

# AOS-W 8.6.0.3



## **Copyright Information**

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

<https://www.al-enterprise.com/en/legal/trademarks-copyright>

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2020)

## **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

---

<b>Contents</b> .....	<b>3</b>
Revision History .....	5
<b>Release Overview</b> .....	<b>6</b>
Supported Browsers .....	6
Contacting Support .....	7
<b>New Features and Enhancements</b> .....	<b>8</b>
<b>Supported Platforms</b> .....	<b>9</b>
Mobility Master Platforms .....	9
OmniAccess Mobility Controller Platforms .....	9
AP Platforms .....	10
<b>Regulatory Updates</b> .....	<b>12</b>
<b>Resolved Issues</b> .....	<b>13</b>
<b>Known Issues and Limitations</b> .....	<b>28</b>
<b>Upgrade Procedure</b> .....	<b>36</b>
Migrating from AOS-W 6.x to AOS-W 8.x .....	36
Important Points to Remember .....	36
Memory Requirements .....	37

---

Backing up Critical Data .....	38
Upgrading AOS-W .....	40
Downgrading AOS-W .....	42
Before Calling Technical Support .....	44

## 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:



---

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

---

- [New Features and Enhancements on page 8](#)
- [Supported Platforms on page 9](#)
- [Regulatory Updates on page 12](#)
- [Resolved Issues on page 13](#)
- [Known Issues and Limitations on page 28](#)
- [Upgrade Procedure on page 36](#)

For a list of terms, refer [Glossary](#).

## Supported Browsers

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

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

## Contacting Support

**Table 2:** *Contact Information*

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

### New Features and Enhancements in AOS-W 8.6.0.3

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

#### CLI

A new parameter, **network** is added to the **airgroupprofile** command. The **network default** is enabled whenever an **airgroupprofile** is configured in either distributed or centralized mode. This parameter allows the users to,

- Block or blacklist the client or server based on the MAC address or MAC OUI.
- Limit the number of maximum allowed IP addresses per server.
- Limit the number of maximum tokens allowed per server or client.

The following are the limitation of the **network default** parameter:

- User defined network profile is not supported.
- The default network profile is always enabled and cannot be disabled when any **airgroupprofile** is activated.
- The default network profile can be modified only from **/md** hierarchy node.
- In case of multiple islands, the network profile is activated only to the island where the **airgroupprofile** is activated.

```
(host) [md] (config) #airgroupprofile network default
(host) [md] (Network profile "default") #blacklist-mac <macaddr>
(host) [md] (Network profile "default") #max-ip-per-device <number of ip addresses>
(host) [md] (Network profile "default") #max-tokens-per-device <number of tokens>
```

#### IPv6

##### Network Advertisement

Starting from AOS-W 8.6.0.3, a stand-alone switch sends the network advertisement to the MAC address available in Source Link-Layer Address option.

#### LLDP

Starting from AOS-W 8.6.0.3, when an AP is in active-standby mode, LLDP packets transmitted from eth1 interface will use eth1's hardware address as Layer-2 source MAC address.

### Supported Platforms in AOS-W 8.6.0.3

This chapter describes the platforms supported in this release.

### Mobility Master Platforms

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

**Table 3:** Supported Mobility Master Platforms in AOS-W 8.6.0.3

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

### OmniAccess Mobility Controller Platforms

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

**Table 4:** Supported OmniAccess Mobility Controller Platforms in AOS-W 8.6.0.3

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

## AP Platforms

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

**Table 5:** Supported AP Platforms in AOS-W 8.6.0.3

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

**Table 5: Supported AP Platforms in AOS-W 8.6.0.3**

AP Family	AP Model
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP387	OAW-AP387
500 Series	OAW-AP504, OAW-AP505
510 Series	OAW-AP514, OAW-AP515
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

This chapter contains the Downloadable Regulatory Table (DRT) file version introduced in this release.

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

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

### Regulatory Updates in AOS-W 8.6.0.3

The following DRT file version is part of this release:

- DRT-1.0\_74492

### Resolved Issues in AOS-W 8.6.0.3

This chapter describes the issues resolved in this release.

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-137577 AOS-139523 AOS-145692 AOS-196723	167045 169550 177729	The <b>authentication</b> process in a Mobility Master crashed and the WebUI of the Mobility Master was inaccessible. This issue occurred when the <b>show global-usertable</b> command was executed. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-156424 AOS-156777 AOS-185158 AOS-193880 AOS-198034 AOS-198568	192581 193081	Invalid SSIDs were displayed in the <b>Dashboard &gt; WLAN</b> page in the WebUI. This issue occurred when a few APs were broadcasting invalid SSIDs. The fix ensures that the WebUI displays only the valid SSIDs. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	AOS-W 8.2.2.0
AOS-157882 AOS-200009	194655	The <b>Dashboard &gt; Overview &gt; Clients</b> page displayed incorrect roles for wired clients connected to a OAW-RAP. The fix ensures that the WebUI displays the correct role for wired clients. This issue was observed in stand-alone switches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-182579 AOS-195790 AOS-196493 AOS-197868 AOS-197989	—	APs and clients got disconnected frequently from the managed device. This issue occurred when heartbeats were randomly missed on the managed device. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.3.0.2 or later versions in a cluster setup.	AOS-W 8.3.0.2
AOS-185212 AOS-185375	—	The Authentication process crashed in a OAW-4750 standalone switch running ArubaOS 8.3.0.0 or later versions. The fix ensures that the switch works as expected. This issue was observed in OAW-4750 switches running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-188271 AOS-196680 AOS-197718	—	A few OAW-AP515 access points running AOS-W 8.5.0.0 or later versions crashed and rebooted unexpectedly. The fix ensures that the access points work as expected.	AOS-W 8.5.0.0

**Table 6: Resolved Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-188360	—	The <b>show configuration effective detail</b> command displayed incorrect device level configuration hierarchy. The fix ensures that the correct device level configuration hierarchy is displayed. This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.0
AOS-189118 AOS-200233	—	VIA clients running Alcatel-Lucent VIA version 3.2 and 3.4 were unable to establish connection with the switch through SSL fallback mode and the following error messages were displayed: <ul style="list-style-type: none"> <li>■ <b>Controller is not responding</b></li> <li>■ <b>UDP packets are dropped</b></li> <li>■ <b>SSL tunneling could not be turned on</b></li> </ul> This issue occurred when UDP port 4500 was blocked. The fix ensures that the clients can establish connection with the switch through SSL fallback mode. This issue was observed in Mobility Masters running AOS-W 8.3.0.1 or later versions.	AOS-W 8.3.0.1
AOS-189476 AOS-192948	—	The managed device displayed the error message <b>authmgr[8721]: &lt;522349&gt; &lt;8721&gt; &lt;DEBUG&gt; [authmgr] MAC 04:bd:88:c4:d7:6a IP 10.128.10.45: drop pkt non-DHCP pkt, Option-12 hostname needed for accounting</b> while configuring aaa profile user name with dhcp option 12 flag enabled and the user-table was also not updated. The fix ensures that the user table is updated and the managed device does not show the error message. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.1
AOS-190230 AOS-194760	—	A few OAW-RAPs failed to come up on the managed device after reboot of the APs, and got the same inner IP address which was already assigned to other OAW-RAPs. This issue occurred when most of the OAW-RAP whitelist database entries were deleted from the Mobility Master. The fix ensures that the OAW-RAPs work as expected. This issue was observed in APs running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-190380 AOS-196361	—	A few users were unable to connect to VIA server from the guest account. This issue occurred when PBR was not applied to data packets from UDP port 4500 . As a result, the client traffic was not forwarded correctly. The fix ensures that the users are able to connect to the VIA server. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-190927 AOS-192132	—	A few managed devices running AOS-W 8.4.0.4 or later versions became unresponsive without console access. This issue was observed due to <b>STM</b> process memory leak. The fix ensures that the managed devices work as expected.	AOS-W 8.4.0.4
AOS-191348	—	Client was unable to load the captive portal page. This issue occurred in a system with proxy settings. The fix ensures that the captive portal page loads without any issue. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191549	—	Users were unable to discover Apple TV. The issue occurred when AirGroup was enabled in Centralized mode. The fix ensures that users are able to discover Apple TV. This issue was observed in the Mobility Masters running AOS-W 8.4.0.3 or later versions.	AOS-W 8.4.0.3
AOS-192005	—	A managed device was in <b>CONFIG FAILURE</b> state and displayed the error message, <b>Module CERT DOWNLOAD MANAGER PORT is busy. Please try later.</b> This issue occurred while uploading server certificate for captive portal authentication. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-192163	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as <b>Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).</b> The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.4 or later versions.	AOS-W 8.3.0.4
AOS-192274	—	The command <b>show running-config</b> did not display LACP related information. The fix ensures that the <b>show running-config</b> command display LACP related information. This issue was observed in Mobility Masters running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-192814 AOS-199107	—	The Auto Associate feature of AirGroup did not work as expected and AP related information on AirGroup server was incorrect when clients roamed between different managed devices. The fix ensures that the feature works as expected. This issue occurred when GSM entries were not updated. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions in centralized or distributed mode.	AOS-W 8.3.0.7
AOS-193046 AOS-196703	—	Master IP configuration details were missing on the managed device and the managed device acted as a stand-alone switch. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later devices.	AOS-W 8.3.0.0
AOS-193320	—	Alcatel-Lucent SFP J8177D transceiver did not work with OAW-4450 switches. The fix ensures that the SFP J8177D transceiver works with OAW-4450 switches. This issue was observed in OAW-4450 switches running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-193362 AOS-198030	—	A Mobility Master was unable to establish connection with OmniVista 3600 Air Manager. This issue occurred when OmniVista 3600 Air Manager was not reachable from the management interface. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Master Hardware Appliance running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-193425	—	GSM entries were missing on the Mobility Master for some wireless users. The fix ensures that the GSM entries are available for the wireless users. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions in a cluster setup.	AOS-W 8.3.0.7

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193744 AOS-198906	—	The <b>mcell</b> process was in <b>PROCESS_NOT_RESPONDING</b> state after configuring master-redundancy on a standby Mobility Master. This issue occurred due to connectivity issue between active Mobility Master and the standby Mobility Master. The fix ensures that the process work as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-193888	—	A few APs rebooted unexpectedly. This issue occurred when the switch IP address was incorrect in a non-cluster datazone setup. The fix ensures that the APs work as expected. This issue was observed in access points running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-193976	—	APs rebooted unexpectedly. The log file listed the reason for the event as <b>Critical process /aruba/bin/sapd [pid XXXX] DIED, process marked as RESTART</b> . This issue occurred when the AP fails over to HA standby. The fix ensures that the APs work as expected. This issue was observed in access points running AOS-W 8.1.0.0 or later versions.	AOS-W 8.5.0.1
AOS-194052	—	A few clients were unable to obtain IP addresses. This issue occurred when <b>High Efficiency</b> was enabled on the WPA2-PSK SSID profile of the APs. The fix ensures that the clients are able to obtain the IP addresses. This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.2
AOS-194146	—	A managed device did not display any warning message when the cluster profile name contained more than 32 characters. The fix ensures that the managed device displays a warning message when the cluster profile name exceeds 32 characters. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions in a cluster setup.	AOS-W 8.5.0.2
AOS-194201	—	The value of Tx data bytes transmitted for 5 GHz radio was lesser than the actual transmitted value. The fix ensures that the actual values are transmitted for 5 GHz radio. This issue was observed in OAW-AP205 access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-194250	—	The <b>Configuration &gt; Interfaces &gt; VLANs</b> page did not display the list of VLANs. This issue occurred when a new VLAN ID was configured using the WebUI. The fix ensures that the WebUI displays the list of VLANs configured. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-194325 AOS-194579	—	The <b>datapath</b> process in a managed device crashed multiple times. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.3.0.7

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-194706	—	A managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)</b> . The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.2 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.2
AOS-194727	—	An AP sent RTS requests continuously to one client only and this resulted in a delay or packet drop to other clients. This issue was observed in OAW-AP340 Series access points running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-194785	—	AP was unable to failover to a backup LMS controller and the AP rebooted with the error, <b>Unable to set up IPsec tunnel after 24 tries</b> . The fix ensures that the APs work as expected. This issue was observed in OAW-AP375 access points connected to stand-alone controllers running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-194795 AOS-197097 AOS-201048	—	A managed device did not perform RADIUS authentication. The log file listed the reason for the event as <b>Failed to send the radius request for Station</b> . The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-194813 AOS-198001 AOS-199579 AOS-200149 AOS-200648 AOS-201658	—	The <b>mDNS</b> process crashed and rebooted on a Mobility Master Virtual Appliance unexpectedly. This issue occurred due to memory leak. The fix ensures that the Mobility Master Virtual Appliance works as expected. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-194874	—	High temperature was observed in CPU sensors. The fix ensures that the Mobility Master Hardware Appliance works as expected. This issue was observed in Mobility Master Hardware Appliances running AOS-W 8.3.0.4 or later versions.	AOS-W 8.3.0.4
AOS-194962	—	Some clients were unable to connect to the 2.4 GHz radio channel. This issue occurred when clients disabled the 2.4 GHz radio and enabled it again, causing the 802.11r SSID profile to get disabled between connections. The fix ensures that the clients can connect to the 2.4 GHz radio channel. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-195000	—	A few APs crashed unexpectedly. The log files listed the reason for the event as <b>Kernel panic: softlockup - hung tasks</b> . The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1

**Table 6: Resolved Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195036	—	The <b>authentication</b> process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.6
AOS-195146	—	Allowed vlan did not work when <b>wired-ap profile</b> is enabled with the ports set to trunk mode. This issue was observed in 530 Series and 550 Series access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-195162	—	The WebUI was unresponsive and the licenses were not visible in the <b>Mobility Master &gt; Configuration &gt; Licenses</b> page in the WebUI. This issue occurred when 29 non-default pools were configured and enabled. The fix ensures that the WebUI is responsive and the licenses are visible. This issue was observed in Mobility Masters running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-195163 AOS-197980	—	The <b>ofc_cli_agent</b> process in a Mobility Master crashed unexpectedly. This issue occurred due to mongo database buffer corruption. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-195265	—	A managed device crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b> . This issue occurred due to ACL corruption. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.3
AOS-195322 AOS-198279	—	The authentication module crashed on a managed device. This issue occurred due to memory leak. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-195414 AOS-198954	—	The <b>profmgr</b> process crashed on a switch. This issue occurred when interface access mode was configured on the Mobility Master. The fix ensures that the Mobility Master works as expected. This issue was observed in OAW-4008 switches running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-195444	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:60)</b> . This issue occurred due to high CPU utilization. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-195525	—	A few managed devices that were visible in the <b>Services &gt; Clusters</b> page in the WebUI were not visible when the upgrade cluster task is performed using <b>Configuration &gt; Tasks &gt; Upgrade Cluster</b> page. The fix ensures that the WebUI displays the managed devices in the <b>Configuration &gt; Tasks &gt; Upgrade Cluster</b> page. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195546 AOS-199490 AOS-199985	—	Memory leak was observed in <b>mDNS</b> process. This issue occurred when AirGroup was enabled in distributed mode. The fix ensures that the process works as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-195589 AOS-196087	—	<b>Profmgr</b> process crashed unexpectedly in a Mobility Master. This issue occurred when the VLAN commands entered exceeded 256 characters. The fix ensures that the Mobility Master process works as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.4 or later versions in a cluster-setup.	AOS-W 8.3.0.4
AOS-195968	—	OAW-RAPs could not connect to the managed device after a failover. This issue occurred when PSK authentication was used to provision a OAW-RAP. The fix ensures that the OAW-RAPs are able to connect to the managed device seamlessly. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-195600	—	Users were unable to discover Apple TV. The issue occurred because AirGroup mDNS packet sessions were flagged with 'o' flags during a Skype call initiation by UCC when AirGroup was enabled in Centralized mode. The fix ensures that users are able to discover Apple TV. This issue was observed in the Mobility Masters running AOS-W 8.3.0.8 or later versions. <b>Duplicates:</b> AOS-197877, AOS-199006, AOS-199741, AOS-199284, AOS-200095, AOS-200188, and AOS-200406	AOS-W 8.3.0.8
AOS-195677 AOS-196311	—	The <b>airmatch_recv</b> process crashed unexpectedly in a Mobility Master. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.3.0.7
AOS-195688	—	Some APs frequently detected wrong radars in a high density deployment. The issue was observed only on JP3 regulatory domain. Enhancements to the wireless driver resolved this issue. This issue was observed in OAW-AP325 access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-195749 AOS-195940 AOS-199401 AOS-200278	—	The <b>mDNS</b> module crashed on a Mobility Master. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-195789	—	An AP reported high channel usage on 5Ghz radio. This issue occurred due to a configuration error. The fix ensures that the access points work as expected. This issue was observed in OAW-AP377 access points running AOS-W 8.4.0.1 or later versions.	AOS-W 8.4.0.1

**Table 6: Resolved Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195835	—	The CLI command <b>firewall attack-rate arp</b> did not allow the users to configure attack rate with any value higher than 1024. The fix ensures that users can configure any value between 1-16384. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-195839	—	A VIA client could not auto-upgrade. This issue occurred when the VIA client was terminated to a Mobility Controller Virtual Appliance. The fix ensures that the auto-upgrade feature works as expected. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.0
AOS-195947	—	APs crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Kernel panic - not syncing: Take care of the TARGET ASSERT first</b> . This issue occurred due to kernel buffer. This issue was observed in tri-radio enabled OAW-AP555 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-196043	—	A mismatch of 802.11r configuration was observed between a Mobility Master and the managed devices, as well as between the WebUI and the CLI in a cluster. This issue occurred because 802.11r was not supported in split-tunnel forwarding mode. The fix ensures that 802.11r configuration is consistent across the Mobility Master and managed devices. This issue was observed in Mobility Masters and managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.4.0.4
AOS-196101 AOS-197335	—	Access points crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>external watchdog reset</b> . The fix ensures that the access points work as expected. This issue was observed in OAW-AP203H access points running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-196176 AOS-196945	—	The <b>Dashboard &gt; Security</b> page didn't load the <b>Detected Radios</b> and displayed the error message, <b>Error retrieving information. Please try again later</b> . The fix ensures that the WebUI displays the list of detected radios. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-196215 AOS-199712	—	Some clients were unable to manage multiple clusters using a single Mobility Master. This issue occurred when the Mobility Master assumed that the clusters are on the same VLAN and cannot reuse the same VRRP ID in the cluster profile. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196312 AOS-199450 AOS-199937 AOS-200235	—	Access points were unable to connect to a cluster. This issue occurred because the <b>ap_move</b> flag was not cleared after the <b>apmove</b> command was executed. The fix ensures that the <b>ap_move</b> flag is cleared after the <b>apmove</b> command is executed. This issue was observed in OAW-AP340 Series access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196325 AOS-200875	—	Mobility Master rebooted unexpectedly. This issue occurred due to high memory consumption. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196455 AOS-198499 AOS-200025	—	Mobility Master sent incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.4
AOS-196479	—	Managed devices dropped bcast or mcast traffic on VLANs randomly. This issue occurred because the clients were not getting IP addresses. The fix ensures that the bcast or mcast traffic is not dropped. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.3.0.6
AOS-196489 AOS-199172	—	GSM entries for AirGroup servers were not updated when MAC authenticated clients moved between APs. The fix ensures that the GSM entries are updated with new bssid of the APs. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-196499	—	An AP rebooted multiple times. The fix ensures that the access point works as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196528	—	Users were unable to remove port-channel using the <b>no port monitor port-channel</b> command and CLI displayed the error message, <b>illegal operation: port-channel not being monitored</b> . The fix ensures that the users are able to remove port-channel from port monitor. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.2
AOS-196560 AOS-197671 AOS-198844 AOS-199170 AOS-199375 AOS-200690	—	APs crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>Reboot caused by kernel panic, aruba_am_tx_elem_handler+0x404</b> . The fix ensures that the access points work as expected. This issue is observed in OAW-AP534, OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-196220 AOS-201396	—	An AP displayed the error message, <b>wlan: [0:E:BSSCOLOR] ol_ath_offload_bcn_tx_status_event_handler: beacon tx failed</b> . The fix ensures that the AP work as expected. This issue was observed in access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.2
AOS-196678	—	APs did not generate wireless containment frames and IDS protection was not applied. Hence, clients were not deauthenticated from non-valid APs. This issue occurred when the radio operated in AM mode. The fix ensures that the APs generate wireless containment frames and clients are deauthenticated from non-valid APs. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0

**Table 6: Resolved Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196683	—	Access points came up without standby APs. This issue occurred in a cluster when AP channel scanning detects an invalid AP and skips scanning the remaining APs. The fix ensures that the APs work as expected. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196699 AOS-196870	—	Access points crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>rebooted due to warm-reset [ BadAddr:480d5c0001e890 PC:wlc_mutx_bw_policy_update+0x1afc/0x28b8 [wl_v6] Warm-reset]</b> . The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-196728	—	A Mobility Master Virtual Appliance crashed unexpectedly. The fix ensures that the Mobility Master Virtual Appliance works as expected. This issue was observed in Mobility Master Virtual Appliances AOS-W 8.3.0.0 or later versions in a cluster setup.	AOS-W 8.3.0.8
AOS-196788	—	The <b>OFA</b> process crashed unexpectedly. This issue occurred due to frequent reboot of APs. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-196805	—	The command <b>show ap debug client-stats</b> displayed lower rates for management frames. The fix ensures that the <b>show ap client-stats</b> command displays the correct rates for management frames. This issue was observed in access points running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-196847 AOS-196941 AOS-198485 AOS-201783	—	The <b>Dashboard &gt; Infrastructure &gt; Controller</b> page did not display the list of available switches. The fix ensures that the WebUI displays the list of switches. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196852	—	APs running AOS-W 8.4.0.4 or later versions crashed and rebooted unexpectedly. The fix ensures that the access points work as expected.	AOS-W 8.4.0.4
AOS-196879	—	APs crashed unexpectedly. The log file listed the reason for the event as <b>PC is at aruba_am_tx_pkt_handler_data_ol</b> . This issue occurred after upgrading the APs to AOS-W 8.3.0.10. The fix ensures that the APs work as expected. This issue was observed in OAW-AP315 access points running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-196881	—	Server configuration rules were not pushed to the managed devices. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7

**Table 6: Resolved Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196887 AOS-196959	—	WPA3-SAE-AES Opmode enabled clients were unable to connect to the AP and the AP sent <b>Deauthentication Reason Code: 49 Invalid pairwise masterkey identifier (PMKI) [24-25]</b> deauthentication code. The fix ensures that the AP works as expected. This issue was observed in APs running AOS-W 8.5.0.5 or later versions in a cluster setup.	AOS-W 8.5.0.5
AOS-196896 AOS-197050 AOS-200076 AOS-200077	—	APs crashed and rebooted unexpectedly. This issue occurred during the <b>stm</b> process crash when more than 256 clients connected to a OAW-RAP or OAW-AP on bridge mode got deleted. The fix ensures that the APs work as expected. This issue was observed in OAW-AP325 access points running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196911 AOS-198963	—	Users were unable to connect to APs. Enhancement to the wireless driver fixed the issue. This issue was observed in OAW-AP555 access points running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-196928 AOS-196066 AOS-196943 AOS-197742 AOS-198048 AOS-198328 AOS-198682 AOS-199156	—	Users were unable to discover the wired AirGroup server and experienced packet drops when a UCC Skype call was initiated. This issue occurred when AirGroup was enabled in centralized mode. The fix ensures that the users are able to discover the wired AirGroup servers. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197122	—	Managed devices did not send SNMPv3 information to OmniVista 3600 Air Manager. The fix ensures that the managed devices send the SNMPv3 information to OmniVista 3600 Air Manager. This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-197160 AOS-198571 AOS-200427 AOS-201607	—	Managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b> . This issue occurred due to corrupt ACL entries. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.3.0.8 in a cluster-setup.	AOS-W 8.3.0.8
AOS-197262	—	The command <b>show crashinfo</b> did not display the crash information even when the crash symbol was displayed. The fix ensures that the <b>show crashinfo</b> command displays the correct crash information. This issue was observed in managed devices running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-197310	—	WebUI did not list the available cluster profiles in the <b>Configuration &gt; Services &gt; Cluster &gt; Cluster group-membership</b> drop-down list. The fix ensures that the WebUI lists the available cluster profiles. This issue was observed in managed devices running AOS-W 8.3.0.5 or later versions in a cluster setup.	AOS-W 8.3.0.5

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197393 AOS-200407	—	Radios experienced high number of resets and packet drops were also observed on APs. The fix ensures that the APs work as expected. This issue was observed in OAW-AP340 Series access points running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-197536 AOS-198286 AOS-200371	—	Many clients got disconnected from APs. This issue occurred when a new VLAN was added. The fix ensures seamless connectivity. This issue was observed in access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.0
AOS-197939 AOS-198087	—	After configuring the heartbeat threshold in the WebUI, the VRRP IDs got reset to the default values. The fix ensures that the VRRP IDs are not reset to the default values. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197977 AOS-198348 AOS-198349	—	High memory consumption was observed in <b>dot1x1</b> and <b>dot1x2</b> processes. This issue occurred due to memory leak when the EAP-fragmentation feature was enabled. The fix ensures dot1x1 and dot1x2 process do not consume high memory. This issue was observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.1
AOS-197993 AOS-198889	—	A managed device crashed unexpectedly and high CPU utilization was also observed on the managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-198003	—	Network firewall dropped fragmented packets and hence clients faced connectivity issues. The fix ensures seamless connectivity. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-198110	—	The <b>configuration device move to</b> command displayed the error message, <b>trusted Illegal Operation: There is Session ACL Defined. Cannot make the port untrusted</b> . This issue occurred when the <b>trusted</b> command was executed before and after configuring the session ACL. The fix ensures that the error message is not displayed. This issue was observed in Mobility Masters running AOS-W 8.3.0.9 or later versions.	AOS-W 8.3.0.9
AOS-198112	—	WebUI displayed an error message <b>Invalid IPv4</b> when users tried to configure OmniVista 3600 Air Manager IPv6 address under <b>Configuration &gt; System &gt; AirWave</b> in the Mobility Master node hierarchy. The fix ensures that the OmniVista 3600 Air Manager IPv6 address can be configured using the WebUI. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198232	—	A managed device was unable to forward RADIUS server statistics through SNMP walk. This issue was resolved by combining the RADIUS server statistics of <b>802.1X</b> and <b>authentication</b> processes. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.5

**Table 6: Resolved Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198290 AOS-198836	—	The <b>show ip interface brief</b> command displayed incorrect radio channel information for AAC and non S-AAC managed devices. The fix ensures that the <b>show ip interface brief</b> command displays the correct radio channel information. This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-198360	—	The word <b>switches</b> was misspelled in the <b>show airgroup</b> command output. The fix ensures that the word <b>switches</b> is spelled correctly. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198370	—	The <b>Managed network &gt; Configuration &gt; Task &gt; Bulk configuration upload</b> page displayed an error message, <b>Incorrect header field(Controller VLAN)</b> while uploading the bulk edit configuration. The fix ensures that the WebUI does not display the error message. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198527 AOS-198824	—	The output of <b>show switches</b> command displayed the configuration state of the managed device as <b>NO MM License</b> . This issue occurred due to license synchronization failure. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198669 AOS-198885	—	All rules configured using <b>aaa server-group</b> command were displayed in lowercase. The fix ensures that the rules are displayed in the correct letter cases. This issue was observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198670	—	Forward slash ( <b>/</b> ) did not search for the next hit in CLI output. The fix ensures that the forward slash leads to the next hit in CLI output. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.8
AOS-198699	—	ZTP feature did not work on Huawei 4G dongle with model number E3372h-607. The fix ensures that ZTP works on the modem. This issue was observed in OAW-4005 switches running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-198738	—	Users were unable to access CLI using SSH. This issue occurred in an IPv6 network when the multicast packets were not sent to the Mobility Master Virtual Appliance. The fix ensures that the users can access CLI using SSH. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1

**Table 6:** Resolved Issues in AOS-W 8.6.0.3

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198741	—	Users were unable to configure IPsec tunnels on a few of third party VPN peers and the switch sent the error message, <b>INVALID SYNTAX</b> . This issue occurred when the third-party VPN peers propose IKEV2_FRAGMENTATION_SUPPORTED notify payload but did not send the IKE_AUTH payload as fragments. The fix ensures that the users are able to configure IPsec tunnels. This issue was observed in stand-alone switches running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-198743	—	A few IPv6 enabled OAW-RAPs rebooted unexpectedly. This issue occurred when the Mobility Master was configured with VRRP IP. The fix ensures that the APs work as expected. This issue was observed in OAW-RAPs running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198817	—	APs failed to perform 802.1x authentication. This issue occurred when dot1x authenticated access points were upgraded to ArubaOS 8.6.0.1. The fix ensures that the APs work as expected. This issue was observed in OAW-AP105 access points running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.1
AOS-198828	—	APs did not send temperature values to the server. This issue occurred when the APs did not properly relay RTLS Aeroscout tag to the server. The fix ensures that the access points work as expected. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-199217 AOS-199709	—	Cluster heartbeats were randomly missed on managed devices. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions in a cluster setup.	AOS-W 8.3.0.10
AOS-199237	—	Users were unable to establish connection with a managed device using the <b>mdconnect</b> and <b>logon</b> commands. This issue occurred when master-ssh-pub-cert was not downloaded during the initial boot-up after ZTP. The fix ensures that the commands work as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-199238	—	A managed device displayed the error log, <b>ctamon_gsm_update_section_intf_stats: Failed to Update GSM section intf_stats for , intf_num:0x40e3d6e0, error 43, error_htbl_key_not_found</b> . The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-199667 AOS-199736	—	The system was unresponsive when the <b>show tech-support</b> command was executed. This issue occurred when the <b>show datapath dhcp binding</b> command duplicated the output entries. The fix ensures that the command works as expected. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

**Table 6: Resolved Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199696	—	Managed devices failed to establish connection with <b>IF-MAP</b> enabled ClearPass Policy Manager. This issue occurred when same certificates were added using different names. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-199707	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20)</b> . The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-199739 AOS-201390	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b> . This issue occurred after upgrading the managed device to AOS-W 8.6.0.2 version. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-200002 AOS-200649	—	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>crashed and rebooted due to Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)</b> . This issue occurred due to high CPU utilization. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200102 AOS-200779	—	Clients took a long time to failover to another managed device in a cluster. The fix ensures that the clients failover seamlessly. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a cluster setup.	AOS-W 8.5.0.5
AOS-200146	—	The <b>STM</b> process on an AP crashed. The fix ensures that the access point works as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.4.0.0 or later versions.	AOS-W 8.6.0.0
AOS-200165	—	OAW-AP515 access points running AOS-W 8.5.0.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>rebooted caused by BadPtr:00000010 PC:aruba_periodic_measurements+0x1b10/0x2748 [wl_v6] Warm-reset</b> . The fix ensures that the APs work as expected.	AOS-W 8.5.0.6
AOS-200420	—	Data traffic from VPNC concentrator was not routed back to the managed device. The fix ensures that the managed device works as expected. This issue occurred when the managed device was provisioned with two uplinks. This issue was observed in branch office switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5

### Known Issues and Limitations in AOS-W 8.6.0.3

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

#### Known Issues

Following are the known issues observed in this release.

**Table 7:** *Known Issues in AOS-W 8.6.0.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the <b>show datapath uplink</b> command displays incorrect session count. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-151355	185602	A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
AOS-152326 AOS-187297 AOS-187406 AOS-187549	186957	The beacon displays the country code information intermittently for 5 GHz non-DFS channel. This issue occurs when 802.11h is enabled in the radio profile. This issue is observed in 510 Series access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.4.0.0
AOS-153742 AOS-194948	188871	A stand-alone switch crashes and reboots unexpectedly. The log files list the reason for the event as <b>Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)</b> . 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.	AOS-W 8.5.0.1
AOS-155037	190571	A OAW-RAP fails to boot up. This issue occurs in a OAW-RAP with EST key type <b>X9.62/SECG curve</b> . This issue is observed in OAW-AP303H access points running AOS-W 8.3.0.3 or later versions.	AOS-W 8.3.0.3
AOS-156085 AOS-157704	192119 194393	A few managed devices are unable to obtain the switch-IP address during boot up after an upgrade. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.	AOS-W 8.1.0.0
AOS-182073 AOS-183743	—	An AP crashes and reboots unexpectedly. The log files lists the reason for the event as <b>Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT</b> . This issue is observed in OAW-AP315 access points running AOS-W 8.3.0.5 or later versions.	AOS-W 8.3.0.5

**Table 7: Known Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-182847	—	A few users are unable to copy the <b>WPA Passphrase</b> field and <b>High-throughput</b> profile to a new SSID profile in the <b>Configuration &gt; System &gt; Profiles &gt; Wireless LAN &gt; SSID &gt; &lt;SSID_Profile&gt;</b> option of the WebUI. 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.	AOS-W 8.4.0.0
AOS-184947 AOS-192737	—	The jitter and health score data are missing from the <b>Dashboard &gt; Infrastructure &gt; Uplink &gt; Health</b> page in the WebUI. This issue is observed in Mobility Master running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-184977 AOS-188242 AOS-188378 AOS-197491	—	The output of basic commands such as <b>show version</b> , <b>show clock</b> , and <b>show image version</b> are unable to display any information and the default gateway details are missing in a managed device. This issue occurs when the <b>/tmp</b> directory runs out of memory because of too many logs from the Policy Manager. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-188090 AOS-196004 AOS-199152	—	The <b>Dashboard &gt; Overview &gt; Clients</b> page of the WebUI displays incorrect usage values intermittently. This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-188527 AOS-193897	—	The IP address of the NAT configured managed device is visible in the HTTP header of the web server. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-188898 AOS-198730 AOS-200227	—	The <b>postgres</b> module crashes on a switch. This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.2.6
AOS-190071 AOS-190372	—	A few users are unable to access the websites when WebCC is enabled on the user role. 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. <b>Workaround:</b> <ul style="list-style-type: none"> <li>■ Remove web category from the ACL rules and apply <b>any any any permit</b> policy.</li> <li>■ Disable WebCC on the user role.</li> <li>■ Change the VLAN of user role from trunk mode to access mode.</li> </ul>	AOS-W 8.4.0.0
AOS-191216 AOS-196523 AOS-199160	—	A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as <b>Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2)</b> . This issue is observed in managed devices running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-191394	—	APs crash and reboot unexpectedly. The log file lists the reason for the event as <b>Reboot caused by kernel panic: Take care of the TARGET ASSERT first</b> . This issue is observed in 500 Series access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0

**Table 7: Known Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191612	—	The MAC address of users connected using VIA is not sent to ClearPass Policy Manager for authentication. This issue is observed when IKE V2 with EAP-FTC is used for VIA authentication. This issue is observed in Mobility Masters running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-192568 AOS-192736	—	A few clients are unable to connect to APs even though High-Efficiency was disabled on all the SSID profiles of the APs. This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.1
AOS-192725 AOS-190476 AOS-196004	—	The <b>Dashboard &gt; Overview</b> page of the WebUI displays incorrect number of users intermittently. This issue is observed in Mobility Masters running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-192738 AOS-197047	—	The Mobility Master list in the WebUI incorrectly displays the mac address of the primary Mobility Master for the secondary Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-193184	—	L2 connected managed devices move to L3 connected state after upgrade. This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-193775 AOS-194581 AOS-197372	—	A mismatch of AP count and client count is observed between the Mobility Master and the managed device. This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.2
AOS-193840	—	The managed device loses connectivity to IPv6 gateway intermittently. This issue is observed in managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-193883 AOS-197756	—	A few APs are unable to use DHCP IPv6 addresses and option 52 for master discovery. 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. <b>Workaround:</b> Delete the IPv4 addresses from ap system profile using the command, <b>ap system-profile</b> and from high availability profiles using the command, <b>ha</b> .	AOS-W 8.3.0.8
AOS-194370	—	High memory utilization is observed in the <b>cluster manager</b> process of managed devices. This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions in a cluster setup.	AOS-W 8.4.0.2
AOS-194846	—	The commands <b>show ap arm history</b> and <b>show airmatch debug optimization</b> do not display the output. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-194911	—	Incorrect flag output is displayed for APs configured with 802.1X authentication when the <b>show ap database</b> command is executed. This issue is observed in APs running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2

**Table 7: Known Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-194964	—	A few users are unable to clone the configuration from an existing group to a new group in a Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.4.0.1 or later versions. <b>Workaround:</b> Execute the <b>rf dot11a-radio-profile &lt;profile name&gt;</b> command to change the operating mode of the AP from am-mode to ap-mode.	AOS-W 8.5.0.2
AOS-195177	—	Managed devices frequently generate internal system error logs. This issue occurs when the <b>sapd</b> process reads a non-existent interface. This issue is observed in OAW-4650 switches running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-195228	—	The device status is always displayed as inactive when SNMP walk is performed. This issue is observed in stand-alone switches running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-195434	—	An AP crashes and reboots unexpectedly. The log files list the reason for the event as <b>Reboot caused by kernel panic: Fatal exception</b> . This issue is observed in APs running AOS-W 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.2
AOS-195526	—	Some clients are unable to get the DHCP address. This issue occurs because the ACE entries of the logon role ACL changes to <b>Deny all</b> when the PEFNG feature is disabled. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-195939	—	UBT users are assigned <b>logon</b> role when they receive the same IP addresses. This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196115	—	Users are unable to configure untrusted VLAN in the <b>Configuration &gt; Interfaces &gt; Ports</b> page of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-196457	—	High radio noise floor is observed on APs. This issue is observed on OAW-AP515 access points running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196560 AOS-197671	—	APs crash and reboot unexpectedly. The log files list the reason for the event as <b>Reboot caused by kernel panic: Fatal exception in interrupt</b> . This issue is observed in 500 Series access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-196593	—	APs crash and reboot unexpectedly. The log file lists the reason for the event as <b>reboot caused by Kernel panic - not syncing: Fatal exception in interrupt PC is at 0x000C7461</b> . This issue is observed in OAW-AP335 access points running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8

**Table 7: Known Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196697 AOS-199833	—	APs crash and reboot unexpectedly. The log file lists the reason for the event as <b>PC is at wlc_apps_psq+0xc/0x6ec [wl_v6];LR is at wlc_apps_release_count+0xb4/0x164 [wl_v6]</b> . This issue is observed in OAW-AP505 access points running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-196864	—	Adding a new VLAN ID connects L3 but displays that the connected VLAN ID fails with a different ID. 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.	AOS-W 8.5.0.3
AOS-196878 AOS-197216	—	The <b>Datapath</b> process crashes on a managed device. The log file lists the reason for the event as <b>wlan-n09-nc1.gw.illinois.edu</b> . This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-197023	—	Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. <b>Workaround:</b> The following are recommended: In the CLI, create an AP regulatory-domain- profile without any channel configuration, save the changes and later add or delete channels as desired. In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes and later add or delete channels as desired.	AOS-W 8.5.0.4
AOS-197215	—	Users are unable to delete the <b>Weekend</b> entry under <b>Start Day of Time range</b> field in the WebUI. This issue occurs when the users create a new policy rule in the <b>Configuration &gt; Roles &amp; Policies &gt; Policies &gt; &lt;policy_name&gt; &gt; &lt;new_policy_rule&gt;</b> page, and select <b>Access control</b> radio button in the <b>Rule type</b> field of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-197565	—	APs crash and reboot unexpectedly. The log file lists the reason for the event as <b>Dump capture kernel:AP rebooted caused by cold HW reset(power loss)</b> . This issue is observed in access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.2
AOS-197631	—	Policy-based routing is not applied when IPsec map is configured as nexthop. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-197912	—	Multicast traffic is not forwarded to the clients when UAC and AAC are different. This issue occurs when the VLANs assigned by radius server are different from the VLANs configured in the virtual-ap profile. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-197945	—	Access points crash and reboot unexpectedly. The log file lists the reason for the events as, <b>BadAddr:ffff00000010 PC:wlc_dump_aggfifo+0x1160/0x12b0 [wl_v6] Warm-reset</b> . This issue occurs due to memory corruption. This issue is observed in OAW-AP514 and OAW-AP515 access points running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3

**Table 7: Known Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198007	—	APs are unable to ping managed devices and the APs keep switching between clusters. This issue is observed in access points running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-198024	—	Users are unable to access any page after the fifth page using the <b>Maintenance &gt; Access Point</b> page in the WebUI. This issue is observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198157	—	A stand-alone switch crashes and reboots unexpectedly. The log file lists the reason for the event as <b>Reboot Cause: Datapath timeout (Intent:cause: 86:56)</b> . This issue is observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198218	—	After reboot, the GRE tunnel of a standby switch is UP instead of DOWN in a VRRP instance and this results in network loop. This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198266	—	MAC authenticated clients are unable to reauthenticate even after enabling reauthentication. This issue is observed in stand-alone switches running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198475	—	Users are unable to upgrade the Mobility Master Virtual Appliance to AOS-W 8.5.0.0 or later versions. This issue is observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-198483	—	WebUI does not have an option to map the <b>rf dot11-60GHz-radio-profile</b> to an AP group. This issue is observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-198834 AOS-200088 AOS-200555 AOS-201312	—	Managed devices crash and reboot unexpectedly. The log file lists the reason for the event as <b>rebooted due to Soft Watchdog reset (Intent:cause:register de:86:70:4)</b> . This issue is observed in OAW-4750XM switches running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-198849 AOS-198850	—	Users are unable to configure 2.4 GHz radio profile in the <b>Configuration &gt; System &gt; Profiles &gt; 2.4 GHz radio profile</b> page and the WebUI displays the error message, <b>Feature is not enabled in the license</b> . This issue is observed in stand-alone switches running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198787 AOS-198929	—	A OAW-RAP does not come up on a managed device when Verizon U730L modem is used. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198991	—	Users are unable to add VLAN to an existing trunk port using the <b>Configuration &gt; Interfaces &gt; VLANs</b> page of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.2

**Table 7: Known Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199012 AOS-198865	—	A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)</b> . This issue is observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-199381	—	Users are unable to connect to the backup SSID of a OAW-RAP. This issue occurs when the users try to connect after AP reboot. This issue is observed in OAW-RAPs running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.2
AOS-199420	—	ClientMatch steered clients to APs that are deployed in different clusters. This issue is observed in access points running AOS-W 8.2.2.2 or later versions.	AOS-W 8.2.2.2
AOS-199423	—	Some L3 redundant Mobility Masters witness <b>profmgr</b> error logs. This issue occurs when the Mobility Master is upgraded to a later version of AOS-W. This issue is observed in Mobility Masters running AOS-W 8.5.0.5-FIPS.	AOS-W 8.5.0.5
AOS-199492	—	A few APs do not get displayed in the <b>show airgroup aps</b> command output and the <b>auto-associate policy</b> stops working as expected. This issue occurs when the AirGroup domain is in distributed mode and is not validated in a cluster deployment. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-199539	—	All the profiles listed under an AP group get marked as default except the VAP profile. This issue is observed in managed devices running AOS-W 8.5.0.4 or later versions. <b>Workaround:</b> Run <b>ccm-debug full-config-sync</b> command on the effected managed device.	AOS-W 8.5.0.4
AOS-199878 AOS-198897 AOS-200006 AOS-200080	—	An AP crashes and reboots unexpectedly. The log file lists the reason for this event as <b>Reboot caused by kernel panic: CPU stall</b> . This issue is observed in OAW-AP303H access points running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-200071 AOS-201068	—	Some clients are getting <b>U-APSD disabled in association</b> response though they are able to connect to an SSID without any issues. This issue does not allow the client to enter power saving mode and reduces the talk time from 12 hours to 3 hours. This issue is observed in access points running AOS-W 8.3.0.0 or later versions. <b>Workaround:</b> Disable the 802.11r profile in the configurations using the <b>no dot11r</b> command.	AOS-W 8.6.0.2
AOS-200187	—	Mobility Master is assigning duplicate IP addresses to Branch office switches from the VLAN pool. This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5

**Table 7: Known Issues in AOS-W 8.6.0.3**

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201171	—	Clients are unable to receive traffic from APs. This issue occurs when large number of clients are associated to APs and when aggressive power saving transitions are observed on the associated clients. This issue is observed in access points AOS-W 8.6.0.3.	AOS-W 8.6.0.3
AOS-201463	—	An AP is unable to receive IPv6 address from IPv6 RA. This issue occurs when static IPv4 addresses are configured on LACP enabled APs. This issue is observed in access points running AOS-W 8.6.0.3. <b>Workaround:</b> Do not configure static IPv4 addresses for LACP enabled APs.	AOS-W 8.6.0.3
AOS-201681	—	Data traffic to clients on radio 2 fails. This issue occurs due to cluster failover. This issue is observed in tri-radio enabled OAW-AP555 access points running AOS-W 8.6.0.3. <b>Workaround:</b> The following are recommended: <ul style="list-style-type: none"><li>■ Disable the tri-radio mode.</li><li>■ Associate the clients to Radio 0.</li></ul>	AOS-W 8.6.0.3

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



CAUTION

---

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

---

Topics in this chapter include:

- [Migrating from AOS-W 6.x to AOS-W 8.x on page 36](#)
- [Important Points to Remember on page 36](#)
- [Memory Requirements on page 37](#)
- [Backing up Critical Data on page 38](#)
- [Upgrading AOS-W on page 40](#)
- [Downgrading AOS-W on page 42](#)
- [Before Calling Technical Support on page 44](#)

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

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

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

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



NOTE

---

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

---

## Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Master Licensing Guide*.
- Multiversion is supported only if the Mobility Master is running two code versions higher than the code versions running on the managed devices. For example multiversion is supported if a Mobility Master is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.3.0.0 and will not be supported if the managed devices are running AOS-W 8.2.0.0 or AOS-W 8.4.0.0.

## Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. Following are best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the managed device to a desired location. Delete the following files from the managed device to free some memory:

- **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 38](#) 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 38](#) to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 38](#) to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.



---

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

---

## Deleting a File

You can delete a file using the WebUI or CLI.

### In the WebUI

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

### In the CLI

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

## Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Log files
- Flash backup

## Backing up and Restoring Flash Memory

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

### In the WebUI

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

1. In the Mobility Master node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the flash memory to the **flashbackup.tar.gz** file.
3. Click **Copy Backup** to copy the file to an external server.  
You can copy the backup file from the external server to the flash memory using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the flash memory, navigate to the **Maintenance > Configuration Management > Restore** page and click **Restore**.

### In the CLI

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

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

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

```
(host) #backup flash
Please wait while we take the flash backup.....
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```
3. Execute either of the following command to transfer the flash backup file to an external server or storage device.  

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

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

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

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

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

4. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the flash memory.  

```
(host) #restore flash
Please wait while we restore the flash backup.....
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

## Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.



CAUTION

---

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see [Memory Requirements on page 37](#).

---



When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message is displayed 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 AOS-W image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-W image:
  - a. Download the **Alcatel.sha256** file from the download directory.
  - b. Load the AOS-W image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
  - c. Verify that the output produced by this command matches the hash value found on the customer support site.



---

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

---

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



---

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

---

9. Select **Save Current Configuration**.

10. Click **Upgrade**.
11. Click **OK**, when the **Changes were written to flash successfully** message is displayed.

## In the CLI

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

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

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

or

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

or

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

4. Execute the **show image version** command to check if the AOS-W image is loaded on the flash partition. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

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

5. Execute the **copy** command to load the new image to the non-boot partition.

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Master.

```
(host)#reload
```

8. Execute the **show version** command to verify that the upgrade is complete.

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

## Verifying the AOS-W Upgrade

Verify the AOS-W upgrade in the WebUI or CLI.

## In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See [Backing up Critical Data on page 38](#) for information on creating a backup.

## In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the AOS-W image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See [Backing up Critical Data on page 38](#) for information on creating a backup.

## Downgrading AOS-W

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

### Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see [Backing up Critical Data on page 38](#).
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

## In the WebUI

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

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



---

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

---

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

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

## In the CLI

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

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

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

or

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

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

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

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

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



---

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

---

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

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

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

## Before Calling Technical Support

Provide the following information when you call the Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with IP addresses and interface numbers.
- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.

- The date and time when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information.