# AOS-W 8.5.0.10

Alcatel·Lucent Enterprise

Release Notes

## Copyright Information

## Open Source Code

## Revision History

The following table provides the revision history of this document.

**Table 1:** *Revision History*

| Revision | Change Description |
|---|---|
| Revision 01 | Initial release. |

This AOS-W release notes includes the following topics:

NOTE

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

## Important Points Before Upgrading to AOS-W 8.5.0.0

**Starting from AOS-W 8.5.0.0, your CPU should support version SSE4.2.** For deployments on versions prior to AOS-W 8.5.0.0, SSSE3 is the minimum supported version. Additionally the CPU should also support Intel VT.

### DPI Classification

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 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
- Mozilla Firefox 58 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

## Contacting Support

**Table 2:** *Contact Information*

| **Contact Center Online** | |
|---|---|
| Main Site | https://www.al-enterprise.com |
| Support Site | https://businessportal2.alcatel-lucent.com |
| Email | ebg_global_supportcenter@al-enterprise.com |
| **Service & Support Contact Center Telephone** | |

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

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

## CLI

### ssh command

The following modifications are introduced:

- The **ssh disable-mac hmac-sha1** command disables HMAC-SHA1 authentication and enables HMAC-SHA1-96 and HMAC-SHA2-256 authentication .
- The **ssh disable-mac hmac-sha1-96** command disables HMAC-SHA1-96 authentication and enables HMAC-SHA1 and HMAC-SHA2-256 authentication.

Issue the **ssh disable-mac hmac-sha1 hmac-sha1-96** command or **ssh disable-mac hmac-sha1-96 hmac-sha1** command to disable both algorithms of HMAC-SHA1 authentication and to enable HMAC-SHA2-256 authentication.

### show airgroup command

A new parameter, **ppm** is added to the **show airgroup internal- state statistics** command. The **show airgroup internal- state statistics ppm** command displays the packet per minute statistics. The following command displays the packet per minute statistics:

```
(host) [mynode] #show airgroup internal-state statistics ppm
```

The sub-parameters **daily, hourly, weekly,** and **minutes** display the corresponding packet per minute statistics.

```
(host) [mynode] #show airgroup internal-state statistics ppm daily
(host) [mynode] #show airgroup internal-state statistics ppm weekly
(host) [mynode] #show airgroup internal-state statistics ppm hourly
(host) [mynode] #show airgroup internal-state statistics ppm minutes
```

The optional sub-parameter **<count>** limits the amount of information to be displayed in each row for the output of this command.

```
(host) [mynode] #show airgroup internal-state statistics ppm 20
```

### show tech-support command

A new parameter, **airgroup** has been added to the **show tech-support** command. The **show tech-support airgroup** command displays AirGroup related tech-support logs.

## OAW-RAP Termination on Mobility Master Virtual Appliance

Mobility Master Virtual Appliances can establish tunnels with OAW-RAPs provisioned with custom CA certificates. The Mobility Master Virtual Appliance will use the CA certificate public key sent by the OAW-RAP to establish the tunnel.

If a OAW-RAP is terminating on a cluster, all cluster nodes should use the same custom CA certificate and the same should be provisioned on OAW-RAP.

NOTE

This feature works only when the OAW-RAP is provisioned with custom certificate.

# Supported Platforms

This chapter describes the platforms supported in this release.

## Mobility Master Platforms

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

**Table 3:** *Supported Mobility Master Platforms in AOS-W 8.5.0.10*

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

## OmniAccess Mobility Controller Platforms

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

**Table 4:** *Supported OmniAccess Mobility Controller Platforms in AOS-W 8.5.0.10*

| OmniAccess Mobility Controller Family | OmniAccess Mobility Controller Model |
|---|---|
| OAW-40xx Series Hardware OmniAccess Mobility Controllers | OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030 |
| OAW-4x50 Series Hardware OmniAccess Mobility Controllers | OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850 |
| OAW-41xx Series Hardware OmniAccess Mobility Controllers | OAW-4104 |
| MC-VA-xxx Virtual OmniAccess Mobility Controllers | MC-VA-50, MC-VA-250, MC-VA-1K |

## AP Platforms

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

**Table 5:** *Supported AP Platforms in AOS-W 8.5.0.10*

| AP Family | AP Model |
|---|---|
| OAW-AP100 Series | OAW-AP104, OAW-AP105 |
| OAW-AP103 Series | OAW-AP103 |
| OAW-AP110 Series | OAW-AP114, OAW-AP115 |
| OAW-AP130 Series | OAW-AP134, OAW-AP135 |
| OAW-AP 170 Series | OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1 |
| OAW-AP200 Series | OAW-AP204, OAW-AP205 |
| OAW-AP203H Series | OAW-AP203H |
| OAW-AP205H Series | OAW-AP205H |
| OAW-AP207 Series | OAW-AP207 |
| OAW-AP203R Series | OAW-AP203R, OAW-AP203RP |
| OAW-AP210 Series | OAW-AP214, OAW-AP215 |
| OAW-AP 220 Series | OAW-AP224, OAW-AP225 |
| 228 Series | OAW-AP228 |
| OAW-AP270 Series | OAW-AP274, OAW-AP275, OAW-AP277 |
| OAW-AP300 Series | OAW-AP304, OAW-AP305 |
| OAW-AP303 Series | OAW-AP303 |
| OAW-AP303H Series | OAW-AP303H |

**Table 5:** *Supported AP Platforms in AOS-W 8.5.0.10*

| AP Family | AP Model |
|---|---|
| OAW-AP310 Series | OAW-AP314, OAW-AP315 |
| OAW-AP318 Series | OAW-AP210AP-318 |
| OAW-AP320 Series | OAW-APAP-324, OAW-AP325 |
| OAW-AP330 Series | OAW-AP334, OAW-AP335 |
| OAW-AP340 Series | OAW-AP344, OAW-AP345 |
| OAW-AP360 Series | OAW-AP365, OAW-AP367 |
| OAW-AP370 Series | OAW-AP374, OAW-AP375, OAW-AP377 |
| OAW-AP387 | OAW-AP387 |
| OAW-AP510 Series | OAW-AP514, OAW-AP515 |
| OAW-AP530 Series | OAW-AP534, OAW-AP535 |
| OAW-AP550 Series | OAW-AP555 |
| OAW-RAP3 Series | OAW-RAP3WN, OAW-RAP3WNP |
| OAW-RAP100 Series | OAW-RAP108, OAW-RAP109 |
| OAW-RAP155 Series | OAW-RAP155, OAW-RAP155P |

# Chapter 4
# Regulatory Updates

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the switch Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at businessportal2.alcatel-lucent.com.

The following DRT file version is part of this release:

- DRT-1.0_75968

# Chapter 5
# Resolved Issues

This chapter describes the issues resolved in this release.

NOTE

We have migrated to a new defect tracking tool. All the bugs are listed with the new bug ID, which is prefixed by AOS.

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-125305 | 151011 | **Symptom:** Clients were unable to connect to APs. The fix ensures seamless connectivity.<br>**Scenario:** This issue occurred when **STM** process failed to discover VLANs. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.<br>**Duplicates:**<br>**New Bug IDs:** AOS-122776, AOS-124619, AOS-139533, AOS-145308, and AOS-188376<br>**Old Bug IDs:** 147957, 150132, 169561, and 177209 | Station Management | All platforms | AOS-W 8.3.0.0 |
| AOS-148643<br>AOS-150529 | 182036<br>184499 | **Symptom:** Clients were unable to connect to the 802.1X SSID when UAC and AAC were different. The fix ensures seamless connectivity.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | Station Management | All platforms | AOS-W 8.3.0.0 |
| AOS-157462<br>AOS-202579 | 194010 | **Symptom:** The **web_cc** process crashed on a managed device. The ix ensures that the **web_cc** process works as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.6 or later versions. | WebCC | All platforms | AOS-W 8.2.2.6 |
| AOS-186411 | — | **Symptom:** A few users were unable to remove a VLAN from the port channel trunk. The fix ensures that the users are able to remove VLAN from the port channel trunk.<br>**Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions. | Interface | All platforms | AOS-W 8.3.0.0 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-187025<br>AOS-201544 | — | **Symptom:** The **Dashboard > Services** page did not display the list of AirGroup servers and an error message, **Error retrieving information. Please try again later** was displayed. The fix ensures that WebUI displays the list of AirGroup servers.<br>**Scenario:** This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions. | AirGroup | All platforms | AOS-W 8.3.0.0 |
| AOS-188073 | — | **Symptom:** The value of the **Max Negotiated Tx Rate** was incorrect after changing the **vht-support-mcs** and **supported-mcs-set** values. The fix ensures that the correct values are displayed.<br>**Scenario:** This issue was observed in APs running ArubaOS 8.5.0.0 or later versions. | AP-Wireless | All platforms | AOS-W 8.5.0.0 |
| AOS-188271<br>AOS-196680<br>AOS-201542<br>AOS-201956<br>AOS-202569<br>AOS-202570 | — | **Symptom:** A few APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **BadAddr:20000002d PC:crypto_authenc_ahash+0x2c/0x90 Warm-reset.** Enhancements to the wireless driver fixed the issue.<br>**Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions. | AP-Wireless | OAW-AP515 access points | AOS-W 8.5.0.0 |
| AOS-188777 | — | **Symptom:** The device name was not updated in a Mobility Master whitelist table after removing the AP / Device name in Activate. The fix ensures that the device name gets updated correctly.<br>**Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions. | CPsec-Whitelist Management | All platforms | AOS-W 8.3.0.0 |
| AOS-188793 | — | **Symptom:** The output of the **show audit-trail** command displayed incorrect message for the **BOCMGR** process in a Mobility Master. The fix ensures that the command does not display the incorrect message.<br>**Scenario:** This issue occurred when the Mobility Master was connected to the Activate server. This issue was observed in Mobility Masters running AOS-W 8.2.2.3 or later versions. | Configuration | All platforms | AOS-W 8.2.2.3 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-188898<br>AOS-198730<br>AOS-200227 | — | **Symptom:** The **postgres** process crashed on a managed device. The fix ensures that the managed devices work as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions. | Database | All platforms | AOS-W 8.2.2.6 |
| AOS-188979<br>AOS-201731 | — | **Symptom:** A few LEAP authenticated wireless clients were unable to connect to OAW-AP535 access points. Enhancements to the wireless driver fixed the issue.<br>**Scenario:** This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.5 or later versions. | AP-Wireless | OAW-AP535 access points | AOS-W 8.5.0.5 |
| AOS-189194 | — | **Symptom:** The 5 GHz and 2.4 GHz antenna values were swapped after AP provisioning rules was configured using the **Configuration > Access Points > Provisioning Rules** page of the WebUI. The fix ensures that 5 GHz and 2.4 GHz antenna values are not swapped.<br>**Scenario:** This issue occurred when a user selected the **Set Antenna Gain for Dual Band mode** option from the **Actions** drop-down list in the **Configuration > Access Points > Provisioning Rules** page, and entered the **5 GHz** and **2.4 GHz** field values in the WebUI. This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.3 or later versions. | WebUI | All platforms | AOS-W 8.5.0.0 |
| AOS-189945<br>AOS-190084 | — | **Symptom:** A fatal error message was displayed when there was a mismatch between the AOS-W versions of a Mobility Master and managed device. Changes to the log levels resolved this issue.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | DDS | All platforms | AOS-W 8.3.0.0 |
| AOS-189982<br>AOS-200329 | — | **Symptom:** The **Configuration >WLANs** page did not display WLANs at lower node levels. The fix ensures that the WebUI displays the complete list of WLANs.<br>**Scenario:** This issue occurred when WLAN profiles were created with the same name but with different case. This issue was observed in Mobility Masters running AOS-W 8.3.0.6 or later versions. | WebUI | All platforms | AOS-W 8.3.0.6 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-191112 | — | **Symptom:** A few data packets were lost when the packets were forwarded using AP Packet Capture. The fix ensures that the APs work as expected.<br>**Scenario:** This issue occurred when the APs were in Air Monitor mode. This issue was observed in OAW-AP325 and OAW-AP335 access points running AOS-W 8.5.0.0 or later versions. | AP Datapath | OAW-AP325 and OAW-AP335 access points | AOS-W 8.5.0.0 |
| AOS-191216<br>AOS-196523<br>AOS-199160<br>AOS-203960 | — | **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:e0:2).** The fix ensures that the managed device works as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.4 or later versions. | switch-Platform | All platforms | AOS-W 8.5.0.4 |
| AOS-191446<br>AOS-201647 | — | **Symptom:** Users were unable to change the password of PSK authenticated SSID profiles from lower node levels. The fix ensures that the users are able to change the password.<br>**Scenario:** This issue occurred when the AP group was mapped to an IoT profile. This issue was observed in managed devices running AOS-W 8.5.0.6 or later versions. | IoT | All platforms | AOS-W 8.5.0.6 |
| AOS-191612 | — | **Symptom:** The MAC addresses of users connected using VIA were not sent to ClearPass Policy Manager for authentication. The fix ensures that the MAC addresses are sent to ClearPass Policy Manager for authentication.<br>**Scenario:** This issue occurred when IKE V2 with EAP-FTC was used for VIA authentication. This issue was observed in Mobility Masters running AOS-W 8.5.0.1 or later versions. | IPsec | All platforms | AOS-W 8.5.0.1 |
| AOS-191752 | — | **Symptom:** Some APs were not being reclassified though the classification rules were modified using the **ids ap-classification-rule** command. The fix ensures that the APs get reclassified.<br>**Scenario:** This issue was observed when the AP classifications were changed using ids-rules, but the old classification rules did not change. This issue was observed in APs running AOS-W 8.2.0.0 or later versions. | Air Management-IDS | All platforms | AOS-W 8.2.0.0 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-192237<br>AOS-203521 | — | **Symptom:** APs logged the error message, **An internal system error has occurred error Unable to add eth2 to STP device: Device or resource busy**. The fix ensures that the error message is not displayed.<br>**Scenario:** This issue was observed in OAW-AP203H, OAW-AP303H, and OAW-AP205H access points running AOS-W 8.3.0.0 or later versions. | AP-Platform | OAW-AP203H, OAW-AP303H, and OAW-AP205H access points | AOS-W 8.3.0.0 |
| AOS-192593 | — | **Symptom:** The output of the **show switches** command displayed the error message, **Module Configuration Manager is busy. Please try later**. The fix ensures that the error message is not displayed.<br>**Scenario:** This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions. | Configuration | All platforms | AOS-W 8.6.0.0 |
| AOS-192868 | — | **Symptom:** The AirWave graph for some clients displayed zero value. The fix ensures that the correct graph is displayed.<br>**Scenario:** This issue occurred when the **CL_TX_DATA_BYTES_ TRANSMITTED** counter and the **CL_RX_DATA_BYTES** counter were decremented from **AMON_STATION_STATS_MESSAG** counter, and the wireless clients downloaded huge files from the wired FTP servers. This issue was observed in OAW-4030 switches running AOS-W 8.3.0.0 or later versions. | Air Management-IDS | OAW-4030 switches | AOS-W 8.3.0.0 |
| AOS-193033<br>AOS-198921<br>AOS-198953 | — | **Symptom:** A few clients were not redirected to the captive portal page. The fix ensures that captive portal is working as expected.<br>**Scenario:** This issue occurred because the **Nginx** process failed due to a race condition. This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions. | Captive Portal | All platforms | AOS-W 8.4.0.2 |
| AOS-193761 | — | **Symptom:** The output of **show airmatch debug solution list-all** command did not display the AP name. The fix ensures that the output of the command displays the AP name.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions. | AirMatch | All platforms | AOS-W 8.6.0.0 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-193840 | — | **Symptom:** A managed device lost connectivity to IPv6 gateway intermittently. The fix ensures that the managed device works as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions. | switch- Datapath | All platforms | AOS-W 8.3.0.6 |
| AOS-194571 | — | **Symptom:** Some wireless clients experienced **IEEE80211_IOCTL_ARUBA_STA_STATS_64** call overflow with a 32-bit value that led to counter reset. This issue is resolved by updating the stats with the correct 64 bit stats.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | AP-Wireless | All platforms | AOS-W 8.3.0.0 |
| AOS-194709 | — | **Symptom:** Users were unable to run a **traceroute** command to any public IP address. The fix ensures that the users are able to run a **traceroute** command to any public IP address.<br>**Scenario:** This issue occurred when the managed device was using only one uplink, irrespective of the number of uplinks available. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | Routing | All platforms | AOS-W 8.3.0.0 |
| AOS-194846 | — | **Symptom:** The commands **show ap arm history** and **show airmatch debug optimization** did not display any output. The fix ensures that the AirMatch optimization works on the Mobility Master as expected.<br>**Scenario:** This issue occurred when AirMatch optimization did not work on the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions. | AirMatch | All platforms | AOS-W 8.3.0.7 |
| AOS-194930 | — | **Symptom:** The **Auth Sub-type** column under **Managed Network > Dashboard > Overview > Clients** table displayed **None** though the authentication sub-type was **EAP-PEAP.** The fix ensures that the WebUI displays the authentication sub-type.<br>**Scenario:** This issue occurred in 802.1X authenticated users after a failed station reauthentication attempt. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions. | Base OS Security | All platforms | AOS-W 8.3.0.7 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-195177 | — | **Symptom:** Managed devices frequently generated internal system error logs. The fix ensures that managed devices do not generate error logs frequently.<br>**Scenario:** This issue occurred when the **sapd** process read a non-existent interface. This issue was observed in OAW-4650 switches running AOS-W 8.3.0.7 or later versions. | AP-Wireless | OAW-4650 switches | AOS-W 8.3.0.7 |
| AOS-195646 | — | **Symptom:** The **Authentication** process crashed on a managed device unexpectedly. The fix ensures that the managed device works as expected.<br>**Scenario:** This issue occurred because of incorrect parsing of PAPI messages. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions in a cluster setup. | Base OS Security | All platforms | AOS-W 8.4.0.4 |
| AOS-196229<br>AOS-196264<br>AOS-205903 | — | **Symptom:** Random values were displayed as the host name of a Mobility Master. The fix ensures that random values are not displayed.<br>**Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.8 or later versions. | Configuration | All platforms | AOS-W 8.5.0.8 |
| AOS-196541 | — | **Symptom:** API on an AOS-W Mobility Master did not operate over port 443. The fix ensures that API operates over port 443.<br>**Scenario:** This issue occurred when there was no rule for login or token generation over port 443. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions. | Web Server | All platforms | AOS-W 8.5.0.4 |
| AOS-196593 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **reboot caused by Kernel panic - not syncing: Fatal exception in interrupt PC is at 0x000C7461**. Enhancements to the wireless driver resolved the issue.<br>**Scenario:** This issue was observed in OAW-AP335 access points running AOS-W 8.3.0.8 or later versions. | Station Management | OAW-AP335 access points | AOS-W 8.3.0.8 |
| AOS-196697<br>AOS-199833 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **PC is at wlc_apps_psq+0xc/0x6ec [wl_v6];LR is at wlc_apps_release_count+0xb4/0x164 [wl_v6]**. The fix ensures that the APs work as expected.<br>**Scenario:** This issue is observed in access points running AOS-W 8.3.0.8 or later versions. | AP-Wireless | All platforms | AOS-W 8.3.0.8 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-197192 | — | **Symptom:** A few wireless clients were able to authenticate even after the expiry time of the local-user database. The fix ensures that the clients are unable to authenticate after the expiry period.<br>**Scenario:** This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions. | Local Database | All platforms | AOS-W 8.3.0.0 |
| AOS-197224<br>AOS-204629 | — | **Symptom:** A Mobility Controller Virtual Appliance returned RADIUS attribute values in an incorrect order, causing firewall to drop data packets. The fix ensures that the Mobility Controller Virtual Appliance returns RADIUS attribute values in correct order.<br>**Scenario:** This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.4.0.4 or later versions. | 802.1X | All platforms | AOS-W 8.4.0.4 |
| AOS-197309 | — | **Symptom:** Clients were unable to obtain the user role from ClearPass Policy Manager. The fix ensures that clients are able to obtain the user role.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions. | RADIUS | All platforms | AOS-W 8.5.0.3 |
| AOS-197565 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **Dump capture kernel:AP rebooted caused by cold HW reset(power loss).** The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in APs running AOS-W 8.5.0.0 or later versions. | AP-Platform | All platforms | AOS-W 8.5.0.2 |
| AOS-197631 | — | **Symptom:** Policy-based routing was not applied when IPsec map was configured as nexthop. The fix ensures that the managed devices work as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions. | Base OS Security | All platforms | AOS-W 8.6.0.0 |
| AOS-197912 | — | **Symptom:** Multicast traffic was not forwarded to the clients when UAC and AAC were different. The fix ensures that the managed device works as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions. | Station Management | All platforms | AOS-W 8.0.0.0 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-197918 | — | **Symptom:** Redirect pause was enabled although welcome page was disabled in captive portal. The fix ensures that when the welcome page is disabled, the redirect pause is ignored.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions. | Captive Portal | All platforms | AOS-W 8.5.0.0 |
| AOS-197945 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the events as, **BadAddr:ffff00000010 PC:wlc_dump_ aggfifo+0x1160/0x12b0 [wl_v6] Warm-reset.** The fix ensures that the APs work as expected.<br>**Scenario:** This issue occurred due to memory corruption. This issue was observed in OAW-AP514 and OAW-AP515 access points running AOS-W 8.5.0.3 or later versions. | AP-Wireless | OAW-AP514 and OAW-AP515 access points | AOS-W 8.5.0.3 |
| AOS-197994 | — | **Symptom:** FTP ALG in a session based ACL did not trigger correctly. The fix ensures that the FTP ALG works as expected.<br>**Scenario:** This issue occurred when DPI was enabled. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | switch- Datapath | All platforms | AOS-W 8.3.0.0 |
| AOS-198007 | — | **Symptom:** Some APs were unable to ping managed devices and the APs kept switching between clusters.<br>**Scenario:** This issue was observed in APs running AOS-W 8.3.0.8 or later versions. | UCC | All platforms | AOS-W 8.3.0.8 |
| AOS-198157 | — | **Symptom:** A stand-alone switch crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (Intent:cause: 86:56)**. The fix ensures that the stand-alone switch works as expected.<br>**Scenario:** This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions. | switch- Datapath | All platforms | AOS-W 8.6.0.0 |
| AOS-198173<br>AOS-197956 | — | **Symptom:** The **show ap association** command displayed the association ID of a deauthenticated client and hence other clients were unable to use that particular association ID. The fix ensures that the association ID of a deauthenticated client is cleared.<br>**Scenario:** This issue occurred when the opmode was changed from WPA2 to WPA3. This issue was observed in Mobility Masters running AOS-W 8.5.0.10. | Station Management | All platforms | AOS-W 8.5.0.10 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-198218 | — | **Symptom:** After reboot, the status of a GRE tunnel of a standby switch was UP instead of DOWN in a VRRP instance and this resulted in network loop. The fix ensures that the tunnel stays down if the VRRP instance is in shutdown state.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions. | GRE | All platforms | AOS-W 8.5.0.3 |
| AOS-198261<br>AOS-202300 | — | **Symptom:** Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:f0:2).** The fix ensures that the Mobility Master works as expected.<br>**Scenario:** This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions. | switch-Platform | All platforms | AOS-W 8.3.0.0 |
| AOS-198266 | — | **Symptom:** MAC authenticated clients were unable to reauthenticate even after enabling reauthentication. The fix ensures that the user is deauthenticated and then, reauthenticated when the server times out.<br>**Scenario:** This issue occurred when the server timed out and reauthentication was not triggered. This issue was observed in stand-alone switches running AOS-W 8.0.0.0 or later versions. | Authentication | All platforms | AOS-W 8.5.0.5 |
| AOS-198364 | — | **Symptom:** A few APs in AM mode were unable to detect the neighboring 2.4 GHz channels. The fix ensures that the APs can detect 2.4 GHz channels.<br>**Scenario:** This issue occurred when the AP was power cycled. This issue was observed in APs running AOS-W 8.5.0.3 or later versions. | AP-Wireless | All platforms | AOS-W 8.5.0.3 |
| AOS-198488 | — | **Symptom:** An AP rebooted unexpectedly and set an **F** flag. The fix ensures that the AP work as expected.<br>**Scenario:** This issue occurred when an 802.1X client was connected to the AP in bridge mode or tunnel mode for wired 802.1X authentication. This issue was observed in OAW-AP205H and OAW-AP303H access points running AOS-W 8.5.0.3 or later versions. | AP-Platform | OAW-AP205H and OAW-AP303H access points | AOS-W 8.5.0.3 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-198511 | — | **Symptom:** A few managed devices displayed an error, **Similar name certificate already exists on the same or different path. upload with a different name** when a new certificate was uploaded. The fix ensures that the error message is not displayed.<br>**Scenario:** This issue occurred when the same new certificate was uploaded with its old name and the certificate manager received the **crypto pki-import** command twice for a single certificate addition. This issue was observed in managed devices running AOS-W 8.4.0.5 or later versions. | Certificate Manager | All platforms | AOS-W 8.4.0.5 |
| AOS-198605 | — | **Symptom:** A few APs failed to transition to a standby managed device during a datacenter failover. The fix ensures that the APs failover to the standby managed device.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions. | Cluster-Manager | All platforms | AOS-W 8.3.0.10 |
| AOS-198780 | — | **Symptom:** A few OAW-4104 switches did not detect the Huawei E3372s-153 (HiLink Mode) 4G LTE USB Modem. The fix ensures that the modem is detected.<br>**Scenario:** This issue was observed in OAW-4104 switches running AOS-W 8.5.0.0 or later versions. | switch-Platform | OAW-4104 switches | AOS-W 8.5.0.0 |
| AOS-198822<br>AOS-203559<br>AOS-203959 | — | **Symptom:** The **show iap table, show user-table internal**, and **show global-user-table list** commands did not display entries in the output. The fix ensures that the commands work as expected.<br>**Scenario:** This issue occurred after upgrading to AOS-W 8.4.0.4. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions. | Web Server | All platforms | AOS-W 8.4.0.4 |
| AOS-198825 | — | **Symptom:** A managed device displayed multiple stale entries when the **client-match pending events** command was executed.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | ClientMatch | All platforms | AOS-W 8.3.0.0 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-198834<br>AOS-200088<br>AOS-200555<br>AOS-201312 | — | **Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **rebooted due to Soft Watchdog reset (Intent:cause:register de:86:70:4).** The fix ensures that the managed device works as expected.<br>**Scenario:** This issue was observed in OAW-4750XM switches running AOS-W 8.3.0.10 or later versions. | switch Platform | OAW-4750XM switches | AOS-W 8.3.0.10 |
| AOS-199012<br>AOS-198865 | — | **Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed device works as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions. | switch-Datapath | All platforms | AOS-W 8.4.0.4 |
| AOS-199119 | — | **Symptom:** IPv6 DNS address, 2001:4860:4860::8888 was not reachable from source ports 33536 and higher. The fix ensures that during MLD snooping, packets are forwarded over port-channel as well.<br>**Scenario:** This issue occurred because UDP packets were treated as ICMPv6 packet and the packets were dropped. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions. | IPv6 | All platforms | AOS-W 8.0.0.0 |
| AOS-199184 | — | **Symptom:** Wired clients lost connectivity and the managed devices took a long time to recover from an uplink failure. The fix ensures that the managed devices work as expected.<br>**Scenario:** This issue occurred when the managed devices were using PPPoE as an uplink. This issue was observed in managed devices running AOS-W 8.3.0.12 or later versions. | PPPoE | All platforms | AOS-W 8.3.0.12 |
| AOS-199238 | — | **Symptom:** A managed device displayed the error log, **ctamon_gsm_update_section_intf_stats: Failed to Update GSM section intf_stats for , intf_num:0x40e3d6e0, error 43, error_htbl_key_not_found.** The fix ensures that the managed device works as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions. | switch-Datapath | All platforms | AOS-W 8.4.0.4 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-199381 | — | **Symptom:** Users were unable to connect to the backup SSID of a OAW-RAP. The fix ensures that the users are able to connect to the backup SSID of a OAW-RAP.<br>**Scenario:** This issue occurred when the users tried to connect after an AP reboot. This issue is observed in OAW-RAPs running AOS-W 8.6.0.1 or later versions. | RAP+BOAP | All platforms | AOS-W 8.6.0.2 |
| AOS-199420 | — | **Symptom:** Clients roam between APs that are deployed in different clusters. The fix ensures that the clients do not roam between APs that are deployed in different clusters.<br>**Scenario:** This issue was observed in access points running AOS-W 8.2.2.2 or later versions. | ClientMatch | All platforms | AOS-W 8.2.2.2 |
| AOS-199539 | — | **Symptom:** All the profiles listed under an AP group got marked as default except the VAP profile. The fix ensures that the profiles are marked correctly.<br>**Scenario:** This issue was observed in APs running AOS-W 8.5.0.4 or later versions. | AP-Platform | All platforms | AOS-W 8.5.0.4 |
| AOS-199663 | — | **Symptom:** The configuration changes and the mesh auto settings were reset automatically. The fix ensures that the APs work as expected.<br>**Scenario:** This issue occurred after a reboot of mesh auto APs. This issue was observed in APs running AOS-W 8.5.0.4 or later versions. | Mesh | All platforms | AOS-W 8.5.0.5 |
| AOS-199868 | — | **Symptom:** MAC clients lost connectivity when they roamed between APs. The fix ensures seamless connectivity.<br>**Scenario:** This issue occurred when machine authentication was enabled. This issue was observed in APs running AOS-W 8.6.0.0 or later versions. | 802.1X | All platforms | AOS-W 8.6.0.0 |
| AOS-199878<br>AOS-198897<br>AOS-200006<br>AOS-200080 | — | **Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: CPU stall**. The fix ensures that the AP work as expected.<br>**Scenario:** This issue was observed in OAW-AP303H access points running AOS-W 8.5.0.4 or later versions. | AP-Wireless | OAW-AP303H access points | AOS-W 8.5.0.4 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-199884 | — | **Symptom:** Mobility Master logged the following error messages:<br>■ **PAPI_Free: This buffer 0x4f6c48 may already be freed**<br>■ **PAPI_Free: Bad state index 0 state 0x1.**<br>The fix ensures that the error message is not displayed.<br>**Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. | VRRP | All platforms | AOS-W 8.5.0.5 |
| AOS-199926 | — | **Symptom:** The **show ip ospf database** command displayed the **Link State ID** in reverse endian order and hence, OSPF neighbors received routes in reverse endian order. The fix ensures that **Link State IDs** are displayed in the correct order.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions. | OSPF | All platforms | AOS-W 8.6.0.2 |
| AOS-199933 | — | **Symptom:** A Mobility Master failed to synchronize the RAP whitelist from Activate. The fix ensures that the Mobility Master works as expected.<br>**Scenario:** This issue occurred when the full-name or the description fields of a RAP whitelist entry had a space. This issue was observed in Mobility Masters running AOS-W 8.4.0.4 or later versions. | CPsec-Whitelist Management | All platforms | AOS-W 8.4.0.4 |
| AOS-199989 | — | **Symptom:** Managed devices crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**. The fix ensures that the managed devices work as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions. | switch-Datapath | All platforms | AOS-W 8.6.0.2 |
| AOS-200014 | — | **Symptom:** Clients failed to connect to a GHz network broadcasted by OAW-AP510 Series access points. Enhancements to the wireless driver resolved the issue.<br>**Scenario:** This issue was observed in OAW-AP510 Series access points running AOS-W 8.6.0.2 or later versions. | AP-Wireless | OAW-AP510 Series access points | AOS-W 8.6.0.2 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-200071 | — | **Symptom:** Some clients were getting the **U-APSD disabled in association** response though they were able to connect to an SSID without any issues. Therefore, the clients were unable to enter power saving mode and reduced the talk time from 12 hours to 3 hours. The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in APs running AOS-W 8.3.0.0 or later versions. | Station Management | All platforms | AOS-W 8.6.0.2 |
| AOS-200084 | — | **Symptom:** A few APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT**. The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in OAW-AP305 access points running AOS-W 8.4.0.4 or later versions. | AP-Wireless | OAW-AP305 access points | AOS-W 8.4.0.4 |
| AOS-200130 | — | **Symptom:** Users were unable to change the port status to trusted or untrusted using either WebUI or CLI. The fix ensures that the users are able to change the port status.<br>**Scenario:** This issue was observed in stand-alone switches running AOS-W 8.5.0.2 or later versions. | Interface | All platforms | AOS-W 8.5.0.2 |
| AOS-200187 | — | **Symptom:** A Mobility Master assigned duplicate IP addresses to Branch office switches from the VLAN pool. The fix ensures that the Mobility Master does not assign duplicate IP addresses.<br>**Scenario:** This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. | BOC | All platforms | AOS-W 8.5.0.5 |
| AOS-200252 | — | **Symptom:** APs logged the error message, **wlc_isr:MI_BUS_ERROR: MI_PSMX_INT 0x28002440, wlc_hw->clk:1**. The fix ensures that APs work as expected.<br>**Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.2 or later versions. | AP-Wireless | OAW-AP515 access points | AOS-W 8.6.0.2 |
| AOS-200275 | — | **Symptom:** When the **interface gigabitethernet no description** command was executed, the GE0/0/0 value was sent by default. This issue is resolved by removing the default description when the **no description** command is executed.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.2.2.6 or later versions. | switch-Platform | All platforms | AOS-W 8.2.2.6 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-200319 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic: WLAN FW crashes with Assertion vdev_handle->type == WAL_VDEV_TYPE_STA failed.** Enhancements to the wireless driver fixed the issue.<br>**Scenario:** This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.7 or later versions. | AP-Wireless | OAW-AP535 and OAW-AP555 access points | AOS-W 8.5.0.7 |
| AOS-200442 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **WLAN FW Crash at ar_wal_peer.c:7218 Assertion !CHK_TID_FLG(ptid, WAL_TID_IN_SCHEDQ) failed.** The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.7 or later versions. | AP - Wireless | OAW-AP535 access points | AOS-W 8.5.0.7 |
| AOS-200446 | — | **Symptom:** Some users were unable to change the cluster Profile under **Configuration > Services > Cluster** tab of the WebUI. The fix ensures that users are able make changes to the cluster Profile.<br>**Scenario:** This issue occurred when there was no VRRP ID configured but the cluster Profile requested for a VRRP passphrase. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions. | WebUI | All platforms | AOS-W 8.5.0.5 |
| AOS-200462 | — | **Symptom:** A few managed devices did not respond to the SNMP queries from OmniVista 3600 Air Manager regarding rogue information. The fix ensures that managed devices respond to SNMP queries.<br>**Scenario:** This issue occurred when:<br>■ there was a mismatch in the message length between **WMS** process and **AM** process.<br>■ the managed device was running a higher version of AOS-W than that of the AP.<br>This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions. | Air Management-IDS | All platforms | AOS-W 8.3.0.8 |
| AOS-200534<br>AOS-203370 | — | **Symptom:** The output of the **show ap active** command displays **SA (AAC=0.0.0.0)**. The fix ensures that the output of the **show ap active** command displays the correct values.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.7 or later versions. | Mesh | All platforms | AOS-W 8.5.0.7 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-200566 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **wlc_txq_enq_spq+0x3c/0x158 crash**. The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.2 or later versions. | AP-Wireless | OAW-AP515 access points | AOS-W 8.5.0.2 |
| AOS-200699<br>AOS-200760 | — | **Symptom:** Some users were unable to delete the configured SNMP V3 trap hosts. The fix ensures that users can delete SNMP v3 trap hosts.<br>**Scenario:** This issue occurred when IPv4 and IPv6 address type flags were missing. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions. | SNMP | All platforms | AOS-W 8.5.0.0 |
| AOS-200733 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8.** The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in APs running AOS-W 8.5.0.3 or later versions. | AP-Wireless | All platforms | AOS-W 8.5.0.3 |
| AOS-201042 | — | **Symptom:** A large number of packet drops were observed in a few APs. The fix ensures that the APs work as expected.<br>**Scenario:** This issue occurred when the AP SAP MTU datapath tunnel was set to 1514. This issue was observed in APs running AOS-W 8.3.0.6 or later versions. | AP Datapath | All platforms | AOS-W 8.3.0.6 |
| AOS-201117 | — | **Symptom:** Some users observed a constant increase in the **Rx Failure** parameter values under the **show datapath frame apname** command output. The fix ensures that the correct **Rx Failure** values are displayed.<br>**Scenario:** This issue occurred due to a misinterpretation between the **Rx Failure** and the **Rx Packets** values. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | AP Datapath | All platforms | AOS-W 8.3.0.0 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-201138 | — | **Symptom:** The VLAN broadcast-multicast traffic optimization configured in a managed device blocked FDB update messages generated by the managed device. The fix ensures that broadcast-multicast traffic optimization allows the FDB update frames to pass.<br>**Scenario:** This issue occurred when the **fdb-update-on-assoc** parameter under **wlan virtual-ap <profile-name>** command was enabled in a Layer-2 cluster. This issue was observed in managed devices and stand-alone switches running AOS-W 8.5.0.5 or later versions. | switch-Datapath | All platforms | AOS-W 8.5.0.5 |
| AOS-201152 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **AP Reboot reason: BUGSoftLockup:CPU#1 stuck for 22s! [kworker/1:2:2288] PC:_ udelay+0x30/0x48 Warm-reset.** The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.6 or later versions. | AP-Wireless | OAW-AP515 access points | AOS-W 8.5.0.6 |
| AOS-201210 | — | **Symptom:** When the **show aaa authentication-server radius statistics** command was executed, a few RADIUS authentication servers always displayed the **expAuthTm** value as 0. The fix ensures that RADIUS authentication servers display the correct **expAuthTm** value.<br>**Scenario:** This issue was observed when the managed devices were upgraded to AOS-W 8.5.0.5 or later versions. | RADIUS | All platforms | AOS-W 8.5.0.5 |
| AOS-201329 | — | **Symptom:** CPsec toggling stopped working after upgrading to AOS-W 8.5.0.8. The fix ensures that CPsec toggling works as expected.<br>**Scenario:** This issue occurred when CPsec was disabled at multiple node levels and re-enabled only at the higher node level. This resulted in an override of CPsec configurations at the lower node levels. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions. | Configuration | All platforms | AOS-W 8.3.0.10 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-201612 | — | **Symptom:** Role and policies configured on a Mobility Master were displayed in a different order on the managed devices in the **Configuration > Roles & Policies > Roles** tab. Hence, the managed device denied traffic. The fix ensures that the policies are displayed in the correct order.<br>**Scenario:** This issue occurred when the default ACLs got deleted during the initial configuration synchronization after an upgrade. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. | Configuration | All platforms | AOS-W 8.3.0.8 |
| AOS-201831 | — | **Symptom:** The **S-UAC** process in a cluster member sent the **fdb-update-on-assoc** message sporadically. This issue is resolved by sending the **fdb-update-on-assoc** message only when **fdb-update-on-assoc** is enabled and the station is not dormant.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.5 in a cluster topology. | Station Management | All platforms | AOS-W 8.5.0.5 |
| AOS-202110 | — | **Symptom:** The **Active Controller** field displayed a hyphen (-) for some APs under **Dashboard > Infrastructure > Access Devices** page in the WebUI. The fix ensures that the WebUI displays the list of active switches.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions. | Monitoring | All platforms | AOS-W 8.5.0.6 |
| AOS-202195 | — | **Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the managed device works as expected.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions. | IPsec | All platforms | AOS-W 8.3.0.6 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-202257 | — | **Symptom:** A few OAW-40xx Series switches displayed the warning message, **At least 1000 MB of free flash space is recommended to keep the system stable. Please clean up your flash filesystem** although some controllers in the series have less than1GB memory allocated to it. This issue is resolved by changing the warning message to A**t least 600 MB of free flash space is recommended to keep the system stable. Please clean up your flash filesystem.**<br>**Scenario:** This issue was observed in OAW-40xx Series switches running AOS-W 8.5.0.10. | switch-Platform | All platforms | AOS-W 8.5.0.10 |
| AOS-202341 | — | **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 54:86:0:2c).**<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions. | switch-Datapath | All platforms | AOS-W 8.3.0.8 |
| AOS-202450 | — | **Symptom:** OAW-RAPs rebooted unexpectedly. The fix ensures that the OAW-RAPs work as expected.<br>**Scenario:** This issue occurred when the **activate whitelist download** command was executed and the Mobility Master modified the existing whitelist database entries. This issue was observed in OAW-RAPs running AOS-W 8.5.0.7 or later versions. | Base OS Security | All platforms | AOS-W 8.5.0.7 |
| AOS-202515<br>AOS-202658 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file lists the reason for the event as **Panic:assert Warm-reset**. The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in APs running AOS-W 8.5.0.2 or later versions. | AP Datapath | All platforms | AOS-W 8.5.0.2 |
| AOS-202551 | — | **Symptom:** An AP displayed an error message, **An internal system error has occurred at file parser.c function parse_mgmt line 656 error parse_mgmt Size mismatch on frame** multiple times. The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.7 or later versions. | AP-Wireless | OAW-AP535 access points | AOS-W 8.5.0.7 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-202691 | — | **Symptom:** The **Key Management** column in the **Configuration > WLANs** page of the WebUI displays multiple **wpa2-psk-tkip** entries. The fix ensures that multiple **wpa2-psk-tkip** entries are not displayed.<br>**Scenario:** This issue occurred when multiple wpa2-psk-tkip opmode SSIDs were created. This issue was observed in stand-alone switches running AOS-W 8.5.0.4 or later versions. | WebUI | All platforms | AOS-W 8.5.0.4 |
| AOS-202739 | — | **Symptom:** A few APs displayed the error message, **WPA Passphrase not configured for AP**. The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in APs running AOS-W 8.3.0.9 or later versions. | Base OS Security | All platforms | AOS-W 8.3.0.9 |
| AOS-202754 | — | **Symptom:** A few APs failed to display the association status of IoT devices in the output of **show ap debug mgmt-frames** command. The fix ensures that the association status of IoT devices are displayed in the output.<br>**Scenario:** This issue was observed in OAW-AP300 Series access points running AOS-W 8.6.0.2 or later versions. | AP-Wireless | OAW-AP300 Series access points | AOS-W 8.6.0.2 |
| AOS-202816<br>AOS-203413 | — | **Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the managed device works as expected.<br>**Scenario:** This issue occurred when SSL-fallback enabled VIA clients were connected to the managed device. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. | switch-Datapath | All platforms | AOS-W 8.3.0.0 |
| AOS-203183 | — | **Symptom:** Users are unable to perform SNMPGET and an error message, **No Such Instance currently exists at this OID** was displayed. The fix ensures that SNMPGET works as expected on OIDs returned by other SNMP get operations.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions. | SNMP | All platforms | AOS-W 8.6.0.2 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-203219 | — | **Symptom:** The URL hash key was not appended to the captive portal redirect URL. The fix ensures that the URL hash key is hashed to the redirect URL.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions. | Captive Portal | All platforms | AOS-W 8.6.0.4 |
| AOS-203322 | — | **Symptom:** The command **tar clean logs** did not remove the logs.tar.7z file. The fix ensures that the command works as expected.<br>**Scenario:** This issue was observed Mobility Masters running AOS-W 8.5.0.10. | switch-Platform | All platforms | AOS-W 8.5.0.10 |
| AOS-203357 | — | **Symptom:** The fix ensures that the user role is updated. Traffic outage was observed in managed devices when the role of wired user got updated as a tunneled user with a different VLAN.<br>**Scenario:** This issue occurred when there was a delay in the 802.11X authentication and the use role was not updated. This issue was observed in stand-alone controllers running AOS-W 8.5.0.10. | Tunnel node Manager | All platforms | AOS-W 8.5.0.10 |
| AOS-203374 | — | **Symptom:** VIA authentication timed out although the server responded without any delay. The fix ensures that the VIA authentication works without delay.<br>**Scenario:** This issue was observed in OAW-4550 switches running AOS-W 8.0.0.0 or later versions. | IPsec | OAW-4550 switches | AOS-W 8.3.0.0 |
| AOS-203398 | — | **Symptom:** A stand-alone switch sent invalid time stamp values to the server. The fix ensures that incorrect time stamp values are not sent to the server.<br>**Scenario:** This issue was observed in stand-alone switches running AOS-W 8.6.0.3 or later versions | IoT | All platforms | AOS-W 8.6.0.3 |
| AOS-203418 | — | **Symptom:** A OAW-RAP failed to come up and the OAW-RAP ignored the certificates of the Mobility Controller Virtual Appliance. The fix ensures that the OAW-RAP works as expected.<br>**Scenario:** This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.6.0.4 or later versions. | IPsec | All platforms | AOS-W 8.6.0.4 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-203585<br>AOS-204245 | — | **Symptom:** APs logged the error message, **aruba_change_channel 735 Waiting for VAP INIT to complete**. This issue is resolved by changing the logging level to debug.<br>**Scenario:** This issue was observed in access points running AOS-W 8.3.0.0 or later versions. | AP-Wireless | All platforms | AOS-W 8.3.0.0 |
| AOS-203859 | — | **Symptom:** Windows clients were unable to get WINS server information from the Mobility Master. The fix ensures that Windows clients are able to get WINS server information from the Mobility Master.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.11 or later versions. | IPsec | All platforms | AOS-W 8.3.0.11 |
| AOS-204367 | — | **Symptom:** When the **show crypto ipsec sa** command was executed, the Map name was not displayed in the output The fix ensures that the command displays the map name.<br>**Scenario:** This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions. | IPsec | All platforms | AOS-W 8.5.0.8 |
| AOS-204390 | — | **Symptom:** RADIUS source interface was not working on a managed device. The fix ensures that RADIUS source interfacing works as expected.<br>**Scenario:** This issue occurred when RadSec was enabled. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions. | Base OS Security | All platforms | AOS-W 8.5.0.8 |
| AOS-204428<br>AOS-204450 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.<br>**Scenario:** This issue was observed in OAW-AP303H access points running AOS-W 8.3.0.0 or later versions. | AP-Wireless | OAW-AP303H access points | AOS-W 8.3.0.0 |
| AOS-204532 | — | **Symptom:** Configurations committed on the managed devices were not available on the Mobility Master during backup. The fix ensures that the configurations are available on the Mobility Master.<br>**Scenario:** This issue occurred when the node-name or path limit exceeded 99 characters. This issue was observed in managed devices running AOS-W 8.4.0.1 or later versions. | Configuration | All platforms | AOS-W 8.4.0.1 |

**Table 6:** *Resolved Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-204917<br>AOS-205979 | — | **Symptom:** The **dpagent** process crashed on a managed device and the managed device log the error message, **Memory usage limit exceeded for process: dpagent current pages.** The fix ensures that the managed device works as expected.<br>**Scenario:** This issue occurred due to high memory utilization. This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions. | switch-Datapath | All platforms | AOS-W 8.5.0.1 |
| AOS-205128<br>AOS-202985 | — | **Symptom:** APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Rebooting the AP because of FW ASSERT**. The fix ensures that APs work as expected.<br>**Scenario:** This issue occurred due to a channel change. This issue was observed in OAW-AP300 Series, OAW-AP303 Series, OAW-AP303H Series, OAW-AP310 Series, OAW-AP318 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP344, OAW-AP360 Series, OAW-AP370 Series, and OAW-AP387 access points running AOS-W 8.5.0.6 or later versions. | AP-Wireless | OAW-AP300 Series, OAW-AP303 Series, OAW-AP303H Series, OAW-AP310 Series, OAW-AP318 Series, OAW-AP320 Series, OAW-AP330 Series, OAW-AP344, OAW-AP360 Series, OAW-AP370 Series, and OAW-AP387 access points | AOS-W 8.5.0.6 |
| AOS-201250 | — | **Symptom:** Some managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - low on free memory.** The fix ensures that the managed devices work as expected.<br>**Scenario:** This issue was not limited to any switch platform or AOS-W release version. | Base OS Security | All platforms | AOS-W 8.5.0.5 |
| | | | | | |

# Chapter 6
# Known Issues and Limitations

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

NOTE

We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

## Limitation

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

NOTE

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

## Known Issues

Following are the known issues observed in this release.

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-131325<br>AOS-146748 | 159222<br>179137 | **Symptom:** An incorrect number of clients are displayed in the **Dashboard > Overview > Clients >Wireless Clients table > active-standby IP field** page of the WebUI<br>**Scenario:** This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running AOS-W 8.1.0.0 or later versions.<br>**Workaround:** None. | Base OS Security | All platforms | AOS-W 8.1.0.0 |
| AOS-145410<br>AOS-146962 | 177352<br>179430 | **Symptom:** A managed device crashes and reboots with the error message, **Atleast 2000 MB free flash is recommended to keep system stable. Please clean up your flash file.**<br>**Scenario:** This issue occurs when a managed device receives IP packets larger than one segment. This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions.<br>**Workaround:** None. | switch-Platform | All platforms | AOS-W 8.2.0.2 |
| AOS-145566 | 177559 | **Symptom:** A Mobility Master is unable to forward the traffic that is sourced from an IP interface in the gateway.<br>**Scenario:** This issue occurs when netdestinations are used in the routing ACL rule. This issue is observed in Mobility Masters running AOS-W 8.0.1.0 or later versions.<br>**Workaround:** None. | Policy-Based Routing | All platforms | AOS-W 8.0.1.0 |
| AOS-151022<br>AOS-188417 | 185176 | **Symptom:** The output of the **show datapath uplink** command displays an incorrect session count.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.<br>**Workaround:** None. | switch-Datapath | All platforms | AOS-W 8.1.0.0 |
| AOS-151355 | 185602 | **Symptom:** A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.<br>**Workaround:** None. | Policy-Based Routing | All platforms | AOS-W 8.0.1.0 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-153185 | 188148 | **Symptom:** The **Dashboard > Security > Active rogue > Locate** option does not function in the WebUI.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.1 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.3.0.1 |
| AOS-153742<br>AOS-194948 | 188871 | **Symptom:** A stand-alone switch crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**.<br>**Scenario:** This issue is observed in OAW-4010 switches running AOS-W 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.<br>**Workaround:** None. | switch- Datapath | OAW-4010 switches | AOS-W 8.5.0.1 |
| AOS-155801 | 191726 | **Symptom:** The SNMP walk performed from OmniVista 3600 Air Manager does not produce correct results.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.3.<br>**Workaround:** None. | SNMP | All platforms | AOS-W 8.3.0.3 |
| AOS-156068 | 192100 | **Symptom:** The **DDS** process in a managed device crashes unexpectedly.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions.<br>**Workaround:** None. | Base OS Security | All platforms | AOS-W 8.2.1.1 |
| AOS-156742<br>AOS-156977 | 193031<br>193319 | **Symptom:** A user is unable to make any change to IP Probe configuration, after forwarding a complete configuration using API.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.0.1.0 |
| AOS-157492 | 194064 | **Symptom:** VRRP authentication fails in a managed device.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0.<br>**Workaround:** None. | VRRP | All platforms | AOS-W 8.2.1.0 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-157795 | 194516 | **Symptom:** A few managed devices are unable to process two **APN usb-init** strings using the **uplink cellular apn** command with Huawei E3372 modem.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.<br>**Workaround:** None. | switch-Platform | All platforms | AOS-W 8.3.0.6 |
| AOS-182847 | — | **Symptom:** A few users are unable to copy the **WPA Passphrase** field and **High-throughput** profile to a new SSID profile using the **Configuration > System > Profiles > Wireless LAN > SSID > <SSID_Profile>** option in the WebUI.<br>**Scenario:** This issue occurs when a new SSID profile is created from an existing SSID profile in the WebUI. This issue is observed in managed devices running AOS-W 8.4.0.0 in a Mobility Master-Managed Device topology.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.4.0.0 |
| AOS-183226<br>AOS-195616<br>AOS-196228<br>AOS-193980<br>AOS-197435 | — | **Symptom:** A few clients lose L3 connectivity though the L2 connectivity is up.<br>**Scenario:** This issue occurs when the client enters power saving mode and the AP queues packets. This issue is observed in OAW-AP200 Series access points running AOS-W 8.3.0.0 or later versions.<br>**Workaround:** None. | AP-Wireless | OAW-AP200 Series access points | AOS-W 8.3.0.0 |
| AOS-183706 | — | **Symptom:** The tx radio power of a few APs are lesser than the tx radio power of other APs in the same network.<br>**Scenario:** This issue is observed in APs running AOS-W 8.3.0.6 or later versions.<br>**Workaround:** None. | AP-Wireless | All platforms | AOS-W 8.3.0.6 |
| AOS-184135<br>AOS-195866 | — | **Symptom:** A few users are unable to download applications from Google Play Store.<br>**Scenario:** This issue occurs when the YouTube application is blocked. This issue is observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.<br>**Workaround:** None. | switch-Datapath | All platforms | AOS-W 8.4.0.0 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-184801 | — | **Symptom:** A few managed devices crash and reboot unexpectedly. The log files list the reason for the event as **Datapath exception**.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0.<br>**Workaround:** None. | switch -Datapath | All platforms | AOS-W 8.4.0.0 |
| AOS-184947<br>AOS-192737 | — | **Symptom:** The jitter and health score data are missing from the **Dashboard > Infrastructure > Uplink > Health** page in the WebUI.<br>**Scenario:** This issue is observed in Mobility Master running AOS-W 8.4.0.4 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.4.0.4 |
| AOS-185538 | — | **Symptom:** A high number of EAP-TLS timeouts are observed in a managed device.<br>**Scenario:** This issue occurs because multiple IP addresses are assigned to each client. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions. | Base OS Security | All platforms | AOS-W 8.3.0.8 |
| AOS-186133 | — | **Symptom:** A few managed devices display abnormally high multicast traffic in **Performance Summary > All Radios** monitoring page.<br>**Scenario:** This issue is observed in OAW-AP320 Series access points running AOS-W 8.3.0.6.<br>**Workaround:** None. | AP-Wireless | OAW-AP320 Series access points | AOS-W 8.3.0.6 |
| AOS-186774 | — | **Symptom:** When the **show memory cfgm** command is executed, a large memory allocation is displayed in the output of the command.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.3.0.6 |
| AOS-187115 | — | **Symptom:** The application name is incorrect in the **Configuration > Roles & Policies > Policies > <Policy name>** policy configuration WebUI page.<br>**Scenario:** This issue occurs when the WebUI is accessed for the first time. This issue is observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.2.2.0 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-187422<br>AOS-189258 | — | **Symptom:** The output of **show log all** and **show audit-trail** commands displays the unencrypted password entered for non-profile commands such as **aaa test-server** command.<br>**Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.3.0.5 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.3.0.5 |
| AOS-187834 | — | **Symptom:** A few APs do not send Port VLAN IDs in an LLDP packet although the **native-vlan-id** parameter is set using the **ap system-profile** command.<br>**Scenario:** This issue is observed in APs running AOS-W 8.2.2.0 or later versions.<br>**Workaround:** None. | AP-Platform | All platforms | AOS-W 8.2.2.5 |
| AOS-187911 | — | **Symptom:** The **Wireless Clients** section of the **Dashboard > Overview** page in the WebUI displays incorrect client usage values.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.<br>**Workaround:** Add a tooltip over the usage tab to mention that the current client usage value accounts for the last 15 min. | WebUI | All platforms | AOS-W 8.4.0.0 |
| AOS-188090<br>AOS-196004<br>AOS-199152 | — | **Symptom:** The **Dashboard > Overview > Clients** page of the WebUI displays incorrect usage values intermittently.<br>**Scenario:** This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions.<br>**Workaround:** None. | Monitoring | All platforms | AOS-W 8.4.0.0 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-188285 | — | **Symptom:** A mesh portal reboots continuously because the **wpa_hex_key** value exceeds more than 132 bytes string in **the ap mesh-recovery-profile cluster <cluster_id> wpa-hexkey <wpa_hex_key>** command. The log files list the reason for the event as **AP rebooted Tue Jun 11 10:40:01 CDT 2019; Critical process /aruba/bin/meshd [pid 2450] DIED, process marked as RESTART**.<br>**Scenario:** This issue is observed in APs running AOS-W 8.3.0.7 as a mesh portal.<br>**Workaround:**<br>■ Modify **mesh-recovery-profile** by using **mesh-recovery-generate** command.<br>■ Reboot the mesh portal and issue the **setenv mesh_role 0** command on apboot in the console port of the AP.<br>■ Reprovision the AP to mesh portal. | Mesh | All platforms | AOS-W 8.3.0.7 |
| AOS-188478 | — | **Symptom:** The OAW-RAP whitelist file does not contain the first MAC address entry.<br>**Scenario:** This issue occurs when the user executes the **show whitelist-db rap export-css <filename>** command to export the OAW-RAP whitelist file to the switch directory. This issue is observed in stand-alone switches running AOS-W 8.3.0.5 or later versions.<br>**Workaround:** None. | Local Database | All platforms | AOS-W 8.3.0.5 |
| AOS-190071<br>AOS-190372 | — | **Symptom:** A few users are unable to access websites when WebCC is enabled on the user role.<br>**Scenario:** This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0.<br>**Workaround:**<br>Perform the following steps to resolve the issue:<br>■ Remove web category from the ACL rules and apply **any any any permit** policy.<br>■ Disable WebCC on the user role.<br>■ Change the VLAN of user role from trunk mode to access mode. | WebCC | OAW-4005 switches | AOS-W 8.4.0.0 |
| AOS-190240<br>AOS-192168 | — | **Symptom:** The SNMP OIDs provide incorrect result in a cluster setup.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.<br>**Workaround:** None. | SNMP | All platforms | AOS-W 8.3.0.0 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-191539 | — | **Symptom:** The configuration synchronization fails and **CONFIG Failure** is displayed as the status of the synchronization displays in a managed device. The log files list the **Error: Tunnel is an L2 GRE Tunnel, Delete the Vlans, before changing the mode." executing "tunnel mode gre 2048** error message.<br>**Scenario:** This issue occurs when the interface tunnel is set as 2048. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.<br>**Workaround:** None. | Interface | All platforms | AOS-W 8.4.0.1 |
| AOS-192725<br>AOS-190476<br>AOS-196004 | — | **Symptom:** The **Dashboard > Overview** page of the WebUI displays incorrect number of users intermittently.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.8 or later versions.<br>**Workaround:** None. | Monitoring | All platforms | AOS-W 8.3.0.8 |
| AOS-192738<br>AOS-197047 | — | **Symptom:** The Mobility Master list in the WebUI incorrectly displays the mac address of the primary Mobility Master for the secondary Mobility Master.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.10 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.3.0.10 |
| AOS-193083 | — | **Symptom:** The cluster upgrade fails on a 2-node cluster because the AP platform capacity of the managed device is only 4 and the hash table size is calculated as zero.<br>**Scenario:** This issue is observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions.<br>**Workaround:** None. | Cluster-Manager | All platforms | AOS-W 8.5.0.0 |
| AOS-193184 | — | **Symptom:** All L2 connected managed devices in a cluster move to L3 connected state after an upgrade.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | Cluster-Manager | All platforms | AOS-W 8.5.0.2 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-193560<br>AOS-198565<br>AOS-200262<br>AOS-204794 | — | **Symptom:** The number of APs that are DOWN are incorrectly displayed in the WebUI. However, CLI displays the correct status of APs.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.4.0.4 |
| AOS-193775<br>AOS-194581<br>AOS-197372 | — | **Symptom:** A mismatch of AP count and client count is observed between the Mobility Master and the managed device.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.<br>**Workaround:** None. | Monitoring | All platforms | AOS-W 8.5.0.2 |
| AOS-193883<br>AOS-197756 | — | **Symptom:** A few APs are unable to use DHCP IPv6 addresses and option 52 for master discovery.<br>**Scenario:** This issue occurs when the APs do not clear the previous LMS entries after the upgrade. This issue is observed in access points running AOS-W 8.3.0.8 or later versions.<br>**Workaround:** Delete the IPv4 addresses from AP system profile using the command, **ap system-profile** and from high availability profiles using the command, **ha.** | AP Platform | All platforms | AOS-W 8.3.0.8 |
| AOS-194082<br>AOS-196092 | — | **Symptom:** A few APs crash and reboot unexpectedly. The log files lists the reason for the event as **BadPtr:00000006 PC:wlc_keymgmt_ wsec+0x28/0xa4 [wl_v6] Warm-reset.**<br>**Scenario:** This issue is observed in access points running AOS-W 8.6.0.0 or later versions.<br>**Workaround:** None. | AP-Wireless | All platforms | AOS-W 8.6.0.0 |
| AOS-194370 | — | **Symptom:** High memory utilization is observed in the **cluster manager** process of managed devices.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions in a cluster setup.<br>**Workaround:** None. | Cluster-Manager | All platforms | AOS-W 8.4.0.2 |
| AOS-194381 | — | **Symptom:** Some managed devices lose the route-cache entries and drop the VRRP IP addresses sporadically.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.<br>**Workaround:** None. | switch-Datapath | All platforms | AOS-W 8.3.0.7 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-194911 | — | **Symptom:** An incorrect flag output is displayed for APs configured with 802.1X authentication when the **show ap database** command is executed.<br>**Scenario:** This issue is observed in APs running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | AP-Platform | All platforms | AOS-W 8.5.0.2 |
| AOS-194925<br>AOS-195413 | — | **Symptom:** A branch office switch is unable to failover to a secondary VPNC managed device.<br>**Scenario:** This issue occurs because the secondary VPNC's MAC address is not updated on the running configuration of the switch. This issue is observed in Mobility Master Virtual Appliances and Branch office switches running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.5.0.2 |
| AOS-194964 | — | **Symptom:** A few users are unable to clone the configuration from an existing group to a new group in a Mobility Master.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.4.0.1 or later versions.<br>**Workaround:** Change the operating mode of the AP from am-mode to ap-mode using the **ap spectrum local-override** command. | Configuration | All platforms | AOS-W 8.5.0.2 |
| AOS-195089 | — | **Symptom:** The DNS traffic is incorrectly getting classified as Thunder and is getting blocked.<br>**Scenario:** This issue occurs when the DNS traffic is blocked and peer-peer ACL is denied for users. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.<br>**Workaround:** None. | switch-Datapath | All platforms | AOS-W 8.3.0.7 |
| AOS-195100<br>AOS-198302 | — | **Symptom:** The health status of a managed device is incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master's WebUI.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.3.0.7 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-195228 | — | **Symptom:** The device status is always displayed as inactive when SNMP walk is performed.<br>**Scenario:** This issue is observed in stand-alone switches running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | SNMP | All platforms | AOS-W 8.5.0.2 |
| AOS-195434 | — | **Symptom:** An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**.<br>**Scenario:** This issue is observed in APs running AOS-W 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology.<br>**Workaround:** None. | AP-Wireless | All platforms | AOS-W 8.5.0.2 |
| AOS-195526 | — | **Symptom:** Clients are unable to get the DHCP address.<br>**Scenario:** This issue occurs because the ACE entries of the logon role ACL changes to **Deny all** when the PEFNG feature is disabled. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions.<br>**Workaround:** None. | Base OS Security | All platforms | AOS-W 8.3.0.8 |
| AOS-195939 | — | **Symptom:** UBT users are assigned **logon** role when they receive the same IP addresses.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | Tunnel-Node-Manager | All platforms | AOS-W 8.5.0.2 |
| AOS-196115 | — | **Symptom:** Users are unable to configure untrusted VLAN in the **Configuration > Interfaces > Ports** page of the WebUI.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.5.0.0 |
| AOS-196864 | — | **Symptom:** Although a new VLAN ID is successfully connected, the managed device displays that the VLAN ID fails with a different ID.<br>**Scenario:** This issue is observed when new VLANs are added and the total number of VLANs are 100/101, 200/201, 300/301 and likewise. This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions.<br>**Workaround:** None. | Cluster-Manager | All platforms | AOS-W 8.5.0.3 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-196878<br>AOS-197216 | — | **Symptom:** The **Datapath** process crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.**<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | DPI | All platforms | AOS-W 8.5.0.2 |
| AOS-197023 | — | **Symptom:** Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.<br>**Workaround:** Either of the following steps are recommended:<br>■ In the CLI, execute the **ap regulatory-domain-profile** command to create an AP regulatory-domain-profile without any channel configuration, save the changes, and later add or delete channels as desired.<br>■ In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes, and later add or delete channels as desired in the **Configuration > AP Groups** page. | WebUI | All platforms | AOS-W 8.5.0.4 |
| AOS-197048 | — | **Symptom:** Some clients face degraded Wi-Fi download speed after the managed device resumes function post standby mode.<br>**Scenario:** This issue occurs when the AP does not setup an aggregation session. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions.<br>**Workaround:** None. | AP-Wireless | All platforms | AOS-W 8.3.0.8 |
| AOS-197127 | — | **Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2).**<br>**Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 8.3.0.7 or later versions in a cluster setup.<br>**Workaround:** None.<br>**Duplicates:** AOS-197060, AOS-197130, AOS-197137, AOS-197161, AOS-197163, AOS-198720, AOS-201821 | switch-Datapath | OAW-4x50 Series switches | AOS-W 8.3.0.7 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-197134 | — | **Symptom:** User roles are incorrectly listed as downloaded user roles and the error message, **user role already exists** is displayed.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions.<br>**Workaround:** None. | RADIUS | All platforms | AOS-W 8.5.0.3 |
| AOS-197215 | — | **Symptom:** Users are unable to delete the **Weekend** entry in **Start Day** of **Time range** field in the WebUI.<br>**Scenario:** This issue occurs when the users create a new policy rule in the **Configuration > Roles & Policies > Policies > <policy_name> > <new_policy_rule>** page, and select **Access control** radio button in the **Rule type** field of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.2.2.6 |
| AOS-197497 | — | **Symptom:** AirMatch selects the same channel for two neighboring APs even after radar detection.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions.<br>**Workaround:** None. | AirMatch | All platforms | AOS-W 8.5.0.3 |
| AOS-198281 | — | **Symptom:** The details of the **Up** time in **Managed network > Dashboard > Access Points > Access Points** table does not get updated correctly.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.2.2.6 |
| AOS-198475 | — | **Symptom:** A user is unable to upgrade a Mobility Master Virtual Appliance to AOS-W 8.5.0.0 or a later version.<br>**Scenario:** This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.5.0.0 or later versions.<br>**Workaround:** None. | switch-Datapath | All platforms | AOS-W 8.5.0.5 |
| AOS-198483 | — | **Symptom:** WebUI does not have an option to map the **rf dot11-60GHz-radio-profile** to an AP group.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.5.0.4 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-198787<br>AOS-198929 | — | **Symptom:** A OAW-RAP does not come up on a managed device when Verizon U730L modem is used.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.<br>**Workaround:** None. | OAW-RAP | All platforms | AOS-W 8.6.0.0 |
| AOS-198849<br>AOS-198850 | — | **Symptom:** Users are unable to configure 2.4 GHz radio profile in the **Configuration > System > Profiles > 2.4 GHz radio profile** page and the WebUI displays the error message, **Feature is not enabled in the license.**<br>**Scenario:** This issue is observed in stand-alone switches running AOS-W 8.5.0.3 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.5.0.3 |
| AOS-199306<br>AOS-201623 | — | **Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt [packet_lookup_frame+0x30/0x68].**<br>**Scenario:** This issue is observed in APs running AOS-W 8.3.0.6 or later versions.<br>**Workaround:** None. | AP-Wireless | All platforms | AOS-W 8.3.0.6 |
| AOS-199423 | — | **Symptom:** Some L3 redundant Mobility Masters generate **profmgr** error logs.<br>**Scenario:**. This issue is observed in Mobility Masters running AOS-W 8.5.0.5-FIPS.<br>**Workaround:** None. | Interface | All platforms | AOS-W 8.5.0.5 |
| AOS-199947 | — | **Symptom:** The **Lic. FeatureBit** parameter under the License Client Table changes to **enabled** for Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance.<br>**Scenario:** This issue occurs when EVAL license is deleted and the licenses are displayed as 0. This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.3.0.11 or later versions.<br>**Workaround:** None. | Licensing | All platforms | AOS-W 8.3.0.11 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-200765 | — | **Symptom:** Managed devices log the error message, **<199804> <4844> \|authmgr\| \|cluster\| gsm_auth.c, auth_gsm_publish_ip_user_local_section:1011: auth_gsm_publish_ip_user_local_section: ip_user_local_flags.**<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions in a cluster setup.<br>**Workaround:** None. | Cluster-Manager | All platforms | AOS-W 8.3.0.7 |
| AOS-201150<br>AOS-201997<br>AOS-204328 | — | **Symptom:** A few APs crash and reboot unexpectedly. The log file lists the reason for the event as **AP Reboot reason: External-WDT-reset.**<br>**Scenario:** This issue is observed in OAW-AP510 Series access points running AOS-W 8.6.0.2 or later versions.<br>**Workaround:** None. | AP-Platform | OAW-AP510 Series access points | AOS-W 8.6.0.2 |
| AOS-201200 | — | **Symptom:** The **show license-pool-profile** command does not display the output when executed in the **/mm/my node** hierarchy.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.6 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.5.0.5 |
| AOS-201240 | — | **Symptom:** When a trusted VLAN is added using the **Interface > Ports > Allowed VLANs** page, the Mobility Master automatically issues the **no trusted vlan** command.<br>**Scenario:** This issue occurs when trunk mode is initially configured using the CLI and later modified using the WebUI. This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.5.0.2 |
| AOS-201273 | — | **Symptom:** IPsec tunnels are not established between the Mobility Master and managed devices in an IPv6 environment, and the switch-IP address is not displayed in the managed devices.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W running ArubaOS 8.5.0.0 or later versions.<br>**Workaround:** Bring up the managed device with master IPv4 or master IPv6 address from the setup dialog, instead of configuring master IPv4 address to master IPv6 address and vice-versa. | Configuration | All platforms | AOS-W 8.6.0.0 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-201439<br>AOS-201448 | — | **Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**.<br>**Scenario:** This issue is observed in OAW-AP303H access points running AOS-W 8.5.0.5 or later versions.<br>**Workaround:** None. | AP-Wireless | OAW-AP303H access points | AOS-W 8.5.0.5 |
| AOS-202126<br>AOS-205098 | — | **Symptom:** The **profmgr** process continuously restarts on the Mobility Master and hence configurations are not pushed to the managed devices.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.5.0.8 |
| AOS-202129<br>AOS-204127 | — | **Symptom:** The **Configuration > AP groups** page does not have the **Split radio** toggle to enable the tri-radio feature.<br>**Scenario:** This issue is observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.6.0.0 |
| AOS-202290 | — | **Symptom:** The error message, **Cannot modify existing server-group from different node in config path** is displayed when users try to create or modify an aaa server group.<br>**Scenario:** This issue occurs when similar naming conventions are used for different folders under the same hierarchy. This issue is observed in Mobility Masters running AOS-W 8.5.0.6 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.5.0.6 |
| AOS-202370 | — | **Symptom:** Some managed devices reset when the **activate sync** command is issued.<br>**Scenario:** This issue occurs when the node paths that are configured for Activate and Mobility Master use different cases. This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.5.0.5 |
| AOS-202565 | — | **Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as **kfree+0x74/0xf8 crash.**<br>**Scenario:** This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.2 or later versions.<br>**Workaround:** None. | AP-Wireless | OAW-AP515 access points | AOS-W 8.5.0.2 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-202803 | — | **Symptom:** The error message, **cluster was fractured during the upgrade** is displayed during the cluster live upgrade process and therefore, cluster live upgrade cannot be performed.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.07 or later versions.<br>**Workaround:** None. | Cluster-Manager | All platforms | AOS-W 8.5.07 |
| AOS-203097 | — | **Symptom:** The WebUI prompts that additional VLANs will be deleted when a user tries to delete a VLAN.<br>**Scenario:** This issue is observed in stand-alone switches running AOS-W 8.3.0.10 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.3.0.10 |
| AOS-203170 | — | **Symptom:** The class attribute field is missing in the accounting packets of the VIA connection profile.<br>**Scenario:** This issue occurs when IKEv2 is enabled in the VIA connection profile. This issue is observed in managed devices running AOS-W 8.4.0.1 or later versions.<br>**Workaround:** None. | IPsec | All platforms | AOS-W 8.6.0.2 |
| AOS-203184 | — | **Symptom:** Users are unable to perform captive portal authentication when login URL of the captive portal profile points to ClearPass Policy Manager.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.7 or later versions.<br>**Workaround:** None. | switch-Datapath | All platforms | AOS-W 8.5.0.7 |
| AOS-203201 | — | **Symptom:** The managed device is unable to download configurations from the Mobility Master using VPNC.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.2.2.6 or later versions.<br>**Workaround:** None. | Configuration | All platforms | AOS-W 8.2.2.6 |
| AOS-203336 | — | **Symptom:** The **Dashboard > Infrastructure > Access Points** page of the WebUI and the **show log** command display different values for the last AP reboot time.<br>**Scenario:** This issue is observed in stand-alone switches running AOS-W 8.5.0.5 or later versions.<br>**Workaround:** None. | WebUI | All platforms | AOS-W 8.5.0.5 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-203597<br>AOS-203927 | — | **Symptom:** The number of VIA licenses used are higher than the total number of users connected to VIA.<br>**Scenario:** This issue occurs when VIA clients initiate IKE exchange with incomplete details and hence, fail to establish IKE tunnels with managed devices. This issue is observed in managed devices running AOS-W 8.2.0.0 or later versions.<br>**Workaround:** Reboot the managed device to restore the VIA licenses. | IPsec | All platforms | AOS-W 8.5.0.6 |
| AOS-203698 | — | **Symptom:** A mismatch is observed in ACL positions between the Mobility Master and the managed devices.<br>**Scenario:** This issue occurs when the ACLs of the user-role are changed. This issue is observed in Mobility Masters and managed devices running AOS-W 8.5.0.6 or later versions.<br>**Workaround:** None. | Base OS Security | All platforms | AOS-W 8.5.0.6 |
| AOS-203712 | — | **Symptom:** Avaya Spectalink wireless phones reboot unexpectedly with the error message, **No AVPP response from 192.168.249.001.**<br>**Scenario:** This issue occurs because of the IP packet size. This issue is observed in managed devices running AOS-W 8.5.0.7 or later versions.<br>**Workaround:** None. | Base OS Security | All platforms | AOS-W 8.5.0.7 |
| AOS-204414 | — | **Symptom:** The VLAN range configured using the **ntp-standlaone vlan-range** command are not correctly sent to the managed devices.<br>**Scenario:** This issue occurs when the user repeatedly modifies the VLAN range. This issue occurs in Mobility Masters running AOS-W 8.0.1.0 or later versions.<br>**Workaround:** Delete the VLAN range configured on the Mobility Master and re-configure the **ntp-standlaone vlan-range.** | Configuration | All platforms | AOS-W 8.0.1.0 |
| AOS-204948 | — | **Symptom:** APs crash and reboot unexpectedly. The log file lists the reason for the event as, **kernel panic: Fatal exception with NIP: e445c71c LR: e4490ac0 CTR: c0567b30.**<br>**Scenario:** This issue is observed in APs running AOS-W 8.5.0.7 or later versions.<br>**Workaround:** None. | AP-Wireless | All platforms | AOS-W 8.5.0.7 |

**Table 7:** *Known Issues in AOS-W 8.5.0.10*

| New Bug ID | Old Bug ID | Description | Component | Platform | Reported Version |
|---|---|---|---|---|---|
| AOS-205010 | — | **Symptom:** The **OFA** process in a managed device crashes unexpectedly.<br>**Scenario:** This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.<br>**Workaround:** None. | SDN-Platform | All platforms | AOS-W 8.5.0.8 |
| AOS-205112 | — | **Symptom:** The **auth** process in a managed device crashes unexpectedly.<br>**Scenario:** This issue occurs due to a memory leak in the **OFA** process. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.<br>**Workaround:** None. | SDN-Platform | All platforms | AOS-W 8.3.0.7 |
| AOS-205190 | — | **Symptom:** The **auth** process in a managed device crashes unexpectedly.<br>**Scenario:** This issue occurs when openflow is used to add or delete ACLs. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.<br>**Workaround:** None. | Base OS Security | All platforms | AOS-W 8.3.0.7 |
| AOS-205253<br>AOS-205644 | — | **Symptom:** Public key authentication fails on OpenSSH version 7.<br>**Scenario:** This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.<br>**Workaround:** None. | Base OS Security | All platforms | AOS-W 8.5.0.5 |

# Upgrade Procedure

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

CAUTION

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

Topics in this chapter include:

## Important Points to Remember and Best Practices

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** section of the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on the your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.

- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer *Alcatel-Lucent Mobility Master Licensing 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. Following are the best practices for memory requirement:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 60 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 60 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log file:** 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 60 to copy the **logs.tar** files to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

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

### Deleting a File

You can delete a file using the WebUI or the CLI.

#### In the WebUI

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

### In the CLI

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

# Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Logs
- Flashbackup

## Backing up and Restoring Flash Memory

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

### In the WebUI

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

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

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

### In the CLI

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

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

   ```
   (host) #write memory
   ```
2. Execute the following command to back up the contents of the flash memory to the **flashbackup.tar.gz** file.

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

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

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

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

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

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

4. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the 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 AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 59.

NOTE

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

### In the WebUI

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

1. Download the AOS-W image from the customer support site.
2. Upload the new software image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-W image:
   a. Download the **Alcatel.sha256** file from the download directory.

   b. Load the AOS-W image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the customer support site.

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

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

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

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

## In the CLI

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

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

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

   or

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

   or

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

4. Execute the **show image version** command to check if the AOS-W image is loaded on the flash 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 to the non-boot partition.

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

   or

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

   or

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

   or

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

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

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

7. Reboot the Mobility Master.

   ```
   (host)# reload
   ```

## Verifying the AOS-W Upgrade

Verify the upgrade using the WebUI or CLI.

### In the WebUI

Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.

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

1. Log in to the WebUI to verify if all the managed devices 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 as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Memory Requirements on page 59 for information on creating a backup.

### In the CLI

Execute the **show version** command to verify the AOS-W image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show 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 APs and clients are as expected.

4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 60 for information on creating a backup.

# Downgrading AOS-W

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

## Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 60.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved AOS-W configuration file.
4. Set the Mobility Master or managed device to boot from the system partition that contains the pre-upgrade AOS-W version.

   When you specify a boot partition or copy an image file to a system partition, Mobility Master or managed device checks if the AOS-W version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the AOS-W version and configuration files.
5. After switching the boot partition, perform the following steps:
   - Restore pre-upgrade flash backup from the file stored on the Mobility Master or managed device. Do not restore the AOS-W flash backup file.
   - Do not import the WMS database.
   - If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded AOS-W version.
   - If any new certificates were added in the upgraded AOS-W version, reinstall these certificates in the downgraded AOS-W version.

Downgrade AOS-W version using the WebUI or CLI.

### In the WebUI

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

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From the **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. From the **Select destination file** drop-down list, enter a file name (other than default.cfg).
   c. Click **Copy**.

2. Determine the partition on which your pre-upgrade AOS-W version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade AOS-W version is not stored on your system partition, load it into the backup system partition by performing the following steps:

CAUTION

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

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

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

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

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

## In the CLI

The following section describes how to downgrade the AOS-W version.

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 pre-upgrade AOS-W version 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 Mobility Master or managed device.

```
(host) # reload
```

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

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

## Before Calling Technical Support

Provide the following information when you call Technical Support:

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