AOS-W 8.6.0.5

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 02	**AOS-203232** has been removed from the **Resolved Issues** section and added to the **Known Issues and Limitations** section.
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

NOTE

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

- 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 26
- Upgrade Procedure on page 38

For a list of terms, refer Glossary.

Important Point Before Upgrading to AOS-W 8.6.0.0

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.

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

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

New Features and Enhancements in AOS-W 8.6.0.5

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.

Supported Platforms in AOS-W 8.6.0.5

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 8.6.0.5*

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 8.6.0.5*

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-10, MC-VA-50, MC-VA-250, MC-VA-1K, MC-VA 4K, MC-VA 6K

NOTE

MC-VA-4K and MC-VA-6K are not orderable SKUs. However, you can scale up by installing multiple instances of MC-VA-1K. For example to deploy 4K APs on a single Mobility Controller Virtual Appliance, you need to add four MC-VA-1K licenses.

AP Platforms

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

Table 5: *Supported AP Platforms in AOS-W 8.6.0.5*

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

Table 5: *Supported AP Platforms in AOS-W 8.6.0.5*

AP Family	AP Model
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303
OAW-AP303H Series	OAW-AP303H
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP387	OAW-AP387
500 Series	OAW-AP504, OAW-AP505
510 Series	OAW-AP514, OAW-AP515
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

Chapter 4
Regulatory Updates

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

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

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

Regulatory Updates in AOS-W 8.6.0.5

The following DRT file version is part of this release:

- DRT-1.0_75772

Resolved Issues in AOS-W 8.6.0.5

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-125305	151011	Clients were unable to connect to APs. This issue occurred when the **STM** process failed to discover VLANs. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions. **Duplicates:** **New Bug IDs:** AOS-122776, AOS-124619, AOS-139533, AOS-145308, and AOS-188376 **Old Bug IDs:** 147957, 150132, 169561, and 177209	AOS-W 8.3.0.0
AOS-148643 AOS-150529	182036 184499	Clients were unable to connect to the 802.1X SSID when UAC and AAC were different. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-183179	—	Video multicast frames were transmitted at the rate of 24 Mbps even when the configuration is set at 54 Mbps. The fix ensures that the video multicast frames are transmitted at the configured value. This issue was observed in OAW-AP555 access points running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-183317 AOS-198642	—	530 Series access points running AOS-W 8.5.0.0 or later versions detected multiple false radars on channel 100, with type ID 255. The fix ensures that the APs do not detect false radars.	AOS-W 8.5.0.0
AOS-187025 AOS-201544	—	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. This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-188271 AOS-196680 AOS-201542 AOS-201956 AOS-202569 AOS-202570	—	OAW-AP515 access points running AOS-W 8.5.0.0 or later versions 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.	AOS-W 8.5.0.0
AOS-188793	—	The output of the **show audit-trail** command displayed incorrect message for the **BOCMGR** process in a Mobility Master. This issue occurred when the Mobility Master was connected to the Activate server. The fix ensures that the command does not display the incorrect message. This issue was observed in Mobility Masters running AOS-W 8.2.2.3 or later versions.	AOS-W 8.2.2.3
AOS-188898 AOS-198730 AOS-200227	—	The **postgres** module crashed on managed devices running AOS-W 8.2.1.0 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.2.2.6
AOS-191216 AOS-196523 AOS-199160 AOS-203960	—	A managed device running AOS-W 8.5.0.4 or later versions crashed and rebooted unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2).** The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.4
AOS-191394 AOS-203029	—	500 Series access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by FW Crash: ar_wal_tx_de.c:68 Assertion 0 failed** The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-191612	—	The MAC addresses of users connected using VIA were not sent to ClearPass Policy Manager for authentication. This issue occurred when IKE V2 with EAP-FTC was used for VIA authentication. The fix ensures that the MAC addresses are sent to ClearPass Policy Manager for authentication. This issue was observed in Mobility Masters running AOS-W 8.5.0.1 or later versions.	AOS-W 8.5.0.1
AOS-192662	—	The CLI command **show ap monitor** displayed lesser number of AP neighbors. The fix ensures that the command displays the correct number of AP neighbors. This issue was observed in OAW-AP555 access points running AOS-W 8.6.0.0.	AOS-W 8.6.0.0
AOS-193033 AOS-198921 AOS-198953	—	A few clients were not redirected to the captive portal page. This issue occurred because the **Nginx** process failed due to a race condition. The fix ensures that captive portal works as expected. This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193383 AOS-203470	—	500 Series access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as r**ebooted with PC is at __qdf_bug+0x0/0x8 [qdf].** The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-194518	—	APs kept retrying a frame although they received Block Acknowledgment (BA) packets from clients. The fix ensures that the APs work as expected. This issue was observed in 500 Series access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-194846	—	The commands **show ap arm history** and **show airmatch debug optimization** did not display any output. This issue occurred when AirMatch optimization did not work on the Mobility Master. The fix ensures that the Airmatch optimization works on the Mobility Master as expected. This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-194930	—	The **Auth Sub-type** column under **Managed Network > Dashboard > Overview > Clients** table displayed **None** though the authentication sub-type was **EAP-PEAP.** This issue occurred in 802.1X authenticated users after a failed station reauthentication attempt. The fix ensures that the WebUI displays the authentication sub-type. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-195228	—	The device status was always displayed as inactive when an SNMP walk was performed. The fix ensures that the device status is displayed correctly. This issue was observed in stand-alone switches running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-195646	—	The **Authentication** process crashed on a managed device running AOS-W 8.4.0.4 or later versions in a cluster setup. The fix ensures that the managed device works as expected. This issue occurred because of incorrect parsing of PAPI messages.	AOS-W 8.4.0.4
AOS-196188 AOS-203466	—	OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt.** Enhancements to the wireless driver resolved the issue.	AOS-W 8.6.0.0
AOS-196593	—	OAW-AP335 access points running AOS-W 8.3.0.8 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **reboot caused by Kernel panic - not syncing: Fatal exception in interrupt PC is at 0x000C7461**. Enhancements to the wireless driver resolved the issue.	AOS-W 8.3.0.8
AOS-196660	—	OAW-AP340 Series access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason as: **Rebooting AP due to default-ip is denied in this network**. The fix ensures that APs work as expected.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196697 AOS-199833	—	OAW-AP505 access points running AOS-W 8.3.0.8 or later versions 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.	AOS-W 8.3.0.8
AOS-196869	—	OAW-AP515 access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **BadAddr:64690a3b303db3 PC:wlc_mutx_bw_policy_update+0x408/0x28b8 [wl_v6] Warm-reset**. This issue occurred when 4 or more MU capable clients were connected to the AP. The fix ensures that the APs work as expected. Duplicates: AOS-199587, AOS-199592, AOS-199431, AOS-201056, AOS-201803, AOS-201192, AOS-201589, AOS-203260, and AOS-203650	AOS-W 8.6.0.0
AOS-197224 AOS-204629	—	A Mobility Controller Virtual Appliance running AOS-W 8.4.0.4 or later versions 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.	AOS-W 8.4.0.4
AOS-197309	—	Clients were unable to obtain the user role from ClearPass Policy Manager. The fix ensures that clients are able to obtain the user role. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197326 AOS-203063	—	Mobility Master running AOS-W 8.5.0.3 or later versions did not generate AirMatch optimization. The fix ensures that the Mobility Master works as expected.	AOS-W 8.5.0.3
AOS-197565	—	APs running AOS-W 8.5.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Dump capture kernel:AP rebooted caused by cold HW reset(power loss).** The fix ensures that the APs work as expected.	AOS-W 8.5.0.2
AOS-197631	—	Policy-based routing was not applied when IPsec map was configured as nexthop. The fix ensures that policy-based routing is applied. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-197912	—	Multicast traffic was not forwarded to the clients when UAC and AAC were different. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-197918	—	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. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	AOS-W 8.5.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197945	—	OAW-AP514 and OAW-AP515 access points running AOS-W 8.5.0.3 or later versions crashed and rebooted unexpectedly. The log file lists the reason for the events as, **BadAddr:ffff00000010 PC:wlc_dump_ aggfifo+0x1160/0x12b0 [wl_v6] Warm-reset.** This issue occurs due to memory corruption. The fix ensures that the APs work as expected.	AOS-W 8.5.0.3
AOS-197994	—	FTP ALG in a session based ACL did not trigger correctly. This issue occurred when DPI was enabled. The fix ensures that the FTP ALG 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-198007	—	APs were unable to ping managed devices and the APs switched between clusters. The fix ensures that the APs work as expected. This issue was observed in access points running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-198157	—	A stand-alone switch running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (Intent:cause: 86:56)**. T The fix ensures that stand-alone switches work as expected.	AOS-W 8.6.0.0
AOS-198173 AOS-197956	—	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. This issue occurred when the opmode was changed from WPA2 to WPA3. The fix ensures that the association ID of a deauthenticated client is cleared. This issue was observed in Mobility Masters running AOS-W 8.5.0.10.	AOS-W 8.5.0.10
AOS-198218	—	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. This issue was observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198261 AOS-202300	—	Mobility Masters running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:f0:2).** The fix ensures that the Mobility Masters work as expected.	AOS-W 8.3.0.0
AOS-198266	—	MAC authenticated clients were unable to reauthenticate even after enabling reauthentication. This issue occurred when the server timed out and reauthentication was not triggered. The fix ensures that the clietnts are deauthenticated and then, reauthenticated when the server recovers from time out. This issue was observed in stand-alone switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.5
AOS-198364	—	A few APs in AM mode were unable to detect the neighboring 2.4 GHz channels. This issue occurred when the AP was power cycled. The fix ensures that the APs can detect 2.4 GHz channels. This issue was observed in APs running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198488	—	An AP rebooted unexpectedly and set an **F** flag. This issue occurred when an 802.1X client was connected to the AP in bridge mode or tunnel mode for wired 802.1X authentication. The fix ensures that the AP work as expected. This issue was observed in OAW-AP205H and OAW-AP303H access points running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198511	—	A few managed devices running AOS-W 8.4.0.5 or later versions 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. 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. The fix ensures that the error message is not displayed.	AOS-W 8.4.0.5
AOS-198605	—	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. This issue was observed in managed devices running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-198787 AOS-198929	—	A OAW-RAP did not come up on a managed device when Verizon U730L modem is used. The fix ensures that the OAW-RAP comes up on the managed device. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198822 AOS-203559 AOS-203959	—	The **show iap table, show user-table internal**, and **show global-user-table list** commands did not display entries in the output .This issue occurred after upgrading to AOS-W 8.4.0.4. . The fix ensures that the commands work 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-198834 AOS-200088 AOS-200555 AOS-201312	—	Some managed devices 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).** This issue was observed in OAW-4750XM switches running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-199119	—	IPv6 DNS address, 2001:4860:4860::8888 was not reachable from source ports 33536 and higher. This issue occurred because UDP packets were treated as ICMPv6 packet and the packets were dropped. The fix ensures that during MLD snooping, packets are forwarded over port-channel as well. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-199184	—	Wired clients lost connectivity and the managed devices took a long time to recover from an uplink failure. This issue occurred when the managed devices were using PPPoE as an uplink. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.3.0.12 later versions.	AOS-W 8.3.0.12

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199291	—	An AAA server sent incorrect authentication response. The fix ensures that the AAA server does not send any incorrect response. This issue was observed in Mobility Masters running AOS-W 8.6.0.5.	AOS-W 8.6.0.5
AOS-199306 AOS-201623	—	APs running AOS-W 8.3.0.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt [packet_lookup_frame+0x30/0x68].** The fix ensures that the APs work as expected.	AOS-W 8.3.0.6
AOS-199381	—	Users were unable to connect to the backup SSID of a OAW-RAP. This issue occurred when the users tried to connect after an AP reboot. The fix ensures that the users are able to connect to the backup SSID of a OAW-RAP. This issue was observed in OAW-RAPs running AOS-W 8.6.0.1 or later versions.	AOS-W 8.6.0.2
AOS-199420	—	Clients roamed 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. This issue was observed in access points running AOS-W 8.2.2.2 or later versions.	AOS-W 8.2.2.2
AOS-199539	—	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. This issue was observed in APs running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-199663	—	After a reboot of mesh auto APs, the configuration changes and mesh auto setting were reset. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-199868	—	MAC clients lost connectivity when they roamed between APs. This issue occurred when machine authentication was enabled. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-199878 AOS-198897 AOS-200006 AOS-200080	—	OAW-AP303H access points running AOS-W 8.5.0.4 or later versions 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 APs work as expected.	AOS-W 8.5.0.4
AOS-199926	—	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. This issue was observed in managed devices running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-199933	—	A Mobility Master running AOS-W 8.4.0.4 or later versions failed to synchronize the RAP whitelist from Activate. This issue occurred when the full-name or the description fields of a RAP whitelist entry had a space. The fix ensures that the Mobility Master works as expected.	AOS-W 8.4.0.4

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-199989	—	Managed devices running AOS-W 8.6.0.2 or later versions 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.	AOS-W 8.6.0.2
AOS-200071	—	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. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.6.0.2
AOS-200084	—	OAW-AP305 access points running AOS-W 8.4.0.4 or later versions 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.	AOS-W 8.4.0.4
AOS-200130	—	Users were unable to change the port status to trusted or untrusted using WebUI or CLI. The fix ensures that users can change the port status. This issue was observed in stand-alone switches running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-200187	—	A Mobility Master assigned duplicate IP addresses to Branch office switches from the VLAN pool. The fix ensures that the duplicate addresses are not assigned. This issue was observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200252	—	OAW-AP515 access points running AOS-W 8.6.0.2 or later versions 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.	AOS-W 8.6.0.2
AOS-200275	—	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. This issue was observed in managed devices running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-200277 AOS-204071	—	Managed devices running AOS-W 8.5.0.8 or later versions logged the error message, **There is only 996 MB left on the flash. At least 1000 MB of free flash space is recommended to keep the system stable**. The fix ensures that the error message is not displayed.	AOS-W 8.5.0.8
AOS-200462	—	A few managed devices did not respond to the SNMP queries from OmniVista 3600 Air Manager regarding rogue information. This issue occurred when: ■ there was a mismatch in the message length between **WMS** process and **AM** process. ■ the managed device was running a higher version of AOS-W than that of the AP. The fix ensures that managed devices respond to SNMP queries. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200534 AOS-203370	—	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. This issue was observed in managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-200568 AOS-202762 AOS-203588	—	GSM channel entries were not replicated from managed device to Mobility Master. The fix ensures that the GSM channel entries are replicated to the Mobility Master. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200595 AOS-203897	—	WebUI displayed the error message **Internal Server Error** when users copied files to SCP server using the **Diagnostics > Technical Support > Copy Files** page. The fix ensures that the WebUI does not display the error message. This issue was observed in OAW-4850 switches running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.4
AOS-200689	—	OAW-AP515 access points running AOS-W 8.6.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **BUGFailureAt:net/core/skbuff.c:1647/consume_skb()! Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.0
AOS-200699 AOS-200760	—	Some users were unable to delete the configured SNMP V3 trap hosts. This issue occurred when IPv4 and IPv6 address type flags were missing. The fix ensures that users can delete SNMP v3 trap hosts. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-201210	—	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. This issue was observed when the managed devices were upgraded to AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201250	—	A few 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. This issue is not limited to any switch platform or AOS-W release version.	AOS-W 8.5.0.5
AOS-201329	—	CPsec toggling stopped working after upgrading to AOS-W 8.6.0.4. 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. The fix ensures that CPsec toggling works as expected. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.10
AOS-201612	—	Role policies configured on a Mobility Master were displayed in a different order on the managed devices in the **Configuration > Roles & Policies > Roles** tab. This issue occurred when the default ACLs got deleted during the initial configuration synchronization after an upgrade. The fix ensures that the policies are displayed in the correct order. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.8

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201681	—	Data traffic to clients on radio 2 failed. This issue occured due to cluster failover. The fix ensures that data traffic does not fail. This issue was observed in tri-radio enabled OAW-AP555 access points running AOS-W 8.6.0.3.	AOS-W 8.6.0.3
AOS-201706	—	BSSIDs were wrongly identified as rouge BSSIDs. The fix ensures that valid BSSIDs are not identified as rouge BSSIDs. This issue was observed in APs running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-202034	—	The **STM** process in a managed device running AOS-W 8.6.0.0 or later versions crashed unexpectedly, due to which a few APs were unable to connect to the managed device. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.0
AOS-202110	—	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. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.6
AOS-202195	—	A managed device running AOS-W 8.3.0.6 or later versions crashed and rebooted unexpectedly. The log file lists 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 devices works as expected.	AOS-W 8.3.0.6
AOS-202257	—	The **show storage** command displayed an error message, **There is only 866 MB left on the flash. At least 1000 MB of free flash space is recommended to keep the system stable. Please clean up your flash filesystem**. The fix ensures that the error message is not displayed. This issue was observed in Mobility Masters running AOS-W 8.5.0.10.	AOS-W 8.5.0.10
AOS-202448	—	OAW-AP535 access points running AOS-W 8.6.0.3 or later versions crashed unexpectedly. The log file listed the reason for the event as **wlan_peer.c:408 Assertion !peer-&gt;peer_delete_in_progress failed**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.3
AOS-202450	—	OAW-RAPs rebooted unexpectedly. This issue occurred when the **activate whitelist download** command was executed and the Mobility Master modified the existing whitelist database entries. The fix ensures that the OAW-RAPs work as expected. This issue was observed in OAW-RAPs running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-202515 AOS-202658	—	APs running AOS-W 8.5.0.2 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Panic:assert Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.2

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202577 AOS-204027 AOS-204410 AOS-204811	—	AirGroup stopped working on managed devices running AOS-W 8.6.0.3 or later versions in a cluster setup. The fix ensures that AirGroup works as expected.	AOS-W 8.6.0.3
AOS-202739	—	A few APs running AOS-W 8.3.0.9 or later versions displayed the error message, **WPA Passphrase not configured for AP**. The fix ensures that the APs work as expected.	AOS-W 8.3.0.9
AOS-202743 AOS-203498 AOS-203507 AOS-204322	—	The **Configuration > Interfaces > VLANs** tab did not display the IP addresses of Mobility Master and managed devices. The fix ensures that WebUI displays the IP addresses. This issue was observed in Mobility Master and managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-202754	—	OAW-AP300 Series access points running AOS-W 8.6.0.2 or later versions 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.	
AOS-203168	—	Managed devices running AOS-W 8.6.0.3 or later versions frequently disconnected from the cluster. Also, the cluster heartbeats were randomly missed on managed devices which led to packet loss. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.3
AOS-203219	—	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. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-203322	—	The command **tar clean logs** did not remove the logs.tar.7z file. The fix ensures that the command works as expected. This issue was observed Mobility Masters running AOS-W 8.5.0.10.	AOS-W 8.5.0.10
AOS-203398	—	A stand-alone switch running AOS-W 8.6.0.3 or later versions sent invalid time stamp values to the server. The fix ensures that incorrect time stamp values are not sent to the server.	AOS-W 8.6.0.3
AOS-203418	—	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. This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-203585 AOS-204245	—	APs running AOS-W 8.3.0.0 or later versions 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.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203656 AOS-204128	—	A managed device displayed an error message, **Please wait while we take the flash backup...Error backing up DBs**, when taking a flash backup. This issue occurred due to incompatible database files. The fix ensures that the database files are migrated in compatible format. This issue was observed when OAW-4850 switches were upgraded from AOS-W 8.3.0.x version to AOS-W 8.6.0.x version.	AOS-W 8.5.0.8
AOS-203698	—	A mismatch was observed in the ACL positions between the Mobility Master and the managed devices. This issue occurred when the ACLs of the user-role are changed. The fix ensures that there is no mismatch in ACL positions. This issue was observed in Mobility Masters and managed devices running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-203702 AOS-204024 AOS-204423 AOS-204544	—	OAW-40xx Series, OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM switches running AOS-W 8.5.0.8 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)** . The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.8
AOS-203859	—	Windows clients were unable to get WINS server information from the Mobility Master running AOS-W 8.3.0.11 or later versions. The fix ensures that windows clients are able to get WINS server information from the Mobility Master.	AOS-W 8.3.0.11
AOS-204025	—	Users were unable to add VLANS to the **Allowed VLANs** field for the trunk port under **Configuration** > **Interfaces** > **Ports** page in the WebUI. The fix ensures that the VLANs are added and displayed in **Allowed VLANs** field. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-204326	—	Clients were unable to connect to OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.4. This issue occurred on APs operating in 5 GHz mode. The fix ensures seamless connectivity.	AOS-W 8.6.0.4
AOS-204367	—	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. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8

Table 6: *Resolved Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204390	—	RADIUS source interface was not working on a managed device running AOS-W 8.5.0.8 or later versions. This issue occurred when RadSec was enabled. The fix ensures that RADIUS source interfacing works as expected.	AOS-W 8.5.0.8
AOS-204428 AOS-204450	—	OAW-AP303H access points running AOS-W 8.3.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.3.0.0
AOS-204532	—	Configurations committed on managed devices are not available on the Mobility Master during backup. This issue occurred when the node-name or path limit exceeds 99 characters. This issue was observed in Mobility Masters running AOS-W 8.4.0.1 or later versions.	AOS-W 8.4.0.1

Known Issues and Limitations in AOS-W 8.6.0.5

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 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** command displays an 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-153742 AOS-194948	188871	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)**. 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-156068	192100	The **DDS** process in a managed device crashes unexpectedly. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions.	AOS-W 8.2.1.1
AOS-157462 AOS-202579	—	The web_cc process crashes on a managed device running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-182847	—	A few users are unable to copy the **WPA Passphrase** field and **High-throughput** profile to a new SSID profile in the **Configuration** > **System** > **Profiles** > **Wireless LAN** > **SSID** > **<SSID_Profile>** 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 **Dashboard** > **Infrastructure** > **Uplink** > **Health** 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

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-185538	—	High number of EAP-TLS timeouts are observed in a managed device. This issue occurs when 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.	AOS-W 8.3.0.8
AOS-187672	—	Memory leak is observed in **arci-cli-helper** process. This issue is observed in Mobility Masters and managed devices running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-188090 AOS-196004 AOS-199152	—	The **Dashboard > Overview > Clients** 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-190071 AOS-190372	—	A few users are unable to access 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. **Workaround:** Perform the following steps to resolve the issue: ■ Remove web category from the ACL rules and apply **any any any permit** policy. ■ Disable WebCC on the user role. ■ Change the VLAN of user role from trunk mode to access mode.	AOS-W 8.4.0.0
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 **Dashboard > Overview** 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	—	All 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

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-193560 AOS-198565 AOS-200262 AOS-204794	—	The number of APs that are DOWN are incorrectly displayed in the WebUI. However, the CLI displays the correct status of APs. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
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. **Workaround:** Delete the IPv4 addresses from ap system profile using the command, **ap system-profile** and from high availability profiles using the command, **ha.**	AOS-W 8.3.0.8
AOS-194381	—	Some managed devices lose the route-cache entries and drop the VRRP IP addresses sporadically. This issue is observed in managed devices 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 **show ap database** 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
AOS-194964	—	A few users are unable to clone 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. **Workaround:** Execute the **rf dot11a-radio-profile <profile name>** command to change the operating mode of the AP from am-mode to ap-mode.	AOS-W 8.5.0.2
AOS-195089	—	The DNS traffic is incorrectly getting classified as **Thunder** and is getting blocked. 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.	AOS-W 8.3.0.7
AOS-195100 AOS-198302	—	The health status of a managed device is incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master's WebUI. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-195101	—	Traffic between Master redundancy Mobility Masters is dropped causing a few processes to be in **PROCESS_NOT_RESPONDING** state. Hence, configurations are not synchronized between the peers. This issue occurs when the **ipsec-mark-mgmt-frames** parameter is enabled in the **firewall wireless-bridge-aging** command. This issue is observed in Mobility Masters running AOS-W 8.2.0.0 or later versions. **Workaround:** Disable **ipsec-mark-mgmt-frames** parameter in the **firewall wireless-bridge-aging** command.	AOS-W 8.5.0.2
AOS-195177	—	Managed devices frequently generate internal system error logs. This issue occurs when the **sapd** 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-195434	—	An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is observed in APs running AOS-W 8.5.0.0 o 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 addresses. This issue occurs when 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.	AOS-W 8.3.0.8
AOS-195939	—	UBT users are assigned **logon** 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 **Configuration > Interfaces > Ports** 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-196229 AOS-196264 AOS-205903	—	Random values are displayed as the host name of a Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 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-196541	—	The API on an AOS-W Mobility Master does not operate over port 443. This issue occurs when there is no rule for login or token generation over port 443. This issue is observed in Mobility Masters running AOS-W 8.5.0.4 or later versions. **Workaround:** Use port 4343 in the API URL to login, subsequently port 443 will work.	AOS-W 8.5.0.4

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
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 so on. 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 **Datapath** process crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.** 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. **Workaround:** The following are recommended: 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. 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.	AOS-W 8.5.0.4
AOS-197048	—	Some clients face degraded Wi-Fi download speed after the managed device resumes function post standby mode. 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.	AOS-W 8.3.0.8
AOS-197127	—	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).** This issue is observed in OAW-4x50 Series switches running AOS-W 8.3.0.7 or later versions in a cluster setup. **Duplicates:** AOS-197060, AOS-197130, AOS-197137, AOS-197161, AOS-197163, AOS-198720, and AOS-201821	AOS-W 8.3.0.7
AOS-197215	—	Users are unable to delete the **Weekend** entry under **Start Day** of **Time range** field in the WebUI. This issue occurs when 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.	AOS-W 8.2.2.6
AOS-197497	—	AirMatch selects the same channel for two neighboring APs even after radar detection. This issue is observed in managed devices running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-197812	—	A mismatch of user roles is observed in the WebUI and CLI of the Mobility Master and managed device. This issue occurs when UDR is configured to assign user role to clients. This issue is observed in both Mobility Masters and managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198024	—	Users are unable to access any page after the fifth page using the **Maintenance > Access Point** 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

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-198281	—	The details of the **Up** time in **Managed network > Dashboard > Access Points > Access Points** table does not get updated correctly. This issue is observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
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 **rf dot11-60GHz-radio-profile** 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-198849 AOS-198850	—	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.** 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-198991	—	Users are unable to add VLAN to an existing trunk port using the **Configuration > Interfaces > VLANs** 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
AOS-199012 AOS-198865	—	A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. This issue is observed in managed devices running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-199423	—	Some L3 redundant Mobility Masters generate **profmgr** error logs. 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 **show airgroup aps** command output and the **auto-associate policy** 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-199884	—	Mobility Master logs the following error messages, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-199947	—	The **Lic. FeatureBit** parameter under the License Client Table changes to **enabled** for Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance. This issue occurs when EVAL license is deleted and the licenses are displayed as 0. This issue is observed in stand-alone switches running AOS-W 8.3.0.11 or later versions.	AOS-W 8.3.0.11

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200446	—	Some users are unable to change the Cluster Profile under **Configuration > Services > Cluster** tab of the WebUI. This issue occurs when there is no VRRP ID configured but the Cluster Profile requests for a VRRP passphrase. This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200733	—	APs crash and reboot unexpectedly. The log file list the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8.** This issue is observed in APs running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-200765	—	Managed deviceslog 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.** This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions in a cluster setup.	AOS-W 8.3.0.7
AOS-201042	—	A large number of packet drops are observed in a few APs running AOS-W 8.3.0.6 or later versions. This issue occurs when the AP SAP MTU datapath tunnel is set to 1514.	AOS-W 8.3.0.6
AOS-201200	—	The **show license-pool-profile** command does not display the output when executed in the **/mm/my node** hierarchy. This issue is observed in Mobility Masters running AOS-W 8.3.0.6 or later versions.	AOS-W 8.5.0.5
AOS-201240	—	When a trusted VLAN is added using the **Interface > Ports > Allowed VLANs** page, the Mobility Master automatically issues the **no trusted vlan** command. This issue occurs 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.	AOS-W 8.5.0.2
AOS-201240	—	Users are unable to add a trusted VLAN using the **Interface > Ports > Allowed VLANs** page and WebUI displays an error message, **VLANs common found in Trusted & Untrusted.** This issue occurs when: ■ Mobility Master automatically issues the **no trusted vlan** command. ■ trunk mode is initially configured using CLI and later modified using the WebUI. This issue is observed in managed devices running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-201273	—	IPsec tunnels are not established between the Mobility Master and managed devices in an IPv6 environment, and the controller-IP address is not displayed in the managed devices. This issue is observed in Mobility Masters running AOS-W running ArubaOS 8.5.0.0 or later versions. **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.	AOS-W 8.6.0.0
AOS-201439 AOS-201448	—	OAW-AP303H access points running AOS-W 8.5.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**.	AOS-W 8.5.0.5
AOS-201454	—	Uplink routing using next-hop list fails after uplink failover. This issue occurs when uplink VLAN 4093 received IP address from a NAT device. This issue is observed in managed devices running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202126 AOS-205098	—	The **profmgr** process continuously restarts on the Mobility Master and hence configurations are not pushed to the managed devices. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-202129 AOS-204127	—	The **Configuration > AP groups** page does not have the **Split radio** toggle to enable the tri-radio feature. 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-202290	—	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. 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.	AOS-W 8.5.0.6
AOS-202341	—	A managed device running AOS-W 8.3.0.8 or later versions crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) ((Intent:cause:register 54:86:0:2c).**	AOS-W 8.3.0.8
AOS-202370	—	Some managed devices reset when the **activate sync** command is issued. 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.	AOS-W 8.5.0.5
AOS-202426 AOS-203652	—	A few 510 Series APs running AOS-W 8.6.0.4 crash and reboot unexpectedly. The log files lists the reason for the event as **PC is at: wlc_phy_enable_hwaci_28nm+0x938 - undefined instruction: 0 [#1]**.	AOS-W 8.6.0.4
AOS-202565	—	OAW-AP515 access points running AOS-W 8.5.0.2 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **kfree+0x74/0xf8 crash.**	AOS-W 8.5.0.2
AOS-202691	—	The **Key Management** column in the **Configuration > WLANs** page of the WebUI displays multiple **wpa2-psk-tkip** entries. This issue occurs when multiple wpa2-psk-tkip opmode SSIDs are created. This issue is observed in stand-alone switches running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-202803	—	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. This issue is observed in Mobility Masters running AOS-W 8.5.07 or later versions.	AOS-W 8.5.07
AOS-203077 AOS-203232	—	Configurations committed using the **firewall cp** command are not synchronized on the standby Mobility Master. This issue occurs when static firewall entries are deleted. This issue is observed in Mobility Masters running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-203097	—	WebUI prompts that additional VLANs will be deleted when a user tries to delete a VLAN. This issue is observed in stand-alone switches running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203098	—	Tunnel user entries are deleted. This issue occurs due to multiple cluster failover. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-203170	—	The class attribute field is missing in the accounting packets of the VIA connection profile. 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.	AOS-W 8.4.0.1
AOS-203184	—	Users are unable to perform captive portal authentication when login URL of the captive portal profile points to ClearPass Policy Manager. This issue is observed in managed devices running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-203201	—	A managed device is unable to download configurations from the Mobility Master using VPNC. This issue is observed in managed devices running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6
AOS-203336	—	The **Dashboard > Infrastructure > Access Points** page of the WebUI and the **show log** command display different values for the last AP reboot time. 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-203438	—	The configuration for EIRP made through the WebUI is not visible in the stand-alone switches running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-203459	—	It takes a long time to import a guest provisioning file with a very few users to the Mobility Master’s local database. This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.3
AOS-203517 AOS-204709	—	The Datapath module crashes and managed devices crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).** This issue occurs when data packets undergo multiple GRE encapsulation. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-203597 AOS-203927	—	The number of VIA licenses used are higher than the total number of users connected to VIA. 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. **Workaround:** Reboot the managed device to restore the VIA licenses.	AOS-W 8.5.0.6
AOS-203712	—	Avaya Spectalink wireless phones reboot unexpectedly with the error message, **No AVPP response from 192.168.249.001.** 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.	AOS-W 8.5.0.7
AOS-203958	—	Blacklisted clients are visible in **Dashboard > Security > Blacklisted Clients** although these clients are removed using the WebUI. This issue is observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204057	—	4-way handshake is not initiated when MAC authentication fails on OWE clients. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.6.0.3
AOS-204142	—	A few users are assigned the default 802.1X roles from AAA profile instead of SDR-configured roles. This issue occurs when the **no cert-cn-lookup** parameter under **aaa authentication dot1x** command is configured on the 802.1X profile. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.6.0.4
AOS-204187	—	The command **vpn-peer peer-mac** does not support Suite-B cryptography for custom certificates. This issue is observed in Mobility Masters running AOS-W 8.2.2.8 or later versions.	AOS-W 8.2.2.8
AOS-204241	—	Managed devices log spurious DHCP DBUG messages. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-204414	—	The VLAN range configured using the **ntp-standlaone vlan-range** command is not correctly sent to the managed devices. 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. **Workaround:** Delete the VLAN range configured on the Mobility Master and re-configure the **ntp-standlaone vlan-range.**	AOS-W 8.3.0.8
AOS-204529 AOS-204861 AOS-206217	—	The IP Addresses of Wired Clients in **Dashboard > Overview > Clients** page are displayed as 0.0.0.0. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-204663	—	The **show running-config** command does not display a few user roles. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-204697	—	The **Auth** field for 802.1X PUTN users is incorrectly updated as **tunneled-user-MAC** instead of **tunneled-user-Dot1x** when the s**how user-table** command is executed. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-204764	—	AP configurations are reset and APs move to the default AP group after reboot. This issue is observed in APs running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-204917 AOS-205979	—	The **dpagent** process on managed devices running AOS-W 8.5.0.10 or later versions crashes unexpectedly. The log file lists the reason for this event as **Memory usage limit exceeded for process: dpagent current pages**.	AOS-W 8.5.0.10

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-204948	—	Access points running AOS-W 8.5.0.7 crash and reboot unexpectedly. The log file lists the reason for this event as **kernel panic: Fatal exception with NIP: e445c71c LR: e4490ac0 CTR: c0567b30**.	AOS-W 8.5.0.7
AOS-205010	—	The **OFA** process crashes in managed devices, due to an increase in the number of IP user events. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-205025	—	The switch does not retrieve cluster inner-IP from the whitelist database as the request is initiated from an OAW-IAP. This issue is observed in switches running AOS-W 8.6.0.4. Workaround: Provision the OAW-IAP as OAW-RAP.	AOS-W 8.6.0.4
AOS-205112	—	Managed device running AOS-W 8.3.0.7 or later versions reboot unexpectedly. This issue occurs due to a memory leak in the **OFA** process.	AOS-W 8.3.0.7
AOS-205171	—	Mobility Masters and managed devices running AOS-W 8.5.0.7 or later versions display a log message, **Received MAP_ADD from IKE for default-local-master-ipsecmap**. This issue occurs when tunnels are established.	AOS-W 8.5.0.7
AOS-205190	—	The **auth** process in a managed device crashes unexpectedly. 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.	AOS-W 8.3.0.7
AOS-205253 AOS-205644	—	Public key authentication fails on OpenSSH version 7. This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-205634	—	The WebUI does not display the port channel membership. This issue occurs when port members are added to the PC-0 port channel. This is was observed in managed devices running AOS-W 8.6.0.4.	AOS-W 8.6.0.4
AOS-205702	—	OAW-4850 switches running AOS-W 8.3.0.0 or later versions disconnect TCP session and hence internal captive portal is not working. This issue occurs due to **nginx** process crash.	AOS-W 8.5.0.8
AOS-205935	—	Management users created on Mobility Master are not synchronized on standby Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.8
AOS-206115	—	High efficiency and very high throughput values disabled using **wlan ht-ssid profile** command are displayed in the output of **show ap bss-table** command. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.9
AOS-206541	—	The **Maintenance** > **Software Management** page does not display the list of all managed devices that are a part of a cluster. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8

Table 7: *Known Issues in AOS-W 8.6.0.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206636 AOS-206629	—	L2TP VPN connection fails on Mac, IOS and android clients. This issue occurs when: ■ clients initiate L2TP connection on random src port instead of the standard src port, 1701. ■ clients connect behind a NAT device. This issue is observed in managed devices running AOS-W 8.4.0.6 or later versions.	AOS-W 8.4.0.6
AOS-206890	—	The **body** field in **Configuration > Services > Guest Provisioning** page of the WebUI does not allow users to add multiple paragraphs for email messages. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-207411	—	Managed devices are unable to join the L3 redundant Mobility Master. This issue occurs when the managed devices are rebooted after a successful failover to the L3 redundant Mobility Master. This issue is observed in managed devices running AOS-W 8.6.0.1 or later versions. **Workaround:** Restart the **licensemgr** process for the managed devices to join the L3 redundant Mobility Master.	AOS-W 8.6.0.1

Chapter 7 Upgrade Procedure

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

CAUTION

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

Topics in this chapter include:

Important Points to Remember

To upgrade your managed device or Mobility Master:

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

- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Master Licensing Guide*.
- Multiversion is supported only if the Mobility Master is running two code versions higher than the code versions running on the managed devices. For example multiversion is supported if a Mobility Master is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.3.0.0 and will not be supported if the managed devices are running AOS-W 8.2.0.0 or AOS-W 8.4.0.0.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 40 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 40 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 40 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

```
(host) #write memory
```

2. Execute the following command to back up the contents of the flash memory to the **flashbackup.tar.gz** file.

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

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

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


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

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

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

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

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

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

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 39.

NOTE

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

In the WebUI

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

1. Download the AOS-W image from the customer support site.
2. Upload the AOS-W image to a PC or workstation on your network.

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

NOTE

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

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

NOTE

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

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

In the CLI

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

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

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

or

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

or

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

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

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

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

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

   or

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

   or

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

   or

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

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

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

7. Reboot the Mobility Master.

   ```
   (host)#reload
   ```

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

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

Verifying the AOS-W Upgrade

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

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 40 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 40 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 40.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

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

CAUTION

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

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

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

In the CLI

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

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

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

   or

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

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

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

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

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

CAUTION

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

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

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