AOS-W 8.6.0.22 Release Notes

Alcatel·Lucent
Enterprise

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.

Contents

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:

- New Features and Enhancements
- Supported Platforms
- Regulatory Updates
- Resolved Issues
- Known Issues and Limitations
- Upgrade Procedure

For a list of terms, refer Glossary.

Related Documents

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

- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W API Guide*
- *Alcatel-Lucent Mobility Master Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent AP Software Quick Start Guide*

Supported Browsers

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

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	- Windows 10 or later - macOS
Firefox 107.0.1 or later	- Windows 10 or later - macOS
Apple Safari 15.4 (17613.17.1.13) or later	macOS
Google Chrome 108.0.5359.71 or later	- Windows 10 or later - macOS

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our ALE culture and moving forward, ALE will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

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

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

New Features and Enhancements

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

Enhancements to the OFA Core Size

By excluding a section of process memory, OFA core size is reduced. This reduction helps in capturing and debugging OFA cores in scale scenarios.

PoE Support for OAW-AP535 Access Point

OAW-AP535 access points can now boot up while using a USB converter and a console cable that's powered by PoE switch.

Behavioral Changes

This release does not introduce any changes in AOS-W behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.6.0.22.

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 8.6.0.22*

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 8.6.0.22*

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 8.6.0.22*

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
OAW-AP228 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-AP303P
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

Table 5: *Supported AP Platforms in AOS-W 8.6.0.22*

AP Family	AP Model
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 https://myportal.al-enterprise.com/.

The following DRT file version is part of this release:

■ DRT-1.0_87407

The following issues are resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.6.0.22*

New Bug ID	Description	Reported Version
AOS-210186	UBT 1.0 clients switching between Gateway user roles experienced VLAN assignment discrepancies. The fix ensures the feature works as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.0.0
AOS-217784 AOS-243309	Some access points crashed and rebooted unexpectedly. The issue occurred due to a buffer overflow when the Intelligent Thermal Management (ITM) or Intelligent Power Monitoring (IPM) features were enabled on the APs. The fix ensures the APs work as expected. This issue was observed in AP-505H access points running AOS-W 8.6.0.19 or later versions.	AOS-W 8.6.0.19
AOS-228581 AOS-242780 AOS-242783 AOS-228791	VPNCs crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot Cause: Datapath timeout (SOS Assert) (in ipsec_decrypt)**. This issue occurred when the buffer memory was queued in the wrong processor. The fix ensures VPNCs work as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.20
AOS-228707 AOS-237743	The **upgrade managed-devices** command displayed the error message **Download failed** when upgrading VMCs from Mobility Masters. The fix ensures the command executes as expected. This issue was observed in managed devices running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-231952 AOS-239896	Some access points crashed and rebooted unexpectedly. The log files listed the event as: **Firmware Assert - PC : 0x4b1ce6dc, whal_xmit.c:5664 Assertion 0 failedparam0**. The fix ensures the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-232717 AOS-245030 AOS-243103	The VPNC crashed and rebooted unexpectedly with reboot cause: **Nanny rebooted machine - isakmpd process died (Intent:cause:register 34:86:50:60)**. The fix ensures the VPNC works as expected. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.17
AOS-235133 AOS-239713 AOS-234579	Management authentication failed intermittently when **mschapv2** was used. The fix ensures successful management authentication. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.5

Table 6: *Resolved Issues in AOS-W 8.6.0.22*

New Bug ID	Description	Reported Version
AOS-237710	During ARP discovery, devices with the same IP as the AP's default gateway caused the MAC address of the IP to be overwritten in the ARP cache, leading to unexpected rebootstrap processes. The fix ensures the ARP process is executed successfully and APs work as expected. This issue was observed in APs running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-238604	The AP regulatory domain profile displayed different information in the WebUI and CLI. The fix ensures the information displayed in the WebUI matches with the CLI. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.17
AOS-238656 AOS-242252	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as: **Kernel panic - not syncing: Take care of the TARGET ASSERT first (ratectrl.c:999).** The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-238817	In some controllers running AOS-W 8.6.0.19 or later versions, the **Dashboard > Security > Suspected Rogue and Authorized** section of the WebUI displayed the error message: **Error retrieving information. Please try again later**. This caused the list of APs to not populate correctly. This issue occurred due to non UTF-8 characters being used in external BSSIDs. The fix ensures the WebUI displays the correct information. This issue was observed in Mobility Masters running AOS-W 8.6.0.19 or later versions.	AOS-W 8.6.0.19
AOS-238846	The error message **Exceeds the max supported vlans 128** displayed when creating layer 2 VLANs at folder level. The issue was caused by matching strings in other paths being incorrectly included in the device bitmap. The fix ensures only the correct number of VLANs is taken into consideration for the VLAN count. This issue was observed in Mobility Masters running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-238921 AOS-241183 AOS-242610	Some OAW-4750XM switches running AOS-W 8.6.0.17 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. This issue occurred when IPv6 DNS response was received. The fix ensures that the switches work as expected.	AOS-W 8.6.0.17
AOS-239291 AOS-240342 AOS-241393 AOS-242378 AOS-243717 AOS-244878	OmniAccess Mobility Controllers unexpectedly crashed and rebooted. The log files listed the reason for the event as: **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures the controller works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.19 or later versions.	AOS-W 8.6.0.19
AOS-239472 AOS-242785	The **show loginsessions** command displayed multiple entries with empty **User Name** and **User Role**. This issue also caused the SSH process to fail. This issue occurred as the CLI processes from previous sessions were still active in the background. The fix ensures such sessions are timed out accordingly, discarding empty entries in the **show loginsessions** command and resolving issues with the SSH process. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.2

Table 6: *Resolved Issues in AOS-W 8.6.0.22*

New Bug ID	Description	Reported Version
AOS-240419	Some packets loss was observed when sending traffic over a network secured using WPA3 and CNSA. This issue occurred when downloading files from a SMB server in a PC running Windows 10. The fix ensures the APs work as expected. This issue was observed in OAW-AP505 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.5
AOS-240425	The HTTPS connection was interrupted and the ICMP communication was blocked for some VIA clients. This issue occurred when, ■ the default size of 1452 bytes was used for MTU ■ the DF bit was set for IP packets This issue was observed in controllers running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-240435 AOS-242244	Some APs sent random false alerts to OmniVista 3600 Air Manager's monitor to display their status as **Down** while remaining **Active** on the controller. The fix ensures APs work as expected. The issue was observed in switch-managed APs monitored by OmniVista 3600 Air Manager 8.2.15.0 or later versions.	AOS-W 8.7.1.10
AOS-240653	The size of **/mswitch/logs/fpapps.log** file increased indefinitely by 40 MB per month, overutilizing memory resources. The fix ensures the log files are handled as expected. This issue was observed in standalone controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.2
AOS-241086	Some clients were unable to connect to the controller due to crashes of the **auth_mgr** process after upgrading from AOS-W 8.6.0.7 to AOS-W 8.10.0.5 or earlier versions. The fix ensures the clients can connect as expected.	AOS-W 8.10.0.5
AOS-241313	Zebra TC21 barcode scanners were unable to maintain a connection and send traffic when connected to OAW-AP505 devices running AOS-W 8.10.0.5 or earlier versions. The fix ensures TC21 barcode scanners can successfully connect to APs and pass traffic as intended.	AOS-W 8.10.0.5
AOS-241325	In some switches running AOS-W 8.6.0.0 or later versions, the **Beacon Period** in the **Configuration > System > Profiles > RF Management** section in the WebUI, and the **show rf dot11a-radio-profile** command in the CLI was displayed as 100 msec. Instead, the **Beacon Period** should be expressed as 100 time units or 102.4 msec. The fix ensures that the **Beacon Period** value and units are displayed correctly.	AOS-W 8.6.0.0
AOS-241438	A case sensitive check was performed when the following commands were executed in the CLI: ■ **show global-user-table list name <username>** ■ **show global-user-table list role <role name>** ■ **show global-user-table count ap-name <name>** This prevented users from getting accurate search results for usernames or APs. The fix ensures the command works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.10.0.5

Table 6: *Resolved Issues in AOS-W 8.6.0.22*

New Bug ID	Description	Reported Version
AOS-241498 AOS-245217	A corrupt bridge ACL issue was observed in APs running AOS-W 8.6.0.17 or later versions, where some user roles were either missing or containing a duplicate of the **logon** role. This prevented the AP from passing traffic. The fix ensures the ACL bridge works as expected.	AOS-W 8.6.0.17
AOS-241737	The **RADIUS User-Name** attribute contained an empty value in the RADIUS Accounting-Stop packet when an authenticated Captive-Portal client clicked the logout button. The fix ensures the User-Name attribute contains user-name value in the RADIUS Accounting-Stop packet. This issue was observed in managed devices running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-241863 AOS-242637	The ACL was incomplete in the SAPD and data path modules, and it caused connectivity issues. The fix ensures that the process works as expected. This issue was observed in APs running AOS-W 8.10.0.5 or earlier versions.	AOS-W 8.10.0.5
AOS-241937	A few user-based tunnelled users failed to come up on managed devices due to certain race condition in the sequence of events during the user bootstrap process. This issue was observed in managed devices running AOS-W 8.10.0.2 or earlier versions. The fix ensures user-based tunneling works as expected.	AOS-W 8.10.0.2
AOS-242238 AOS-241669	Some users connected to open SSIDs were able to access video services even after their session timed out. The issue occurred due to session expiration times not supported in **datapath**. The fix ensures no video services are allowed to users when their sessions time out. This issue was observed in APs in split tunnel mode running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-242301	The 802.1x module crashed intermittently and occasioned the controller to reboot. This issue occurred due to a double freeing error in the 802.1x module, generated by a timer issue. The fix ensures the module works as expected. This issue was observed in controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.0.0
AOS-242469	Mobile devices were unable to connect to Passpoint SSID. This issue occurred when EAP transactions were sent across two different Radsec connections to cloud guest server. The fix ensures that mobile devices connect to Passpoint SSID as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-242638	In some controllers running AOS-W 8.6.0.0 or later versions, Security Association attributes (SAs) were not cleared when crypto-map was disabled. This caused IKE/IPSec tunnels to block traffic in Site-to-Site connections. The fix ensures IKE/IPSec SAs are properly cleared and built after disabling and re-enabling crypto-maps.	AOS-W 8.6.0.0
AOS-242696	Users were unable to convert OAW-APs running AOS-W 8.6.0.0 or later versions to OAW-IAPs and AOS-W 10.x APs, while attempting to upgrade. This issue occurred when the **ap convert** command was run with pre-validation enabled, and the pre-validation process was interrupted before completion.	AOS-W 8.6.0.0

Table 6: *Resolved Issues in AOS-W 8.6.0.22*

New Bug ID	Description	Reported Version
AOS-242852	In some controllers running AOS-W 8.6.0.0 or later versions, tunneled_ user creation failed upon a bridge miss. This fix ensures tunneled_user is created, even if bridge miss happens.	AOS-W 8.6.0.0
AOS-243132	Some standalone controllers running AOS-W 8.6.0.0 or later versions were not aging out captive portal users from the user table when connected to a wired split tunnel. The fix ensures the controllers perform as expected.	AOS-W 8.6.0.0
AOS-243164	Some OmniAccess Mobility Controllers unexpectedly crashed due to **show-auth-tracebuf** process. A correction in the segmentation fixed the issue. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.0.0.0 or later versions.	AOS-W 8.0.0.0
AOS-243265	Some access points unexpectedly created AP panic dumps. The log files listed the reason as: **Unable to handle kernel NULL pointer dereference at virtual address 00000014**. The fix ensures 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 8.10.0.5
AOS-243621	OmniAccess Mobility Controllers sent incorrect channel bandwidth data for mesh radios reported in SNMP **wlsxWlanRadioTable**. The problem was caused by incomplete information being sent to the module during setup. The fix ensures channel bandwidth data is correctly reported. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.11
AOS-243722	Some Managed Devices running AOS-W 8.6.0.20 or later versions, were unable to display **auth-survivability** cached data when certain time zones were configured, like Asia or Jakarta (WIB). The fix ensures that the data is cached correctly.	AOS-W 8.6.0.20
AOS-243959 AOS-244379 AOS-245581	Some OAW-AP555 running AOS-W 8.6.0.0 or later versions crashed while running the **show ap arm scan_times ap-name** command. This issue led to client devices disconnection. The fix ensures the AP performs as expected in this scenario.	AOS-W 8.6.0.0
AOS-244247	The value for **attack-rate tcp-syn <#>** was unable to be set over 255, causing clients to not be blacklisted. The fix ensures the value can be set over 255. This issue was observed in controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-244358	In the WebUI **Dashboard > Overview > Clients > Name**, the SSID of the clients incorrectly displayed the IP or the MAC address. The fix ensures the SSID displays correctly. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-244628	Some OAW-AP315 were unable to upgrade using the **apflash ap31x-ap32x backup partition** command. The fix ensures the command works as expected. This issue was observed in OAW-AP315 running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21

Table 6: *Resolved Issues in AOS-W 8.6.0.22*

New Bug ID	Description	Reported Version
AOS-244736	Some OmniAccess Mobility Controllers using UBT feature were incorrectly forwarding unicast traffic to other UBT tunnels. The fix ensures the feature works as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-244800 AOS-245378	Some Mobility Controllers unexpectedly crashed. The log files listed the reason as: **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:4).** The fix ensures the controllers work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21
AOS-244875	Some OmniAccess Mobility Controllers acting as BGWs crashed intermittently during the clean-up of 802.1X Authenticated users. The fix ensures the controllers work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-245050	In the WebUI, **Dashboard** > **Infrastructure** > **Model**, some managed devices displayed their name without the prefix **AP**. The fix ensures the names are displayed correctly. This issue was observed in Access Points running AOS-W 8.6.0.20 or later versions in a cluster configuration.	AOS-W 8.6.0.20

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

Limitation

Following are the limitations observed in this release:

Airtime Fairness Mode

Airtime Fairness Mode is not supported in 802.11ax access points.

Port-Channel Limitation in OAW-4850 switches

On OAW-4850 switches with all the member ports of each port-channel configured from the same NAE (Network Acceleration Engine), if one of the member ports experiences link flap either due to a network event or a user driven action, the rest of the port-channels also observe the link flap for less than a second.

No Support for Unique Local Address over IPv6 Network

The IPv6 addresses for interface tunnels do not accept unique local addresses.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** 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-155404 AOS-207878	191106	An AP is unable to establish IKE/IPsec tunnel with the managed device. This issue occurs when the AP is enrolled with EST certificates. This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-156068	192100	The **DDS** process in a managed device running AOS-W 8.2.1.1 or later versions crashes unexpectedly.	AOS-W 8.2.1.1
AOS-182073 AOS-183743	—	An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT: rcRateFind+229; ratectrl_11ac.c:2394**. This issue is observed in OAW-AP315 access points running AOS-W 8.2.1.0 or later versions.	AOS-W 8.2.1.0
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 using WebUI. This issue is observed in managed devices running AOS-W8.4.0.0 or later versions 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 Masters running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-185538 AOS-195334	—	High number of EAP-TLS timeouts are observed in managed devices. 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 AOS-213397	—	Memory leak is observed in the **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-188255 AOS-192725	—	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-188972 AOS-194746 AOS-208631 AOS-213627	—	Mobility Master displays the blacklisted clients although the clients were removed from the managed device. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions in a cluster setup.	AOS-W 8.4.0.4
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:	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
		1. Remove web category from the ACL rules and apply **any any any permit** policy 2. Disable WebCC on the user role. 3. Change the VLAN of user role from trunk mode to access mode.	
AOS-190621 AOS-198482	—	WebUI does not filter the names of the APs that contain the special characters, +, %, and &. This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions.	AOS-W 8.4.0.2
AOS-193184	—	All L2 connected managed devices move to L3 connected state after an 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-193231 AOS-200101 AOS-207456	—	The **Dashboard > Infrastructure > Access Devices** page of the WebUI displays an error message, **Error retrieving information**. This issue is observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-193278 AOS-228782	—	Users are unable to bring up the VPNC after an upgrade. The switch is stuck with an error message, **CONTROLLER-IP/V6 NOT SET(00:1a:1e:05:cd:28)**. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-193560 AOS-198565 AOS-224274 AOS-200262 AOS-204794 AOS-208110 AOS-209989 AOS-212249	—	The number of APs that are DOWN are incorrectly displayed in the **Dashboard > Overview** page of 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 8.6.0.19
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-194080	—	Some controllers display the error message, **Deleting a user IP=fe80::1c4d:d31f:a935:2107 with flags=0x0 from the datapath that does not exist in auth** even if IPv6 is disabled on the managed devices. This issue is observed in stand-alone controllers running AOS-W 8.2.2.10 or later versions.	AOS-W 8.4.0.4
AOS-194370	—	High memory utilization is observed in the **cluster manager** 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

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
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 configurations 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 AOS-204455 AOS-206735	—	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
AOS-195177	—	Some 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 controllers running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-195434	—	Some APs crash and reboot 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 or later versions in a Mobility Master-managed device topology.	AOS-W 8.5.0.2
AOS-196457	—	Clients are reporting various issues in terms of performance, client connectivity, and AP showing up high noise floor for more than 48 hours. This issue is observed in OAW-AP515 access points running AOS-W 8.5.0.2 or later versions.	AOS-W 8.5.0.2
AOS-196590	—	Some OAW-4104 controllers running AOS-W 8.6.0.0, and later versions crash and reboot unexpectedly. This issue is observed when an unsupported third-party cellular modem is connected to the controller for a cellular uplink.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-196864	—	Although a new VLAN ID is successfully connected, the managed devicedisplays that the 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	—	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**: Perform one of the following steps to resolve the issue: 1. 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. 2. 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-197494	—	The **show datapath debug opcode** command displays hexadecimal output. This issue is observed in managed devices running AOS-W 8.3.0.1 or later versions.	AOS-W 8.3.0.1
AOS-197756 AOS-227874 AOS-239268 AOS-193883	—	A few APs are unable to use DHCP IPv6 addresses and option 52 for master discovery. This issue occurs when APs did not clear the previous LMS entries after an upgrade. This issue is observed in access points running AOS-W 8.3.0.8 or later versions. **Workaround**: Delete the IPv4 addresses from the 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-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 controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0

Table 7: *Known Issues in AOS-W 8.6.0.22*

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-198382	—	The output of the command, **show aaa state message** does not display any name for opcodes 204 and 253. The issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198483	—	The 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-198702	—	The warning message, I**nitializing certificates WARNING: can't open config file: /usr/local/ssl/openssl.cnf** displays when upgrading Mobility Masters. This issue is observed in Mobility Masters running AOS-W 8.6.0.21 or later versions.	AOS-W 8.6.0.21
AOS-198829 AOS-199188	—	An incomplete route cache causes the OAW-4104 gateway to not learn the client's ARP. This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
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 an error message, **Feature is not enabled in the license**. This issue is observed in stand-alone controllers running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-198991	—	Users are unable to add a 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-199492	—	Some APs do not get displayed in the **show airgroup aps** command output and the auto-associate policy does not work 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-199724 AOS-214805	—	Reverse Policy Based Routing (PBR) is not working when applied to the VPN tunnel's Access Control List (ACL) in hub and spoke setups. This issue is observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200515 AOS-219987	—	The **DDS** process crashes on managed devices running AOS-W 8.3.0.10 or later versions. This issue occurs when HA is inadvertently attempted between AOS-W 6.5.x and AOS-W 8.x, up to AOS-W 8.9 where the issue is fixed.	AOS-W 8.3.0.10
AOS-200733 AOS-209999	—	Some APs running AOS-W 8.5.0.3 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8**.	AOS-W 8.5.0.3
AOS-200765	—	Some managed devices running AOS-W 8.3.0.7 or later versions in a cluster setup log the error message, **|authmgr| |cluster| gsm_auth.c, auth_ gsm_publish_ip_user_local_section:1011: auth_ gsm_publish_ip_user_local_section: ip_user_ local_ flags**.	AOS-W 8.3.0.7
AOS-200781	—	Some managed devices log the error message, **INFO> |dot1x-proc:1| Sending request for Switch IP6** although there are no IPv6 configurations in the network. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.7.0.0
AOS-201376	—	The measured power, **Meas. Pow** column in the **show ap debug ble-table** command does not get updated when the TX power of an AP is changed. This issue is observed in APs running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-201439 AOS-201448	—	Some 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-202129 AOS-204127	—	The **Configuration** > **AP groups** page does not have the **Split radio** toggle button to enable the tri-radio feature. This issue is observed in stand-alone controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-202519	—	The interface tunnel with IPv6 fails to accept Unique Local Address (ULA) as a valid address. This issue is observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-202552	—	The **Dashboard** > **Traffic Analysis** > **AppRF** page of the WebUI displays **Unknown** for WLANs, Roles, and Devices. This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
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

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203213	—	Some Mobility Masters running AOS-W 8.5.0.8 crash and reboot in a continuous loop. This issue is observed on upgrading to AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
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 controllers running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-203438	—	The EIRP value configured using the WebUI is not visible in stand-alone controllers running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-203614 AOS-209261	—	The Mobility Master dashboard does not display the number of APs and clients present in the network. This issue is observed in Mobility Masters running AOS-W 8.6.0.2 or later versions.	AOS-W 8.6.0.2
AOS-203652	—	Some OAW-AP515 access points running AOS-W 8.6.0.4 crash and reboot unexpectedly. The log files list the reason for the event as: I**nternalError: Oops - undefined instruction: 0 1 SMP PC:wlc_phy_ enable_hwaci_28nm+0x938/0x1b20 [wl_v6] Wa**.	AOS-W 8.6.0.4
AOS-203682 AOS-195432 AOS-218290 AOS-195433 AOS-220829	—	The **Dashboard** > **WLANs** page of the WebUI does not display the list of all the clients and APs. This issue is observed in Mobility Masters running AOS-W 8.5.0.2 or later versions.	AOS-W 8.6.0.15
AOS-204414	—	The VLAN range configured using the **ntpstandalone 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 n**tpstandalone vlan-range**.	AOS-W 8.3.0.8
AOS-205319 AOS-206993 AOS-220039 AOS-225941	—	Some APs running AOS-W 8.6.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**.	AOS-W8.7.0.0
AOS-206178	—	System logs do not display the reason why an AP has shut down. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206541	—	The **Maintenance > Software Management** page does not display the list of all managed devices that are 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
AOS-206752	—	The console log of 7205 controllers running AOS-W 8.5.0.9 or later versions displays the **ofald| |sdn| ERRS ofconn_rx:476 <10.50.1.26:6633> socket read failed, err:Resource temporarily unavailable(11)** message.	AOS-W 8.5.0.9
AOS-206795	—	A user is unable to rename a node from the Mobility Master node hierarchy. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions. **Workaround**: Restart **profmgr** process to rename the node.	AOS-W 8.3.0.7
AOS-207245	—	Some managed devices running AOS-W 8.5.0.8 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 53:86:0:802c)**.	AOS-W 8.5.0.8
AOS-207366	—	The **show advanced options** menu is not available in the **Configuration > Access Points > Campus APs** page of the WebUI. This issue occurs when more than one AP is selected. This issue is observed in Mobility Masters running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-208505	—	Some OAW-AP325 access points running AOS-W 6.5.4.0 are crashing and rebooting unexpectedly. The log file lists the reason for the event as: **Reboot after image upgrade failed: 65280 shutting down watchdog process (nanny will restart it)**. This issue occurred when attempting to upgrade the OAW-AP325 access points to AOS-W 8.6.0.4.	AOS-W 8.6.0.4
AOS-208686	—	The **Dashboard > Services > Wireless Calls** page of the WebUI, displays two different score types without an appropriate header. The units are not the same but are labelled as Score (**Controller > Score- and End-toEnd > Score**) This issue is observed on Mobility Controllers running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-209580	—	The output of the **show ap database** command does not display the **o** or **i** flags, which indicate whether an AP is an outdoor AP or an indoor AP. This issue occurs when the AP installation type is not set to default. This issue is observed in Mobility Masters running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209888 AOS-224884 AOS-228474	—	The **Diagnostics > Tools > AAA Server Test** page of the WebUI displays the **Authentication** status as **0** instead of **Authentication Successful**. This issue is observed in managed devices running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14
AOS-209912	—	A few managed devices fail to filter and drop spoofed ARP responses from the clients. The user entry for the other IP address is present on the managed devices but not in the route cache table. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209977	—	An SNMP query with an incorrect string fails to record the offending IP address. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210198	—	The **Dashboard > Security > Detected Radio** page of the WebUI displays incorrect number of **Clients**. This issue is observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-210329	—	Some managed devices advertise stale maxAge OSPF LSA to its peers which prevents the installation of IKE routes. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210482	—	Some managed devices running AOS-W 8.3.0.6 or later versions display the error message, **Invalid set request** while configuring ESSID for a Beacon Report Request profile.	AOS-W 8.3.0.6
AOS-210992	—	The Mobility Master displays an error message, Flow Group delete: id not found after an upgrade. This issue occurs when logging levels are not configured correctly. This issue is observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212038	—	The **show memory <process-name>** command does not display information related to the **dpagent** process. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212255	—	Some APs are stuck in **Not in Progress** state during cluster live upgrade. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-214846	—	The status of the APs is incorrectly displayed as **Down**. This issue is observed in Mobility Conductors running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-215138 AOS-207006	—	APs go down and UDP 8209 traffic is sent without UDP 4500 traffic. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-215852	—	Mobility Masters running AOS-W 8.6.0.6 or later versions log the error message, **ofa: 07765|ofproto|INFO|Aruba-SDN: 1 flow_mods 28 s ago (1 modifications)**. This issue occurs when openflow is enabled and 35 seconds is configured as UCC session idle timeout.	AOS-W 8.6.0.6
AOS-217890	—	Some managed devices running AOS-W 8.5.0.10 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (SOS Assert)**.	AOS-W 8.5.0.10
AOS-218426	—	The status LED displays incorrect status. This issue is observed in standalone switches running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-218844 AOS-222351 AOS-227400 AOS-231009	—	A Mobility Master picks only 43% of the APs for cluster CRU. This issue is observed in Mobility Masters running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-219765 AOS-231995 AOS-232259	—	Some OAW-AP555 access points running AOS-W 8.6.0.15 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **AP-555 crashed: Take care of the TARGET ASSERT first - ar_wal_tx_seq.c:3041 Assertion seq_ctrl.**	AOS-W .1.7
AOS-220318	—	The **show ap bss-table** command does not display the flags in alphabetical order. Also, some missing flags are displayed in the status legend but are not documented. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-220457 AOS-219484 AOS-219343 AOS-220151	—	The **Configuration > WLANs** page of the WebUI does not allow users to enter new VLANs. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-220465 AOS-216062	—	Huawei E8372h-155 modem not connecting to some 7000 Branch Gateways. This issue is observed is devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-220515	—	Some managed devices running AOS-W 8.0.0.0 or later versions display the error message, **|fpapps| filling up the default gateway configuration.**	AOS-W 8.0.0.0

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220903	—	The **s** flag indicating LACP striping is not displayed in the output of the show ap database long command even if LLDP is enabled on two uplinks. This issue is observed in APs running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-221882 AOS-212772	—	Some IPv6 clients are unable to access websites that have only IPv4 addresses. This issue is observed in Mobility Conductors running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-222493	—	The **AP group** drop-down list in the **Configuration > Access Points > Campus APs** page of the WebUI takes a long time to load the list of available AP groups. This issue is observed in Mobility Masters Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.3
AOS-224143 AOS-221378	—	The output of the **show ap debug radio-stats** command displays incorrect Rx data frame statistics. This issue is observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-224463	—	The RADIUS Radsec server does not work with TPM certificates on Mobility Master running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-225070	—	The AirGroup server table incorrectly displays duplicate host names. This issue is observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-225214	—	A few managed devices incorrectly send the VPNC IP address as 0.0.0.0 to the OmniVista 3600 Air Manager server. This issue is observed in managed devices running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-225263 AOS-232589 AOS-242807	—	L2 database synchronization fails on standby controllers. This issue is observed in stand-alone controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-226426	—	The Mobility Master Hardware Appliances running AOS-W 8.5.0.10 or later versions display the message DHCP WAIT and the menu options are disabled. This issue occurs after a reboot.	AOS-W 8.5.0.10
AOS-226683	—	The **show running-config** command does not display information about the IP RADIUS source-interface loopback. However, the **show configuration effective detail** command displays information about the IP RADIUS source-interface loopback. This issue is observed in managed devices running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-227016 AOS-229420	—	Some users experience a delay while downloading the VIA VPN profile. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227076 AOS-226143	—	AppRF fails to classify traffic for a few applications. This issue is observed in stand-alone controllers running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-227258	—	The **Dashboard > Overview** page of the WebUI displays the status of 2.4 GHz radio even when 2.4 GHz radio was disabled in the rf dot11g-radio-profile. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-227458	—	Some managed devices running AOS-W 8.6.0.10 or later versions log multiple **DHCP-RELAY** and **Cannot find Probe** syslog messages.	AOS-W 8.6.0.10
AOS-227809	—	The process monitor options could not be disabled on the controllers running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14
AOS-228356	—	The **detect-wireless-hosted-network** and **protect-wireless-hosted-network** parameters of the **ids unauthorized-device-profile** command does not work as expected in stand-alone controllers running AOS-W 8.6.0.13 or later versions.	AOS-W 8.6.0.13
AOS-228502	—	A managed device in a cluster was unable to pass through manual SNMP Walk performed on Linux / OmniVista 3600 Air Manager server. This issue is observed in managed devices running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-228799 AOS-238163	—	Some managed devices running AOS-W 8.6.0.16 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Datapath timeout (Fpapps Initiated).**	AOS-W 8.6.0.16
AOS-229474 AOS-229582 AOS-229990	—	The show ap database flags command does not filter the output based on the specified flags. This issue is observed in Mobility Master running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-229948 AOS-226909 AOS-230436 AOS-231548 AOS-232192	—	The **Configuration** > **Access Points** page of the WebUI does not display the list of available APs. Also, the number of available APs differs between the WebUI and CLI. This issue is observed in Mobility Master running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-230475 AOS-231207	—	API enforcement issues are observed when DPI and WebCC rules coexist. This issue is observed in managed devices running AOS-W 8.6.0.13 or later versions.	AOS-W 8.6.0.13

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-230508	—	A few APs crash and reboot unexpectedly. The log files list the reason for the event as **kernel page fault at virtual address 00000000, epc == 8017d554, ra == c005e32c**. This issue is observed in APs running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-232096	—	S-AAC controllers leak data traffic of wireless clients that are connected in split-tunnel forwarding mode. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-232475	—	Neither the **no time-range** command nor the **Configuration** > **Roles and Policies** > **<role>** > **Time Range** field of the WebUI allows users to delete the configured time range. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-233809	—	Users are unable to add GRE tunnels to a tunnel group and an incorrect error message, **Error: Tunnel is already part of a different tunnel-group** is displayed. This issue is observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-236721	—	The **Configuration** > **Roles & Policies** > **Roles** page of the WebUI does not display ACLs configured for the role. However, the CLI displays the list of ACLs. This issue is observed in Mobility Conductors running AOS-W 8.6.0.16 or later versions.	AOS-W 8.6.0.16
AOS-236889 AOS-243540	—	Some managed devices running AOS-W 8.5.0.13 or later versions are unable to fetch user information through controller API calls. The **show user** command output often states: **This operation can take a while depending on number of users. Please be patient**, with no following response.	AOS-W 8.5.0.13
AOS-238407	—	AppRF application or application category ACL is not blocking YouTube on devices connected to APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-239521	—	Users are unable to add a tunnel to a tunnel group and an error message was displayed: **Error: All tunnels must have same vlan membership.** This issue occurs when the VLANs are configured in a different order when compared to the order configured for other tunnels the same group. This issue is observed in managed devices running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-239814 AOS-239815	—	In some controllers running AOS-W 8.6.0.11 or later versions, IPv4 and IPv6 Accounting Messages are using the same session ID with Passpoint. This causes multiple accounting messages to be sent repeatedly.	AOS-W 8.6.0.11

Table 7: *Known Issues in AOS-W 8.6.0.22*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-243266	—	APs upgraded through TFTP get stuck in Upgrading status due to an incorrect automatic change of UDP ports. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.20 or later versions.	AOS-W 8.6.0.20
AOS-244659	—	Some clients are experiencing unexpected issues while roaming when using OpenFlow protocol. This issue is observed in OmniAccess Mobility Controllers running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-245191	—	Some Mobility Masters are unable to establish an SSH connection to the managed devices due to loginsessions not timing out. This issue is observed in managed devices running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18

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

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

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 in a topology where the managed devices are running the same version as the Mobility Master, or two versions lower. 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 8.5.0.0, AOS-W 8.4.0.0, or AOS-W 8.3.0.0.

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 the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:

  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 34 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 34 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 34 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 34.

> 📝 **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 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 34 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 34.

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.