AOS-W 8.6.0.20 Release Notes

Copyright Information

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

Chapter 1
Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 2
Release Overview

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:

- 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

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.

Enhancement to the wlsxWlanStationTable MIB

Starting from AOS-W 8.6.0.20, a new MIB object, **wlanStaApName,** is added to the **wlsxWlanStationTable** MIB to simplify the correlation of APs and stations.

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 8.6.0.20.

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 8.6.0.20*

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 8.6.0.20*

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 8.6.0.20*

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105

Table 5: *Supported AP Platforms in AOS-W 8.6.0.20*

AP Family	AP Model
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

Table 5: *Supported AP Platforms in AOS-W 8.6.0.20*

AP Family	AP Model
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 5
Regulatory Updates in AOS-W 8.6.0.20

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_85589

Chapter 6
Resolved Issues in AOS-W 8.6.0.20

The following issues are resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.6.0.20*

New Bug ID	Description	Reported Version
AOS-207080 AOS-236501	The output of the **show ap active** and **show ap bss-table** commands incorrectly displayed the radio type as high efficiency enabled for non-802.1X APs. This issue occurred when, ■ clients were connected in bridge mode ■ the managed devices act as User Anchor Controllers (UAC) The fix ensures that the commands display the correct radio type for non-802.1X APs. This issue was observed in managed devices AOS-W 8.6.0.4 or later versions in a cluster setup.	AOS-W 8.6.0.4
AOS-209093 AOS-210452 AOS-228137 AOS-237034	Some managed devices running AOS-W 8.6.0.18 or later versions generated multiple AMON receiver errors. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.18
AOS-214203 AOS-238450	Some OAW-AP515 access points running AOS-W 8.6.1.7 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **BadAddr:68637469777348 PC:asap_get_acl_name+0x28/0x1c0 [asap_mod] Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.17
AOS-214531 AOS-233154	The output of the **show ap bss-table** command displayed an incorrect channel, -36. This issue occurred after multiple channel changes on cluster comprised of 3 or more managed devices. The fix ensures that the **show ap bss-table** displays the correct channels. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions in a cluster setup.	AOS-W 8.7.1.8
AOS-214944	The **profmgr** process crashed on Mobility Masters running AOS-W 8.6.0.7 or later versions. This issue occurred while deleting the roles configured for AirGroup. The fix ensures that the Mobility Masters works as expected.	AOS-W 8.6.0.7
AOS-216942 AOS-237622 AOS-237621	Some OAW-AP535 access points running AOS-W 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.10
AOS-219192 AOS-223549 AOS-237599	The **Dashboard > Overview > Wireless Clients** page of the WebUI did not display any information and the error message, **Error retrieving information Please try again later** was displayed. The fix ensures that the WebUI displays the information about clients. This issue was observed in Mobility Masters running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-223221 AOS-237950	Some OAW-AP514 and OAW-AP515 access points running AOS-W 8.6.0.0 or later versions generated the error logs, **CPU: 1 PID: 1979 at ../../../../soft-ap/broadcom/esdk6/main/src/wl/../../src/wl/sys/wlc.c:22608 wlc_calc_frame_time+0x12c/0x410 [wl_v6]().** The fix ensures that the APs work as expected.	AOS-W 8.7.1.4

Table 6: *Resolved Issues in AOS-W 8.6.0.20*

New Bug ID	Description	Reported Version
AOS-226773	The MAC ACLs did not work as expected when OpenFlow was enabled. The fix ensures that the MAC ACLs work as expected. This issue was observed in managed devices running AOS-W 8.6.0.11 or later versions in a cluster setup.	AOS-W 8.6.0.11
AOS-227306	Some managed devices responded to the ARP probe frames with the SRC MAC address of the clients that were not connected to the network. The fix ensures that only intended managed devices respond to the ARP probe frames with the SRC MAC address of the clients. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.5
AOS-229207 AOS-229888	Users observed a discrepancy between the client count displayed in the WebUI of a Mobility Master and the CLI of a managed device. This issue occurred because the WebUI of the Mobility Master reported the client count, including the client entries that were retained to accommodate temporary client disconnections. The fix ensures that the WebUI and CLI display correct number of clients. This issue was observed in Mobility Masters running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-230044 AOS-238628 AOS-234556	Some AP-505H access points crashed and rebooted unexpectedly. The log files listed the reason for reboot as: **Kernel panic - not syncing: Fatal exception**. The fix ensures that the APs work as expected. This issue was observed in AP-505H access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-230798 AOS-231576	The output of the **show global-user-table list** command displayed duplicate user entries for bridge-mode SSIDs. The fix ensures that the command does not display the duplicate entries. This issue was observed in Mobility Masters running AOS-W 8.7.1.8 or later versions.	AOS-W 8.7.1.8
AOS-231206 AOS-239396	The **wpa3_sae** process crashed or was stuck in the **PROCESS_NOT_ RESPONDING_CRITICAL** state. This issue occurred due to timer corruption. The fix ensures that the managed devices work 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-231856	A few APs running AOS-W 8.6.0.0 or later versions crashed unexpectedly. The log files listed the reason for the event as **An internal system error has occurred at file sapd_sysctl.c function sapd_sysctl_write_param line 184 error Error writing /proc/net/wifi0/max_eirp_per_chan : Invalid argument**. This issue occurred due to a change of channel on one or both the radios when EIRP check was done for the new channel. The fix ensures that the EIRP request is processed and no error logs are generated.	AOS-W 8.7.1.8
AOS-232124	High CPU utilization was observed in the **stm** process when client devices utilized TSPEC signaling. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.0 or later versions.	AOS-W 8.8.0.3
AOS-232928	Some stand-alone switches running AOS-W 8.6.0.0 or later versions displayed the error messages, **KASan: use after free in wlc_pcb_fn_find+0xc8/0x160 [wl_v6] at addr ffffffc034931b08** and **KASan: out of bounds access in wlc_pcb_fn_ find+0xc8/0x160 [wl_v6] at addr**. The fix ensures that the switches work as expected. Duplicates: AOS-233808, AOS-234781, and AOS-236854	AOS-W 8.7.1.9
AOS-234103	Some clients experienced downstream packet disruption. The fix ensures that the APs work as expected. This issue was observed in OAW-AP205 access points running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.17

Table 6: *Resolved Issues in AOS-W 8.6.0.20*

New Bug ID	Description	Reported Version
AOS-234265 AOS-232356	Enet port flapping was observed on a few APs that were connected to the Cisco 9300 switches. As a result, the APs rebooted and clients experienced connectivity issues. Enhancements to the wireless driver resolved the issue. This issue was observed in OAW-AP535 access points running AOS-W 8.6.0.14 or later versions.	AOS-W 8.6.0.14
AOS-234627	Some managed devices running AOS-W 8.6.0.17-FIPS or later versions crashed unexpectedly. This issue occurred after issuing the **aaa test-server** command for a Radsec server. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.17-FIPS
AOS-234647	The **stm** process crashed on Mobility Masters running AOS-W 8.6.0.0 or later versions. This issue occurred after a VRRP failover. The fix ensures that the Mobility Masters work as expected,	AOS-W 8.10.0.2
AOS-235401	Some managed devices running AOS-W 8.6.0.17 or later versions did not send the outer IPV6 address to OmniVista 3600 Air Manager. The fix ensures that the managed devices send the IPV6 address correctly.	AOS-W 8.6.0.17
AOS-235744 AOS-235752	Some managed devices were unable to receive any configuration from the Mobility Master. This issue occurred when changes to a few group names were not synchronized on the standby Mobility Master before a reboot. The fix ensures that the managed devices receive configurations from the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-235810	Configuration changes to the SAP MTU value was not displayed correctly. This issue occurred when the storage format of the MTU configuration was changed and when the file was not read correctly. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.9.0.2
AOS-235914 AOS-238305	Some mesh APs running AOS-W 8.6.0.0 or later versions dropped data packets. This issue occurred when MTU length was more than 1500 bytes. The fix ensures that the APs work as expected.	AOS-W 8.7.1.10
AOS-236242	The **apmove** command did not work as expected when the APs were connected to the backup LMS switches. The fix ensures that the users can issue the **apmove** command. This issue was observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.9
AOS-236881	After upgrading Mobility Masters to AOS-W 8.6.0.9 or later versions, the profile manager in the secondary Mobility Master stopped responding. This issue occurred when IPv6 mode was enabled in the secondary Mobility Master because of which it failed to download certificates from the primary Mobility Master. The fix ensures that the secondary Mobility Master works as expected when IPv6 mode is enabled.	AOS-W 8.6.0.9
AOS-236920	Users were unable to convert a few APs to OpenConfig. This issue occurred when the images on the SCP server were not provided with **Read** access. The fix ensures that the APs are converted to OpenConfig seamlessly. This issue was observed in APs running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-237052 AOS-208508	The HTTP traffic of some users was incorrectly redirected by the captive portal. This issue occurred when the ACL changes were not updated on the APs. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5

Table 6: *Resolved Issues in AOS-W 8.6.0.20*

New Bug ID	Description	Reported Version
AOS-237510	Some WPA3-SAE opmode clients were unable to download user roles from ClearPass Policy Manager after a successful MAC authentication. The log file listed the reason for the event as **Cannot be assigned downloadable role, role is in error state**. The fix ensures that the clients are able to download user roles from ClearPass Policy Manager. This issue was observed in managed devices running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-237897	The Webcc logs were stored in an invalid message format and as a result, the syslog server reported incorrect data. The fix ensures that the Webcc logs are logged in a valid message format. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.9
AOS-238147 AOS-239823	Some APs powered up using POE-AT incorrectly came up with **r** flag and were unable to broadcast SSIDs. The fix ensures that the APs work as expected and broadcast SSIDs. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.10
AOS-238410 AOS-238939 AOS-238564 AOS-238487	The **httpd** process crashed on Mobility Masters and managed devices running AOS-W 8.6.0.17 or later versions. This issue occurred when a specific type of cURL request was sent to the switches. The fix ensures that the managed devices and Mobility Masters work as expected.	AOS-W 8.10.0.3
AOS-238456 AOS-238906	Some stand-alone switches failed to perform IKE fragmentation for VIA clients. This issue occurred when VIA clients used EAP-MSCHAPv2 for authentication. The fix ensures that the switches perform IKE fragmentation for VIA clients. This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.11
AOS-238954	Clients that used machine and user authentication were unable to connect to SSIDs. This issue was observed when WPA3 encryption was used. The fix ensures seamless connectivity. This issue was observed in OAW-AP515 access points running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-238701 AOS-238934 AOS-239570	The **authmgr, httpd, fwvisibility, ctamon**, and **ucm** processes were stuck in **NOT_RESPONDING** or I**NITIALIZING** state. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.6.0.19 or later versions in a cluster setup.	AOS-W 8.6.0.19

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

Limitation

Following are the limitations observed in this release:

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 8.6.0.20*

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
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

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
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 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 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-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: 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-W 8.4.0.0
AOS-190621	–	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-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. **Duplicates:** AOS-188255, AOS-190476, AOS-190946, AOS-193586, AOS-194784, AOS-196004, AOS-200375, and AOS-210787	AOS-W 8.3.0.8
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

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
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	–	The number of APs that are DOWN are incorrectly displayed in the **Dashboard > Overview** page of the WebUI. However, the CLI displays the correct number of APs. This issue is observed in Mobility Masters running AOS-W 8.4.0.4 or later versions. **Duplicates**: AOS-198565, AOS-200262, AOS-204794, AOS-212249, AOS-208110, AOS-209989, and AOS-212249	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-193883 AOS-197756	–	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-194080	–	Some switches 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 switches running AOS-W 8.2.2.10 or later versions.	AOS-W 8.2.2.10
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

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
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 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 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-196864	–	Although a new VLAN ID is successfully connected, the managed device displays 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 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:** Perform one of the following steps to resolve the issue: ■ 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.	AOS-W 8.5.0.4

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
		■ 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-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
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-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 an 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 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-200515 AOS-219987	–	The **DDS** process crashes on managed devices running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-200733	–	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, **<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.**	AOS-W 8.3.0.7

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
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-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 switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-202426 AOS-203652	–	Some 510 Series access points running AOS-W 8.6.0.4 crash and reboot unexpectedly. The log files list 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-202552 AOS-203990	–	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
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 EIRP value configured using the WebUI is not visible in stand-alone switches 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-203682	–	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

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
		Duplicates: AOS-195432, AOS-195433, AOS-218290, and AOS-220829	
AOS-204414	–	The VLAN range configured using the **ntp-standalone 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-standalone vlan-range.**	AOS-W 8.3.0.8
AOS-205319 AOS-206993 AOS-216577 AOS-218524	–	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-W 8.6.0.5
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
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 OAW-4450 switches 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-206902 AOS-208241	–	AirGroup users are unable to connect to Sonos speakers. This issue is observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-207006 AOS-215138	–	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-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

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
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.	AOS-W 8.3.0.13
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
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-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

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212772 AOS-221882	–	Some IPv6 clients are unable to access websites that have only IPv4 addresses. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
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 stand-alone 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	–	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 8.7.1.7
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 8.5.0.12
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-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 running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.3
AOS-224463	–	The RADIUS Radsec server does not work with TPM certificates on Mobility Masters running AOS-W 8.6.0.0-FIPS or later versions.	AOS-W 8.6.0.0-FIPS
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

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
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-226017 AOS-231886 AOS-235947	–	The **airmatch_recv** process crashes on Mobility Masters running AOS-W 8.6.0.9 or later versions. The log files list the reason for the event as **Exceeded max number of packet limit**.	AOS-W 8.6.0.9
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
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-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 switches 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 switches running AOS-W 8.6.0.13 or later versions.	AOS-W 8.6.0.13
AOS-229190 AOS-229798 AOS-230295	–	The **Dashboard** > **Overview** > **Clients** page of the WebUI does not display active and standby switch information. This issue is observed in Mobility Masters running AOS-W 8.10.0.0 or later versions.	AOS-W 8.10.0.0
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-228996	–	The **AMON-sender** process crash on managed devices unexpectedly. This issue is observed in OAW-4750XM controllers running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
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 Masters running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
AOS-229948	–	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 Masters running AOS-W 8.6.0.9 or later versions. Duplicates: AOS-226909, AOS-230436, AOS-231548, AOS-232192	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
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-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-234315	–	A few APs send PAPI messages to external IP addresses, and the log displays a random IP address for the **PAPI_Send failed** error message. This issue is observed in APs running AOS-W 8.6.0.15 or later versions.	AOS-W 8.6.0.15
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-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-237815	–	Mobility Masters running AOS-W 8.6.0.19 do not have sufficient free flash space. This issue occurs when the AP image files take up excessive flash space. **Workaround:** ▪ For Mobility Masters running AOS-W 8.6.0.17 and earlier versions, login to the switch console and remove the AP images that start with the letter **N** in	AOS-W 8.6.0.19

Table 7: *Known Issues in AOS-W 8.6.0.20*

New Bug ID	Old Bug ID	Description	Reported Version
		the folder, **/flash/img'x'/mswitch/sap**. ■ For Mobility Masters running AOS-W 8.6.0.17 and later versions, issue the **dir flash** command to get the list of large files in the /flash directory. And then, issue the **delete filename** command to remove files from the **/flash/apimages** directory.	
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-239498	–	Some OAW-AP515 access points running AOS-W 8.6.0.19 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **AP Reboot reason: BadPtr:0000000f PC:wlc_get_txh_info+0x118/0x210 [wl_v6] Warm-reset**.	AOS-W 8.6.0.19
AOS-239260	–	Some OAW-AP505 access points running AOS-W 8.6.0.18 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **BadPtr:00000294 PC:tun_recv_esp2_prep+0x10c/0x15c Warm-reset**.	AOS-W 8.6.0.18
AOS-238836	–	Clients that use machine and user authentication are unable to connect to SSIDs. This issue is observed when WPA3 encryption is used. This issue is observed in APs running AOS-W 8.6.0.18 or later versions.	AOS-W 8.6.0.18
AOS-201857 AOS-239541	–	The **stm** process crashes on OAW-AP115 access points running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3

Chapter 8
Upgrade Procedure

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 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 29 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 29 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 29 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 28.

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.

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

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

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

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

In the CLI

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

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

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

or

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

or

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

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

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Master.

```
(host)#reload
```

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

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

Verifying the AOS-W Upgrade

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

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 29 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 29 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 29.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

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

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

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

d. Click **Upgrade**.

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

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

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

In the CLI

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

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

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

or

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

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

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

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

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

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

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

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