit. This issue is resolved by avoiding memory leak in the **mDNS** process. **Scenario:** This issue occurred because of a memory leak in the **mDNS** process. This issue is observed in managed devices running AOS-W 8.2.2.0 or later versions.	AirGroup	All platforms	AOS-W 8.2.2.0
AOS-156646 AOS-157540	192901 194140	**Symptom:** APs were unable to connect to the managed device. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in OAW-AP370 series access points running AOS-W 8.2.0.0 or later versions.	AP-Platform	OAW-AP370 series access points	AOS-W 8.2.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156834 AOS-158306	193152 195249	**Symptom:** Cluster manager process crashed frequently on a managed device. The fix ensures that managed devices work as expected in a cluster setup. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.2 in a cluster setup.	Cluster-manager	All platforms	AOS-W 8.3.0.2
AOS-156838	193158	**Symptom:** User was unable to reprovision an AP. This issue is resolved by keeping the original characters and not converting them to a different format. **Scenario:** This issue occurred when a special character in a German keypad is used in the AP name. This issue is observed in APs connected to managed devices running AOS-W 8.2.2.1.	Configuration	All platforms	AOS-W 8.2.2.1
AOS-156839 AOS-157104	193159 193492	**Symptom:** The output of the **show aaa authentication-server radius statistics** command displayed incorrect data for **ExpAuthTm**, **Uptime**, and **SEQ** columns. The fix ensures that the correct data is displayed for these columns. **Scenario:** This issue occurred when the RADIUS server did not send any request to the managed device. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.4.0.0
AOS-156874 AOS-156918 AOS-157515	193195 193249 194093	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file 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 works as expected. **Scenario:** This issue was observed in OAW-4750XM switches running AOS-W 8.2.2.0 or later versions.	switch-Datapath	OAW-4750XM switches	AOS-W 8.2.2.0
AOS-157024	193378	**Symptom:** The **all deviceClass** filter is applied by default to an IoT transport profile and when this filter is removed, it is not saved in configuration on the managed device. **Scenario:** This issue occurs when a **Telemetry-HTTPS or Telemetry-Websocket** IoT transport profile is created. This issue is observed in managed devices running AOS-W 8.4.0.0 in Mobility Master-Managed Device topology	BLE	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157049 AOS-185234	193416	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Halt reboot (Intent:cause:register 38:86:50:2)**. The fix ensures that the switch works as expected. **Scenario:** This issue occurred when the **halt** command was executed on the switch. This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions.	Controller-Platform	All platforms	AOS-W 8.3.0.0
AOS-157056	193423	**Symptom:** The **authentication** process in a managed device crashed and the APs rebooted. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when an existing bridge-forwarding mode client joined as a split-tunnel-mode client. This issue was observed in managed devices running AOS-W 8.2.1.0.	Base OS Security	All platforms	AOS-W 8.2.1.0
AOS-157071	193441	**Symptom:** The **Station Management** process crashed continuously in the managed device because the database upgrade in a managed device failed. This issue is resolved by ensuring that a database upgrade is triggered when boot partition is changed. **Scenario:** This issue occurred when a managed device running AOS-W 8.4.0.0 version was downgraded to AOS-W 8.3.0.0 or lower versions, and then the **ap gap-db reinit-db** command was executed. Post this, the managed device was again upgraded to AOS-W 8.4.0.0 by changing the boot partition. This issue is observed in managed devices running AOS-W 8.4.0.0.	Database	All platforms	AOS-W 8.4.0.0
AOS-157162 AOS-183803 AOS-184508	193561	**Symptom:** 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: ■ **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. **Scenario:** This issue occurred when the AP channel updates were not registered with **STM** process. This issue was observed in managed devices running AOS-W 8.2.2.3 or later versions.	Cluster-Manager	All platforms	AOS-W 8.2.2.3

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157155	193553	**Symptom:** The NTP server failed to synchronize after upgrading the managed devices to AOS-W 8.3.0.0 version. The fix ensures that the NTP server synchronizes with the managed device. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	VLAN	All platforms	AOS-W 8.3.0.0
AOS-157233	193662	**Symptom:** Device model name was displayed incorrectly in the **Dashboard > Controllers > Model** page in the WebUI. The fix ensures that the device model name is displayed correctly. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	VRRP	All platforms	AOS-W 8.2.2.0
AOS-157288	193726	**Symptom:** The **show ap arm state** command returned results in XML format instead of JSON format when accessing the switch through REST API. Enhancements to REST API has resolved this issue. **Scenario:** This issue was observed in switches running AOS-W 8.2.1.0 or later versions.	ARM	All platforms	AOS-W 8.2.1.0
AOS-157293	193731	**Symptom:** The **preserve-vlan** parameter of the **wlan virtual-ap** command did not work as expected. The fix ensures that the **preserve-vlan** parameter will allows the clients to retain their previous VLAN assignment if the clients disassociate and re-associate to the same or a different AP. **Scenario:** This issue was observed in Mobility Master running AOS-W 8.2.2.2 or later versions.	Station Management	All platforms	AOS-W 8.2.2.2
AOS-157356	193833	**Symptom:** The **firewall dns-name cache** command filled up and caused service interruptions. This issue is resolved by automatically clearing the IP address list entries every 24 hours. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0	switch-Datapath	All platforms	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157348 AOS-157458	193815 194006	**Symptom:** The output of the **show license server-table** command displayed incorrect count of used licenses for APs. As a result, the APs failed to boot and went into inactive and unlicensed state. The fix ensures that the correct license count is displayed and the APs work as expected. **Scenario:** This issue occurred when the centralized licensing server incorrectly added the licenses from standby Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions in a master-standby topology.	Licensing	All platforms	AOS-W 8.2.0.0
AOS-157563 AOS-158459	194178 195465	**Symptom:** A 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 51:86:50:4).** The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.1 or later versions.	switch Datapath	All platforms	AOS-W 8.2.1.1
AOS-157606	194237	**Symptom:** A management user was unable to login to the managed device by authenticating through a Radius server. This issue is resolved by retrieving the current NAS-Port-type from the managed device at the start of the authentication process. **Scenario:** This issue occurred when the NAS-Port-type was changed to ASYNC from VIRTUAL. This issue was observed in managed devices running AOS-W 8.3.0.3 or earlier versions.	Radius	All platforms	AOS-W 8.3.0.3
AOS-157654	194307	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP215 access points running AOS-W 8.2.2.2.	SDN	OAW-AP215 access points	AOS-W 8.2.2.2
AOS-157770	194484	**Symptom:** The managed devices sent TACACS login request using the OSPF IP address instead of the loopback IP address. The fix ensures that the managed device sends the TACACS login requests using the loopback IP address. **Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.0.	TACACS	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157797 AOS-158350 AOS-158521	194518 195313 195540	**Symptom:** The **mDNS** process in a managed device was in a non-responsive state. This issue is resolved by deleting and relearning the client details with the properties of the new island when a client roams between islands. **Scenario:** This issue occurred when AirGroup was enabled in an island topology and a client roamed across islands. This issue was observed in managed devices running AOS-W 8.2.2.3.	AirGroup	All platforms	AOS-W 8.2.2.3
AOS-157815 AOS-158647	195690 194552	**Symptom:** VOIP phones did not get ARP broadcasts randomly as the STM process was deleting existing VLANs from the tunnel. The fix ensures that the STM process does not delete VLANs from the tunnel when an update is received for a user from authentication server with initial VLAN and assigned VLAN. **Scenario:** This issue occurred when tunneled node was configured on the managed device. This issue was observed in managed devices running AOS-W 8.2.2.3 or later versions.	Tunnel-node-manager	All platforms	AOS-W 8.2.2.3
AOS-156788 AOS-157820	193096 194558	**Symptom:** An AirGroup user was unable to discover Chromecast devices. This issue is resolved by allowing an AirGroup user to discover Chromecast devices irrespective of the case used in the AirGroup server name. **Scenario:** This issue occurred because the AirGroup server name was case sensitive. This issue was observed in managed devices running AOS-W 8.0.0.0.	AirGroup	All platforms	AOS-W 8.0.0.0
AOS-158157	195039	**Symptom:** AP groups created below the managed network heirarchy did not appear in the **AP group** drop-down list box in the **Managed Network > Configuration > Access Points > Whitelist > Campus AP Whitelist > Add New Campus AP whitelist** page of the WebUI. Enhancements to the WebUI has resolved this issue. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	WebUI	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-158180 AOS-158565 AOS-182719 AOS-183629 AOS-184955 AOS-185312 AOS-185342	195080 195592	**Symptom:** The AP licenses were falsely utilized in a mesh setup. The fix ensures that mesh releases relevant licenses instead of consuming the existing ones. **Scenario:** This issue occurred when the existing mesh point consumed licenses during reboot and when there was a radar detection. This issue was observed in managed devices running AOS-W 8.2.2.3 or later versions.	AP-platform	All platforms	AOS-W 8.2.2.3
AOS-158207	195111	**Symptom:** An incorrect redirected URL was displayed during an external captive portal authentication. The fix ensures that the correct redirected URL is displayed on the captive portal page. **Scenario:** This issue was observed in OAW-AP205 access points running AOS-W 8.2.0.0 or later versions.	Captive Portal	OAW-AP205 access points	AOS-W 8.2.0.0
AOS-158227	195138	**Symptom:** A few OAW-AP225 showed inconsistent EIRP values for 2.4 GHz radio. The fix ensures that the correct EIRP values are displayed. **Scenario:** This issue was observed in OAW-AP225 running AOS-W 8.2.0.0 or later versions.	AP- Wireless-2xx	OAW-AP225 access points	AOS-W 8.2.0.0
AOS-158254 AOS-184144	195177	**Symptom:** Some managed devices dropped ARP packets while trying to route traffic to a specific hop IP address. The fix ensures that the managed devices work as expected. **Scenario:** This issue occurred when policy-based routing picked the incorrect next-hop destination address to route the packets. This issue was observed in managed devices running AOS-W 8.4.0.0 in a Mobility Master-Managed Device topology.	Policy-Based Routing	All platforms	AOS-W 8.4.0.0
AOS-158274	195201	**Symptom:** The Override icon in the **WPA passphrase** and **Retype** fields in **Configuration > System >Profiles > SSID profile** still appeared even after manually entering the passphrase and enabling “Remove Override”. The fix ensures that the override icon does not appear in the password fields across the WebUI. **Scenario:** This issue was observed in Mobility Master running AOS-W 8.4.0.0 or later versions.	WebUI	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-158311	195264	**Symptom:** A managed device did not prompt an error or show restriction when configuring a VRRP authentication key. The fix ensures that an error is displayed if a VRRP authentication key is configured with more than 8 characters. **Scenario:** This issue occurred when the VRRP authentication key contained more than 8 characters. This issue was observed in managed devices running AOS-W 8.2.1.0.	VRRP	All platforms	AOS-W 8.2.1.0
AOS-158360	195329	**Symptom:** Managed device crashed unexpectedly. The log file for the event listed the reason as **kernel panic**. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	switch-Platform	All platforms	AOS-W 8.3.0.0
AOS-158455	195461	**Symptom:** The output of the **show configuration system-commands pending** command displayed committed configuration details instead of pending configuration details. The fix ensures that the command displays the pending configuration details. **Scenario:** This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.2.1.0 or later versions.	switch-Platform	All platforms	AOS-W 8.2.1.0
AOS-158599 AOS-182977	195633	**Symptom:** Mobility Master crashed and rebooted unexpectedly. The log file lists the reason for the event as, **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4).** The fix ensures that theMobility Master works as expected. **Scenario:** This issue was observed in Mobility Master rrunning AOS-W 8.2.0.0 or later versions.	switch- Datapath	All platforms	AOS-W 8.2.0.0
AOS-158603	195637	**Symptom:** Some APs failed to come up on the managed device. The fix ensures that the AP functions as expected. **Scenario:** This issue occurred when the managed devicewas upgraded from AOS-W 8.3.0.4 to AOS-W 8.4.0.0. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-181953	—	**Symptom:** Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:2)**. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in Mobility Master running AOS-W 8.3.0.4 or later versions.	switch Datapath	All platforms	AOS-W 8.3.0.4
AOS-181971	—	**Symptom:** APs experienced PSM watchdog timeouts every few seconds. The fix ensures that traffic test does not cause PSM watchdog timeouts. **Scenario:** This issue occurred when a traffic test was conducted on clients running DDMO converted video streams. This issue was observed in 510 Series access points running AOS-W 8.4.0.1 or later versions.	AP-Wireless	510 Series access points	AOS-W 8.4.0.1
AOS-182023	—	**Symptom:** The **Dashboard** page in the WebUI displayed the **A controller is required for information to be displayed** error message. The fix ensures that the **Dashboard** page does not display the error message. **Scenario:** This issue was observed in Mobility Master running AOS-W 8.2.1.0 or later versions.	Configuration	All platforms	AOS-W 8.2.1.0
AOS-182091 AOS-183253 AOS-183255 AOS-184627	—	**Symptom:** The **mDNS** process in a managed device crashed and the managed device rebooted unexpectedly. The fix ensures that the **mDNS** process works as expected. **Scenario:** This issue was observed in Mobility Master running AOS-W 8.2.1.0 or later versions.	AirGroup	All platforms	AOS-W 8.3.0.4
AOS-182911	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP300 Series access points running AOS-W 8.3.0.4 or later versions.	AP-Wireless	OAW-AP300 Series access points	AOS-W 8.3.0.4
AOS-182928 AOS-183355	—	**Symptom:** A switch crashed unexpectedly. The fix ensures that the **mDNS** process does not leak memory and the switch works as expected. **Scenario:** This issue occurred because the **mDNS** process in the switch leaked memory. This issue was observed in OAW-4750 switches running AOS-W 8.3.0.0.	AirGroup	OAW-4750 switches	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-182929	—	**Symptom:** The PIM module in OAW-4x50 Series switch crashed unexpectedly. Enhancements to the PIM module has resolved this issue. **Scenario:** This issue occurred due to a condition of dangling reference. This issue was observed in OAW-4x50 Series switches running AOS-W 8.2.2.3 or later versions in a Mobility Master - Managed Device topology with clustering and IGMP enabled.	PIM-SM	OAW-4x50 Series switches	AOS-W 8.2.2.3
AOS-183023 AOS-185198 AOS-185429	—	**Symptom:** A client was unable to view AirGroup servers in a centralized AirGroup deployment. The fix ensures that the client is able to view AirGroup servers. **Scenario:** This issue occured because of an error in the policy lookup. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AirGroup	All platforms	AOS-W 8.4.0.0
AOS-183148 AOS-183454 AOS-183782 AOS-184700 AOS-185163	—	**Symptom:** Some APs 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. **Scenario:** This issue was observed in OAW-AP214, OAW-AP215, and OAW-AP315 access points running AOS-W 8.0.0.0 or later versions.	AP-Platform	OAW-AP214, OAW-AP215, and OAW-AP315 access points	AOS-W 8.0.0.0
AOS-183227 AOS-185109	—	**Symptom:** The **ip-session access-list** rule were not getting pushed from a managed device to the Mobility Master. The fix ensures that the **ip-session access-list** rules get pushed. **Scenario:** This issue was observed when a switch was upgraded from a 6.x version to an 8.x version. This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions.	Configuration	All platforms	AOS-W 8.3.0.6
AOS-183309	—	**Symptom:** Managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (Heartbeat Initiated)**. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.3 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.2.3

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183508	—	**Symptom:** 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. **Scenario:** This issue was observed in OAW-AP345 access points running AOS-W 8.3.0.6 or later versions.	AP-Wireless	OAW-AP345 access points	AOS-W 8.3.0.6
AOS-183601	—	**Symptom:** Some APs advertised incorrect protection flag in their beacons. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue occurred when 802.11g, 802.11n, or 802.11ac clients were connected to 2.4 GHz radios and low rates of 1 Mbps were removed from the Tx rate of SSID profiles. This issue was observed in OAW-AP305 and OAW-AP315 access points running AOS-W 8.3.0.0 or later versions.	AP-Wireless	OAW-AP305 and OAW-AP315 access points	AOS-W 8.3.0.0
AOS-183640 AOS-184351 AOS-184539 AOS-184540	—	**Symptom:** The **mDNS** process in a Mobility Master Virtual Appliance crashed unexpectedly. This issue is resolved by fixing the memory leak in the **mDNS** process. **Scenario:** This issue occurred when the **show airgroup aps** or **tar logs techsupport** command was executed. This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.2.2.4 or later versions.	AirGroup	All platforms	AOS-W 8.2.2.4
AOS-183717	121422	**Symptom:** A managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4).** The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.3 or later versions.	switch Datapath	All platforms	AOS-W 8.2.2.3
AOS-183885	—	**Symptom:** The telemetry API did not include the Enocean user data type and the BLE local name in the output of the **show ap debug ble-table** command. The fix ensures that the telemetry API includes the Enocean user data type and the BLE local name in the output of the **show ap debug ble-table** command. **Scenario:** This issue was observed in access points running AOS-W 8.4.0.0.	IoT	All platforms	AOS-W 8.4.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183962 AOS-184518	—	**Symptom:** 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. **Scenario:** This issue was observed in OAW-4650 and OAW-4008 switches running AOS-W 8.3.0.0 or later versions.	Ipsec	OAW-4650 and OAW-4008 switches	AOS-W 8.3.0.0
AOS-184093	—	**Symptom:** The **cellular handoff assist** feature did not work even though the clients reached the Signal-to-Noise Ratio threshold rate. The fix ensures that the **cellular handoff assist** feature is triggered. **Scenario:** This issue was observed in OAW-AP305, OAW-AP315, and OAW-AP210AP-318 access points running AOS-W 8.2.0.0 or later versions.	ARM	OAW-AP305, OAW-AP315, and OAW-AP210AP-318 access points	AOS-W 8.2.0.0
AOS-184265 AOS-184964	—	**Symptom:** 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. **Scenario:** This issue occurred due to an error in API response for i**pv6_domain_lookup**. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	Configuration	All platforms	AOS-W 8.4.0.0
AOS-184287	—	**Symptom:** The command **show ap client trail-info** displayed the de-auth reason as Client- match instead of cellular handoff assist. The fix ensures that the command works as expected. **Scenario:** This issue was observed in Mobility Master running AOS-W 8.0.0.0 or later versions.	ARM	All platforms	AOS-W 8.0.0.0
AOS-184545	—	**Symptom:** An AP 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 resolves this issue. **Scenario:** This issue occurred when the AP processed large batch files leading to lock stall detection and causing panic. This issue was observed in OAW-AP303H access points running AOS-W 8.0.0.0 or later versions.	AP Datapath	OAW-AP303H access points	AOS-W 8.0.0.0

Table 6: *Resolved Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184851	—	**Symptom:** The **login-fcgi** process in a switch crashed unexpectedly. This issue is resolved by increasing the array size to 128K for processing request parameters. **Scenario:** This issue occurred when http requests larger than 8k were processed, leading to a segmentation fault. This issue was observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.	Captive Portal	OAW-4850 switches	AOS-W 8.4.0.0
AOS-185346	—	**Symptom:** A Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Control Processor Kernel Panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred due to a softlock causing the crash. This issue was observed in OAW-4x50 Series switches running AOS-W 8.2.0.0 or later versions. **Old Duplicates:** 170224, 171074, 171396, 173372, 174322, 174370, 174917, 175009, 177151, 177457, 177662, 178307, 180558, 180741, 181173, 183588, 185596, 186993, 187232, 187418, 188367, 192790, 193202, 194859	Captive Portal	OAW-4x50 Series switches	AOS-W 8.2.0.0
AOS-183445	—	**Symptom:** The usage graph was not displayed in the **Dashboard > Overview** page of a managed device. The fix ensures that the usage graph is displayed as expected. **Scenario:** This issue occurred because of invalid data for the BSSID statistics and a large number of AMON_BSSID_TUNNEL_STATS_ MESSAGE packets. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.4.0.0
AOS-185187	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **PC is at wlc_chanctxt_set_passive_ use+0x6d4**. Adding a missing check to the source code resolved this issue. **Scenario:** This issue was observed in 510 Series access points running AOS-W 8.4.0.0 or later versions.	AP-Wireless	510 Series access points	AOS-W 8.4.0.0

This chapter describes the known issues and limitations identified in AOS-W 8.5.0.0.

Limitations

This section describes the limitations in AOS-W 8.5.0.0.

No Support for Command-Line Authorization for TACACS and TACACS+ Authentication

Command-line authorization of local management user accounts is currently not supported for TACACS and TACACS+ authentication.

No Support for Captive Portal

Captive portal is not supported for the split-tunnel mode Virtual APs and wired APs, when cluster is enabled.

Known Issues

The following known issues are observed in AOS-W 8.5.0.0.

Table 7: *Known Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-150970	138292	**Symptom:** The **show rft result** command displays **No result to show** as output. **Scenario:** This issue occurs because the RFT feature is not supported in 802.11ax devices. This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP535 and OAW-AP555 access points	AOS-W 8.5.0.0
AOS-155389 AOS-155482 AOS-182832	191076 191205	**Symptom:** A OAW-4850 switch reports uplink negotiation failure on 40G and 1G ports; affecting services. **Scenario:** This issue occurs due to: ■ An oversubscribed 1G port. ■ **bcmc-optimization allow-unknown-unicast** configuration under **interface vlan <>** ■ switch experiencing a flood of unicast traffic ■ Subsequent flapping of either the uplink or 1G port. This issue is observed in OAW-4850 switches running AOS-W 8.0.0.0 or later versions. **Workaround:** ■ Use 10G channels instead of 1G channels. ■ Use one of the following port combinations that are supported on a OAW-4850 switch: 40G and 10G, or 40G and 40G, or 10G and 10G channels.	switch-Platform	OAW-4850 switches	AOS-W 8.0.0.0
AOS-155632 AOS-157337 AOS-157417 AOS-158610	191489 193793 193945 195645	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:70:4)**. **Scenario:** This issue is observed in OAW-4750XM switches running AOS-W 8.2.2.3. **Workaround:** None.	switch-Platform	OAW-4750XM switches	AOS-W 8.2.2.3

Table 7: *Known Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157358 AOS-157430 AOS-157520 AOS-157602 AOS-183568 AOS-185118	193835 193958 194106 194233	**Symptom:**A OAW-4x50 Series controller crashes and the log file states the reason as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:40:2)** **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 8.3.0.1 or later versions. **Workaround:** None.	switch-Platform	OAW-4x50 Series switches	AOS-W 8.3.0.1
AOS-183117 AOS-183777 AOS-183581 AOS-185027 AOS-186155	194395	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **BadAddr:ff020202020203ee PC:phy_ac_noise_unregister_impl+0x360/0x678 [wl] Warm-reset**. **Scenario:** This issue is observed in OAW-AP340 Series access points running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP340 Series access points	AOS-W 8.3.0.3
AOS-183123	—	**Symptom:** The **%** symbol is not displayed for **cluster client threshold values** in **Configuration > System > Profiles > Cluster** page of the WebUI. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.0 in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.0
AOS-183179	—	**Symptom:** Video multicast frames gets transmitted at the rate of 24 Mbps even when the configuration is set at 54 Mbps. **Scenario:** This issue is observed in OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP555 access points	AOS-W 8.5.0.0

Table 7: *Known Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183244 AOS-183758 AOS-185673	—	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **FW assert at tbd.c:39.** **Scenario:** This issue occurs while enabling or disabling dot11k profile. This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.0
AOS-183317	—	**Symptom:** A few APs detect false radars. **Scenario:** This issue is observed in OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP555 access points	AOS-W 8.5.0.0
AOS-183878	—	**Symptom:** The total load percentage of managed devices are not displayed in the logs although more APs are added to the managed devices. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.0 in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.0
AOS-184450	—	**Symptom:** Clients connected to APs are getting deauthenticated. **Scenario:** This issue occurs when bi-directional traffic is introduced among High Efficiency clients due to which the APs are unable to send data to the clients. This issue is observed in APs running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.5.0.0
AOS-184834	—	**Symptom:** The AP and client entries are not displaying zero although the managed device is disabled or shut down. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.0 in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.0
AOS-184705	—	**Symptom:** Some clients get disassociated from the network and get reassociated after few seconds. **Scenario:** This issue is observed in OAW-AP534, OAW-AP535, and OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP534, OAW-AP535, and OAW-AP555 access points	AOS-W 8.5.0.0

Table 7: *Known Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184795	—	**Symptom:** APs are not moving to the standby list when the load balancing thresholds are met. **Scenario:** This issue is observed APs connected to managed devices running AOS-W 8.5.0.0 in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.5.0.0
AOS-184921	—	**Symptom:** Few wired clients are unable to connect to APs. **Scenario:** This issue occurs when the wired clients are connected to the first Ethernet port of the APs. This issue is observed in OAW-AP555 and OAW-AP535 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Platform	OAW-AP555 and OAW-AP535 access points	AOS-W 8.5.0.0
AOS-185115	—	**Symptom:** Some clients are getting disconnected from the APs when the 2.4 GHz radio is reset. **Scenario:** This issue occurs when multiple APs are configured across 2.4 GHz and 5 GHz radios. This issue is observed in APs running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.5.0.0
AOS-185184	—	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Kernel panic; BUG: soft lockup - CPU#0 stuck**. **Scenario:** This issue occurs when: ■ the frame size is smaller and the throughput is higher. ■ the type of frames or destination do not matter as long as the data is sent to the AP's Ethernet port. This issue is observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	530 Series and 550 Series access points	AOS-W 8.5.0.0
AOS-185233	—	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **wal_phy_dev_hw.c:4423 Assertion g_disable_phy_m3_assert == TRUE; Thread name : IST1**. **Scenario:** This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.0
AOS-185259	—	**Symptom:** All radios display poor channel quality under **Dashboard** > **Overview** > **Radios** > **CHANNEL QUALITY** column. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.0. **Workaround:** None.	Station Management	All platforms	AOS-W 8.5.0.0

Table 7: *Known Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185262	—	**Symptom:** Clients are getting disconnected from APs. **Scenario:** This issue is observed in APs running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.5.0.0
AOS-185597	—	**Symptom:** An AP crashes and reboots unexpectedly. The log files lists the reason for the event as **WLAN FW exception at wal_ba_tx_sm().** **Scenario:** This issue is observed in OAW-AP555 and OAW-AP535 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP555 and OAW-AP535 access points	AOS-W 8.5.0.0
AOS-185696	—	**Symptom:** An AP stops responding to data frames and cannot decode block acknowledge from the STA leading to packet drop. After a few packets are dropped, the AP starts acknowledging the data frames and the traffic resumes. **Scenario:** This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP535 and OAW-AP555 access points	AOS-W 8.5.0.0
AOS-185707	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file may not list the reason explicitly since it is an exceptional condition detected in the software. **Scenario:** This issue is observed in OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP555 access points	AOS-W 8.5.0.0
AOS-185779	—	**Symptom:** A few APs continuously observe **wl1: PHYTX** error messages with no clients connected. **Scenario:** This issue is observed in 510 Series access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	AOS-W 8.5.0.0
AOS-185833	—	**Symptom:** A few APs crash unexpectedly. The log file lists the reason for this event as **ar_wal_vdev.c:2528 Assertion;Thread ID : 0x0000005e;PC : 0x4b0c9de8**. **Scenario:** This issue is observed in OAW-AP535 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.0

Table 7: *Known Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185894	—	**Symptom:** A few APs that operate in tunnel node incorrectly set the TID of downlink multicast traffic to 0. **Scenario:** This issue is observed in OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP555 access points	AOS-W 8.5.0.0
AOS-185932	—	**Symptom:** Some clients delete block acknowledge agreement leading to ping timeouts. **Scenario:** This issue occurs randomly when clients are still connected. Once a re-negotiation happens, the traffic resumes normally. This issue is observed in 550 Series access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	550 Series access points	AOS-W 8.5.0.0
AOS-185937	—	**Symptom:** An Access point crashes and reboots unexpectedly. The log files lists the reason for the event as **whal_recv_recovery.c:606 Assertion RX_HW_WDOG_HANG failedparam0 :zero, param1 :zero, param2 :zero.** **Scenario:** This issue is observed in OAW-AP555 and OAW-AP535 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP555 and OAW-AP535 access points	AOS-W 8.5.0.0
AOS-186052	—	**Symptom:** A few APs witness TX mute when a radio reset burst occurs. **Scenario:** This issue occurs due to a reset in G radio that is triggered due to an interference in the AP's operating channel. This issue is observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	530 Series and 550 Series access points	AOS-W 8.5.0.0
AOS-186095	—	**Symptom:** A few APs lose association and reconnect back immediately. **Scenario:** This issue occurs due to a beacon drift. This issue is observed in 530 Series and 550 Series access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	530 Series and 550 Series access points	AOS-W 8.5.0.0
AOS-186096	—	**Symptom:** Some APs randomly observe radio resets. **Scenario:** This issue occurs in OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP555 access points	AOS-W 8.5.0.0

Table 7: *Known Issues in AOS-W 8.5.0.0*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186108	—	**Symptom:** Some clients are unable to send and receive data. **Scenario:** This issue occurs when 802.11r is enabled and clients roam between 2.4 GHz and 5 GHz band. This issue is observed in OAW-AP534 and OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP534 and OAW-AP555 access point	AOS-W 8.5.0.0
AOS-186144	—	**Symptom:** A managed device is unable to enable Tunnel Keepalive automatically, even after configuring Tunnel Heartbeat Interval & Tunnel Heartbeat Retries. **Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.0 in a master-local topology. **Workaround:** None.	GRE	All platforms	AOS-W 8.5.0.0
AOS-186146	—	**Symptom:** Some APs display active RX even though the radio is off. **Scenario:** This issue is observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.0. **Workaround:** None.	AP-Wireless	OAW-AP535 and OAW-AP555 access points	AOS-W 8.5.0.0
AOS-186237 AOS-185529	—	**Symptom:** The status and channel quality of an AP is displayed as **Poor** in the **Dashboard > Overview > Radios** WebUI page of a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.0. **Workaround:** None.	Monitoring	All platforms	AOS-W 8.5.0.0
AOS-186349	—	**Symptom:** The command **ap image-preload** takes any possible maximum value whereas a maximum of only 500 APs can be preloaded at any given time. **Scenario:** This issue is observed in Mobility Master running AOS-W 8.5.0.0. **Workaround:** None.	Image Upgrade	All platforms	AOS-W 8.5.0.0

This chapter details software upgrade procedures. Alcatel-Lucent best practices recommend 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, and/or stand-alone switch.

Topics in this chapter include:

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

If you are migrating from AOS-W 6.x to AOS-W 8.x, note the following points:

- 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 to *Alcatel-Lucent Mobility Master Licensing Guide*.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You must save this list for future use.

- 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 other 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 your 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** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the managed device?
  - Are all managed devices running the same version of software?
  - Which services are used on the managed device (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software 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, see the "Software Licenses" chapter in the *AOS-W 8.x.0.0 User Guide*.

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. To maintain the reliability of your WLAN network, the following compact memory best practices are recommended:

- Confirm that there is at least 100 MB of free memory available for an upgrade using the WebUI or CLI. Execute the **show memory** command to identify the amount of free memory available using the CLI. Do not proceed unless 100 MB of free memory is available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Confirm that there is at least 150 MB of flash space available for an upgrade using the WebUI or CLI. Using the CLI, execute the **show storage** command to identify the amount of flash space available.

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

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free up some used memory. Any managed device logs, crash data, or flash backups should be copied to a location off the managed device, then deleted from the managed device to free up flash space. You can delete the following files from the managed device to free up some memory before upgrading:

- **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 57 to copy the **crash.tar** file to an external server, and then 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 57 to back up the flash directory to a file named **flash.tar.gz**, and then 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 57 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the managed device.

Use the following procedure to delete files and free up memory space:

In the WebUI

From the Mobility Master, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

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 compact flash file system to an external server or mass storage device. At the very least, 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
- Logs

- Flashbackup

Backing up and Restoring Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on a managed device:

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 compact flash file system 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 compact flash file system using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > Configuration Management > Restore** page and click **Restore**.

Backing up and Restoring Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the command line:

1. Make sure you are in the **enable** mode in the CLI, and execute the following command:
   ```
   (host) # write memory
   ```
2. Execute the **backup** command to back up the contents of the compact flash file system 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 the **copy** command to transfer the backup flash 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 backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.
   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.
   ```
   (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

The following sections provide the procedures for upgrading your WLAN network to the latest AOS-W version using the WebUI or CLI.

In the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 56.

NOTE

When you navigate to the **Configuration** tab in the WebUI, the managed device may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade from the WebUI and navigate to the **Configuration** tab as soon as the managed device completes rebooting. This error is expected and disappears after clearing the Web browser cache.

You can install the software image from a TFTP or FTP server using the WebUI page.

1. Download AOS-W from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the **Alcatel.sha256** file from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or 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 support site.

NOTE

The AOS-W image file is digitally signed, and is verified using RSA2048 certificates preloaded at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the managed device will not load a corrupted 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** field 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

Note that the upgrade will not take effect until you reboot.

9. Select the **Save Current Configuration** option.
10. Click **Upgrade**.

    When the software image is uploaded, a popup window displays the message, **Changes were written to flash successfully**.
11. Click **OK**.

    If you chose to automatically reboot in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the upgrade.

When your upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use, and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Memory Requirements on page 56 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

In the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 56.

Upgrading From a Recent Version of AOS-W

To install the AOS-W software image from a PC or workstation using the CLI:

1. Download AOS-W from the customer support site.
2. Open an SSH session on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/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 images are loaded on the switch's flash partitions. 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 onto 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 switch.
   ```
   (host)# reload
   ```
8. Execute the **show version** command to verify that the upgrade is complete.
   ```
   (host)# show version
   ```

When the upgrade is complete, perform the following steps to verify that the switch is functioning as expected.

1. Log in to the CLI to verify that all your switches are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 57 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of AOS-W.

Before You Begin

Before you reboot the switch with the pre-upgrade software version, you must perform the following steps:

1. Back up your switch. For details, see Backing up Critical Data on page 57.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W configuration file.
4. Set the switch to boot from the system partition that contains the previously running AOS-W image.

When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next switch reload. An error message is displayed if the system boot parameters are set for incompatible image and configuration files.

5. After downgrading the software on the switch, perform the following steps:
   - Restore pre-AOS-W flash backup from the file stored on the switch. Do not restore the AOS-W flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in AOS-W, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the switch

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. For **Select source file** option, 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. For **Select destination file** option, enter a file name (other than default.cfg) for Flash File System.
2. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If there is no previous software image 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/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
4. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The switch reboots after the countdown period.
5. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Software Management > About** page.

Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the switch.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:

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

   or

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

2. Set the switch 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 previous software image is stored. You cannot load a new image into the active system partition (the default boot).

   ```
   #show image version
   ```

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

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

5. Reboot the switch.

   ```
   (host) # reload
   ```

6. When the boot process is complete, verify that the switch is using the correct software.

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

Before You Call Technical Support

Before you call Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Alcatel-Lucent device with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless Network Interface Card (NIC) make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file at the time of the problem. Alcatel-Lucent strongly recommends that you consider adding a syslog server, if you do not already have one, to capture the logs.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Alcatel-Lucent device) or any recent changes to your Alcatel-Lucent device and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.

7. Provide the date and time (if possible) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the Alcatel-Lucent device site access information, if possible.