AOS-W 8.7.1.0

Alcatel·Lucent
Enterprise

Release Notes

Contents

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE 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 HPE culture and moving forward, Aruba 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

Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release:

Table 1: *Revision History*

Revision	Change Description
Revision 04	Moved AOS-187448 from the **Known Issues** table to the **Limitations** section.
Revision 03	Added AOS-187448 as a known issue.
Revision 02	Removed AOS-207017 bug from the **Resolved Issues** section.
Revision 01	Initial release.

This AOS-W release notes includes the following topics:

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

For a list of terms, refer to the 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

Contacting Support

Table 2: *Contact Information*

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

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

Hardware Platforms

OAW-AP500H Series Access Points

The Alcatel-Lucent OAW-AP500H Series access points (OAW-AP503H and OAW-AP505H) are high-performance, multi-radio wireless devices that can be deployed in either controller-based (AOS-W) or controller-less (Aruba Instant) modes in hospitality and branch or teleworker deployments.

These hospitality access points support the full 802.11ax (Wi-Fi 6) feature set with dual 2x2 MIMO radios while also supporting 802.11a, 802.11n, and 802.11ac wireless services for 5 GHz and, 802.11b, 802.11g, 802.11n for 2.4 GHz.

Listed below are features of the Aruba 500H Series access points:

- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards.
- One uplink Ethernet port capable of data rates up to 2.5 Gbps.
- Integrated BLE and Zigbee radios.
- Green AP mode.
- Mesh.
- Location beacon applications.
- IoT gateway applications.

The OAW-AP505H access point was released in AOS-W 8.7.0.0.

OAW-AP503H Access Points - Mid-range dual radio Wi-Fi 6 Hospitality APs with the following additional features:

- One uplink Ethernet port capable of data rates up to 1Gbps.
- Two downlink Ethernet ports capable of data rates up to 1 Gbps.
- 5-pin Micro-B connector as console port.

For complete technical details and installation instructions, see *Alcatel-Lucent OAW-AP503H Access Point Installation Guide*.

OAW-AP560 Series Access Points

The Alcatel-Lucent OAW-AP560 Series access points (OAW-AP565 and OAW-AP567) are entry level Wi-Fi 6 (802.11ax) AP series designed to optimize user experience by maximizing Wi-Fi efficiency and reducing airtime contention between clients using Orthogonal frequency-division multiple access (OFDMA), bi-directional multi-user MIMO, and cellular optimization for outdoor and warehouse environments.

The Alcatel-Lucent OAW-AP560 Series access points delivers high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with 2x2 MU-MIMO radios, and supports 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Additional features include:

- Compatible with IEEE 802.3bt, IEEE 802.3at, IEEE 802.3af, IEEE 802.3az PoE standards.
- Integrated BLE and Zigbee radios.
- USB-C console interface.
- Mesh.
- Zero Touch Provisioning through Alcatel-Lucent Central or AirWave.
- Intelligent Power Monitoring (IPM).
- Alcatel-Lucent Advanced Cellular Coexistence (ACC).
- Alcatel-Lucent Air Slice for Extended OFDMA Assurance.

For complete technical details and installation instructions, see *Alcatel-Lucent* OAW-AP560 Series *Access Point Installation Guide*.

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 8.7.1.0*

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 8.7.1.0*

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, OAW-4112
MC-VA-xxx Virtual OmniAccess Mobility Controllers	MC-VA-10, 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 8.7.1.0*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
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-AP303H Series	OAW-AP303H, OAW-AP303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP318
OAW-AP320 Series	OAW-AP324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345

Table 5: *Supported AP Platforms in AOS-W 8.7.1.0*

AP Family	AP Model
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP370EX Series	OAW-AP375EX, OAW-AP377EX
OAW-AP387	OAW-AP387
OAW-AP500 Series	OAW-AP504, OAW-AP505
OAW-AP500H Series	OAW-AP503H, OAW-AP505H
510 Series	OAW-AP514, OAW-AP515, OAW-AP518
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577

Deprecated APs

The following APs are no longer supported from AOS-W 8.7.1.0 onwards:

Table 6: *Deprecated AP Models*

Access Points Series	Model Numbers
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

Table 6: *Deprecated AP Models*

Access Points Series	Model Numbers
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

Chapter 4
Regulatory Updates

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_77091

The following issues are resolved in this release.

Table 7: *Resolved Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-191031	—	A few 802.11ax clients experienced poor MU-MIMO performance. The fix ensures that the access points work as expected. This issue was observed in OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-195350	—	An AP rebooted caused by error **PC is at __qdf_bug+0x0/0x8 [qdf]**. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-198044	—	Mesh portals and mesh points are redirected to different MDs in a cluster environment, but the **show ap mesh topology** result did not include full information of all mesh nodes under a specific mesh tree. The fix ensures that the mesh information is synchronized between MDs to make the show result complete. This issue was observed in switches running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-198785	—	A switch rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:40:2)**. The fix ensures that the switch works as expected. This issue was observed in OAW-4750XMswitches running AOS-W 8.3.0.10.	AOS-W 8.3.0.10
AOS-200801	—	A RAP denied client traffic connected to bridge mode SSID. This issue occurred due to an incorrect **variable: ace index**. The fix ensures that the controllers work as expected. This issue was observed in OAW-4550switches running AOS-W 6.5.4.12 or later versions.	AOS-W 6.5.4.12

Table 7: *Resolved Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201519	—	An OAW-AP325 crashed and rebooted with reason **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the access points work as expected. The issue was observed in OAW-AP325 access points running AOS-W 8.6.0.0 or later versions	AOS-W 8.6.0.0
AOS-202274	—	A OAW-4650switch crashed four times on Trap. This issue occurred due to received snmp v3 packets not getting allocated. The fix ensures that snmp v3 packets are allocated as expected. This issue was observed in OAW-4650switches running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-202416	—	A broadcast loop occurred when Apple devices sent a GARP reply. However, ARP requests or other frames did not cause a broadcast loop. This was due to standby tunnels sending and receiving data. The fix ensures that the controllers work as expected. This issue occurred in switches running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-203743	—	DPI classification did not occur with custom-app on HTTP referer-param. The fix ensures that DPI classification works as expected. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-204385	—	Incorrect position of access policies were observed in the **Configuration > Roles & Policies > Policies** page of the WebUI as well as from the CLI. The fix ensures that the access policies are positioned correctly. This issue was observed in stand-alone controllers running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-204545 AOS-208184 AOS-208757 AOS-209190	—	Few OAW-4750XM switches running AOS-W 8.5.0.8 or later versions crashed unexpectedly. The log file listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:f0:2)**. The fix ensures that the OAW-4750XM switches work as expected.	AOS-W 8.5.0.8
AOS-204780	—	A managed device generated valid client misassociation logs. This issue occurred when a valid client connected to a valid SSID. This issue is resolved by checking if a valid client is misassociated to a monitored AP and checking if the monitored AP is not valid. This issue was observed in managed devices running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-204797	—	A Nova Biomedical StatStrip Glucose Meter could not associate to an OAW-AP303H access point but is able to associate to an OAW-AP535 access point. The fix ensures that the auth response from the access point is sent with a closed algorithm. This issue was observed in an OAW-AP303H access point running AOS-W 8.6.0.4.	AOS-W 8.6.0.4

Table 7: *Resolved Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205189 AOS-205996 AOS-207870	—	A user experienced network latency. This issue occurred due to high CPU utilization in a managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-205326	—	A few 802.11ax clients were stalled during a throughput test. This issue occurred when 20 clients with MU-MIMO and OFDMA enabled, were connected to APs. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-205344	—	A few clients experienced slow connection speed when they connected to APs using mobile devices operating under legacy regulatory rules. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.6.0.4
AOS-205666	—	Performance degradation was observed in OAW-AP535 access points running AOS-W 8.7.0.0 when OFDMA was enabled in **wlan he-ssid-profile** command. Enhancements to the wireless driver resolved this issue.	AOS-W 8.7.0.0
AOS-205667	—	A wrong role was assigned to bridged mode wired port in initial role. This issue is resolved by changing the role name to be case insensitive. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-205684	—	The post authentication role for a bridge-Captive Portal client was carried forward from one VAP to another. This issue is resolved by resetting the role when the authenticated bridge-Captive Portal client switches ESSID. This issue occurred when an authenticated bridge-Captive Portal client switched to a different ESSID and the client kept the authenticated role from the bridge-Captive Portal. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-205783	—	Clients retained the post authentication role even after session-timeout expired. The fix ensures that the clients move to L2 role after session timeout. This issue occurred in bridge mode captive portal in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-205869	—	The **Invalid data: FW CP ACL not found** error message was displayed when the users configured and deleted firewall rules from managed devices using **firewall cp** command. The fix ensures that the error message is not displayed. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.3.0.12
AOS-206047	—	AirGroup cache entries were deleted from the Mobility Master running AOS-W 8.6.0.4 or later versions. This issue occurred when the maximum threshold limit was reached. The fix ensures that the AirGroup cache entries are not deleted.	AOS-W 8.6.0.3

Table 7: *Resolved Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206057	—	Poor performance was observed in OAW-AP535 access points running AOS-W 8.7.0.0 when the MU-MIMO was enabled. Enhancements to the wireless driver resolved this issue.	AOS-W 8.7.0.0
AOS-206071	—	The **Dashboard > Security > Bandwidth** page did not display information about the HT-type of the APs. The fix ensures that the WebUI displays information about the HT-type of the APs. This issue was observed in APs running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-206177	—	Users failed to timeout after an AP reboot and the user entries were retained in the user table although the clients were disconnected few days back. The fix ensures that the user entries are removed from the user table after the clients get disconnected. This issue occurred when the wireless clients were connected using bridge mode to managed devices running AOS-W 8.7.0.0 version.	AOS-W 8.7.0.0
AOS-206452	—	An unknown IP address was displayed in the **Standby Controller** field in the **Dashboard > Overview > Clients > Wireless Clients** page in the WebUI. The fix ensures that the unknown IP address is not displayed for the wireless clients. This issue occurred during the cluster live upgrade process on the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.6.0.2
AOS-206517	—	The captive portal user name changed after 802.1X reauthentication. The fix ensures that the user name does not change after 802.1X reauthentication. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-206629 AOS-206636	—	L2TP VPN connection failed on Mac, IOS, and android clients connected to a managed device. The fix ensures that the managed device works as expected. This issue occurred when: ■ clients initiated L2TP connection on random src port instead of the standard src port, 1701. ■ clients connected behind a NAT device. This issue was observed in managed devices running AOS-W 8.4.0.6 or later versions.	AOS-W 8.4.0.6
AOS-206689	—	A few users were unable to add username containing a period (.) while configuring client entries in the internal database. The fix ensures that both **.** and **@** characters are allowed in the user name. This issue was observed in stand-alone switches running AOS-W 8.3.0.0 or later versions.	AOS-W 8.6.0.4
AOS-206878	—	The Fing mobile application discovered two connected clients and was unable to isolate them, although deny-inter-user-traffic and deny-inter-user-bridging were enabled. This issue is resolved by configuring deny-inter-user-traffic or deny-inter-user-bridging globally on the firewall, irrespective of VLAN BCMC. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206998 AOS-208353	—	A few APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **NOC_ error.c:473 NOCError: FATAL ERRORparam0 :zero, param1 :zero, param2 :zero**. Enhancements to the wireless driver resolved the issue. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.2
AOS-207007	—	Clients were unable to connect to few APs intermittently. Enhancements to the wireless driver resolved this issue. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-207053	—	A few incorrect MAC addresses in the same subnet were listed in the mesh portal. The fix ensures that the wrong entries of the mesh portal are removed from the mesh link table. This issue was observed in APs running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.7
AOS-207073	—	An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Fatal exception in interrupt: PC is at dma_cache_maint_page+0x64/0x160, LR is at __dma_page_dev_to_ cpu+0x2c/0xe4**. Enhancements to the wireless driver resolved this issue. THis issue was observed in OAW-AP305 access points running AOS-W 8.3.0.0.	AOS-W 8.3.0.0
AOS-207337	—	A managed device was stuck at **LAST SNAPSHOT (Master Unreachable)** state although the IPsec tunnel was established with the Mobility Master. The fix ensures that the managed device successfully terminates on the Mobility Master. This issue occurred because the route-cache table had wrong tunnel IDs. This issue was observed in managed devices running AOS-W 8.3.0.0-FIPS or later versions.	AOS-W 8.5.0.9
AOS-207366	—	AP provisioning parameters did not show advanced options when more than one access point was chosen. The fix ensures that advanced options are displayed when more than one access point is chosen. This issue occurred in switches running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-207416	—	The output of the **show whitelist-db rap** and **show ap database long** commands displayed the status of the OAW-RAP as **Provisioned** and **R-c2** respectively, although the OAW-RAP was authenticated using the AP authorization profile. The fix ensures that the OAW-RAP is authenticated in whitelist database and the AP moves to **Rc2** authenticated state. This issue was observed in OAW-RAPs connected to stand-alone switches running AOS-W 8.3.0.0 or later versions.	AOS-W 8.5.0.8
AOS-207439	—	The output of the **show firewall-cp** command displayed negative values. The fix ensures that the output of the command does not display any negative value. This issue was observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6

Table 7: *Resolved Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207552	—	A mismatch of MTU value was observed between the AP and the switch. The fix ensures that the MTU value is consistent across the AP and the switch. This issue occurred when the AP was rebooted after setting the default value of the **rap-gre-mtu** parameter. This issue was observed in APs connected to stand-alone switches running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-207659	—	The **profmgr** process in a managed device crashed and the managed device rebooted unexpectedly. Enhancements to memory management resolved this issue. This issue was observed in managed devices running AOS-W 8.6.0.4.	AOS-W 8.6.0.4
AOS-207787	—	The logging level of the **mini_httpd[4602]: bind 0.0.0.0 - Address already in use** l log has been changed from critical to informational.	AOS-W 8.7.0.0
AOS-207791	—	The **udbserver** process in a managed device crashed and the managed device rebooted unexpectedly. The fix ensures that managed device works as expected. This issue was observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-207893	—	Clients were unable to receive IP addresses. This issue occurred due to high memory utilization in APs caused by the BLE daemon process. The fix ensures that memory utilization in APs is regulated by the creation of a new boot log file at every restart instance of the BLE daemon process. This issue was observed in APs running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-208438	—	Captive portal failed in bridge forwarding mode APs running AOS-W 8.7.0.0. This issue occurred due to an empty AP netdestination list. The fix ensures that captive portal works as expected in bridge forwarding mode APs.	AOS-W 8.7.0.0
AOS-208483	—	Users failed to timeout after an AP reboot and the user entries were retained in the user table although the clients were disconnected few days back. The fix ensures that the user entries are removed from the user table after the clients get disconnected. This issue occurred when the wireless clients connected using bridge mode switched to a VAP terminated on another managed device deployed in a different cluster. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0

Table 7: *Resolved Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208553	—	The **Test** button, in the **Mobility Master > Diagnostics > Tools > AAA Server Test > Test** page of the WebUI, for the AAA server was greyed out for read-only users. The fix ensures that the **Test** button is available for read-only users. This issue was observed in Mobility Masters running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-208557	—	OAW-AP535 access points running AOS-W 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **reboot reason: due to Assertion failed**. Enhancements to the wireless driver fixed the issue.	AOS-W 8.6.0.4
AOS-208987	—	Clients stayed in post auth role in the bridged captive portal even after session timeout. This issue occurred when the clients were authenticated or deauthenticated before timeout. The fix ensures that the clients are not stuck in the post auth role. This issue was observed in managed devices running AOS-W 8.7.0.0.	AOS-W 8.7.0.0

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

Limitation

Following is the limitation 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.

Known Issues

Following are the known issues observed in this release:

Table 8: *Known Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207634	—	The **show ap allowed-channels** command displays the error **No valid country code is set** and does not show any broadcasting SSIDs. This is observed when using the U.S. country code in access points running AOS-W 8.7.1.0	AOS-W8.7.1.0
AOS-207689	—	A continuous error message **wl0: PHYTX error txerr mac 0200 phy b000 0000 0000 tst ffff** is observed with traffic in access points running AOS-W 8.7.1.0	AOS-W 8.7.1.0
AOS-207881	—	The Downlink Ethernet LED indicator is seen even after disconnecting the Downlink Ethernet cable. It is observed in OAW-AP500H Series access points running AOS-W 8.7.1.0 version	AOS-W 8.7.1.0
AOS-208004	—	Performing a Ping Traffic to associated clients across VAPs resulted in several clients reconnecting frequently with various deauth reasons. This issue is observed in access points running AOS-W 8.7.1.0	AOS-W 8.7.1.0

Table 8: *Known Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208029	—	OTA captures show that an ADDBA Response from an AP to a client is missing **BlockAck Param Set**. However, the **BlockAck Param Set** is present when the same ADDBA response is sent from a client to an AP. This issue is observed in OAW-4024 switches running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-208039	—	APs did not send CSA information on the beacon packet. This issue occurs when a fake radar is detected on the DFS channel. This issue is observed in AP-565 and AP-505 access points running AOS-W 8.7.1.0 version.	AOS-W 8.7.1.0
AOS-208176	—	AP is sending first action frame as unencrypted frames after a successful 4-way handshake. This issue occurs when SAE transition mode is enabled. This issue is observed in AP-503H access points running AOS-W 8.7.1.0 version.	AOS-W 8.7.1.0
AOS-208259	—	The LED on the AP-565 does not turn off LED even after 1200 seconds. This issue is observed in AP-565 access points running AOS-W 8.7.1.0 version.	AOS-W 8.7.1.0
AOS-208279	—	Unusual errors like, **<isakmpd 103061> <3413> <ERRS> |ike| 172.30.1.186:4500-> InKe DH Group from KE hdr 2. Expecting DH group 14** are displayed in the log files. This issue is observed in access points running AOS-W 8.7.1.0 version.	AOS-W 8.7.1.0
AOS-208320	—	APs display both green and red LED for a short duration in the initial power-up condition. This issue is observed in 505H series access points running AOS-W 8.7.1.0 version.	AOS-W 8.7.1.0
AOS-208374	—	The output of the **show ap debug airmatch reporting-radio ap-name <ap-name>** and **show airmatch debug reporting-radio ap-name <ap-name>** commands do not display the updated values for **Channel Reason** and **Channel Update Time** parameters when static config, in the form of freeze commands, is applied to one or more radios on the AP. This issue is observed in OAW-AP503H access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-208379	—	An AP running AOS-W 8.7.1.0 reboots unexpectedly. The log file lists the reason for the event as **External-WDT-reset**.	AOS-W 8.7.1.0
AOS-208419	—	The output of the **show ap debug ble-config ap-name <ap-name>** command does not display the AP console in OAW-AP503H and OAW-AP565 access points running AOS-W 8.7.1.0. This issue is observed when BLE console mode is enabled using the **iot radio-profile <profile-name> ble-console** command.	AOS-W 8.7.1.0
AOS-208640		A few High Efficiency clients experience poor performance with OAW-AP505 access points running AOS-W 8.7.1.0. This issue occurs when **HE MU-OFDMA** and **HE MU-MIMO** parameters are enabled.	AOS-W 8.7.1.0
AOS-208664	—	APs running AOS-W 8.7.1.0 display the error log **wl0.1: wlc_ap_sta_probe_complete: SCB_PS_PRETEND_ BLOCKED, expected to see PMQ PPS entry** during multicast video streaming.	AOS-W 8.7.1.0

Table 8: *Known Issues in AOS-W 8.7.1.0*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208745	—	APs display an incorrect CVv flag for clients connected to the AP. This issue is observed in APs running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-208763	—	PoE flaps constantly when AP is brought up using DC and PoE. This issue is observed in APs running AOS-W 8.7.1.0. **Workaround:** Do not enable PoE on the port that is connected to a DC powered AP.	AOS-W 8.7.1.0
AOS-208822	—	OAW-AP504, OAW-AP505, and OAW-AP503H access points running AOS-W 8.7.1.0 display incorrect LED pattern in deep sleep mode.	AOS-W 8.7.1.0
AOS-208838	—	Mesh points print kernel trace and reboot. This issue occurs when AP detects radar signal in DFS channels. This issue is observed in OAW-AP505 and OAW-AP565 access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-208855	—	Mesh Points in a three hops mesh topology are unable to connect to the parent node. This issue occurs when AP detects radar signal in DFS channels. This issue is observed in OAW-AP505 and OAW-AP565 access points running AOS-W 8.7.1.0	AOS-W 8.7.1.0
AOS-208864	—	An AP does not have a channel char in the output of the **show ap mesh active table** and **show ap active when del all license** commands. This issue is observed in OAW-AP567 access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-208969	—	The radio in an AP resets with the **wl1: fatal error, reinitializing- wlc_key_rx_mpdu(645): Resetting radio wl1 consecutive 40 ICV errors** message. This issue is observed in OAW-AP503H access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-209002	—	An AP denies association response during client reconnect with the **RC: Denied; MFP - Try Later** message. This issue is observed in OAW-AP503H access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-209508	—	The 2.4 GHz band 40 MHz static channel assignment in an AP is incorrect. This issue is observed in OAW-AP560 Series access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-210143	—	The PoE current value that is marked on an AP enclosure is not consistent with the data sheet of the AP. This issue was observed in access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0
AOS-210144	—	The DC current value that is marked on an AP enclosure is not consistent with the data sheet of the AP. This issue is observed in access points running AOS-W 8.7.1.0.	AOS-W 8.7.1.0

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, master switch, or stand-alone switch.

Topics in this chapter include:

Important Points to Remember

To upgrade your managed device or Mobility Master:

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

- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Master Licensing Guide.*
- Multiversion is supported in a topology where the managed devices are running the same software 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 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 28 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 28 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 28 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 27.

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.

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 28 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 28 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 28.
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
   ```

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.