AOS-W 8.7.1.3

Alcatel·Lucent
Enterprise

Release Notes

Contents

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 02	The bug, **AOS-214916** was moved to 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://businessportal.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

There are no new features or enhancements introduced in this release.

Support for Huawei E3372h-320 modem

Starting from AOS-W 8.7.1.3, users can issue the **uplink cellular profile e3372h-320** command to provision the Huawei E3372h-320 modem. It is recommended to issue the command, reload and then, insert the modem for a successful provisioning.

CLI

show datapath frame debug command

Starting from AOS-W 8.7.1.3, the output of the **show datapath frame debug** command has been modified to display **vlan bcmc drop frames** instead of **vlan bcmc check fails**.

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 8.7.1.3*

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

OmniAccess Mobility Controller Platforms

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

Table 4: *Supported OmniAccess Mobility Controller Platforms in AOS-W 8.7.1.3*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series Hardware OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series Hardware OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series Hardware OmniAccess Mobility Controllers	OAW-4104, 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 8.7.1.3*

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-AP303P
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
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377

Table 5: *Supported AP Platforms in AOS-W 8.7.1.3*

AP Family	AP Model
OAW-AP370EX Series	OAW-AP375EX, OAW-AP377EX, AP-375ATEX
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

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_79703

The following issues are resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-188972 AOS-194746 AOS-208631 AOS-209396 AOS-213627	—	A Mobility Master displayed blacklisted clients after removing them from the managed device in a cluster setup. The fix ensures that the Mobility Master displays the correct output. This issue was observed in Mobility Masters running AOS-W 8.4.0.4 or later versions.	AOS-W 8.4.0.4
AOS-196399	—	DDS traffic caused IP reassembly failures in datapath. The fix ensures that the Mobility Master works as expected. This issue is observed in Mobility Masters running AOS-W 8.3.0.6 or later versions.	AOS-W 8.3.0.6
AOS-197548 AOS-209545	—	MAC authentication was not initialized when IPv6 was globally disabled. The fix ensures that MAC authentication works as expected. This issue was observed in managed devices running AOS-W 8.3.0.13 or later versions.	AOS-W 8.3.0.13
AOS-201003 AOS-212135	—	Some OAW-RAPs were unable to come up in a cluster. The fix ensures that OAW-RAPs can come up in a cluster. This issue is observed in managed devices running AOS-W 8.0.2.0 or later versions.	AOS-W 8.0.2.0
AOS-203910 AOS-209692 AOS-204905	—	The stand-alone switches running AOS-W 8.6.0.3 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as, **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.3
AOS-203926	—	Voice traffic using NOE protocol was not getting tunneled in split-tunnel forwarding mode. This issue occurred when openflow is enabled. The fix ensures that the voice traffic using NOE protocol is tunneled. This issue was observed in managed devices running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-206213	—	The **show ap tech-support** command displayed multiple **<sapd 311020> <ERRS> Error opening /proc/sys/dev/wifi2** logs. The fix ensures that the command does not display multiple **<sapd 311020> <ERRS> Error opening /proc/sys/dev/wifi2 logs**. This issue was observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206355	—	The **LLDP** process crashed unexpectedly during Zero Touch Provisioning (ZTP) on a OmniAccess Mobility Controller. The fix ensures that the OmniAccess Mobility Controllers work as expected. This issue occurred due to memory corruption. This issue was observed in OmniAccess Mobility Controllers running AOS-W 8.2.2.6 and later versions.	AOS-W 8.2.2.6
AOS-206725	—	The **fpapps** process crashed and the switch rebooted unexpectedly. The fix ensures that the switch works as expected. This issue occurred when an external unsupported USB modem was configured on a stand-alone switch. This issue was observed on OAW-40xx Series switches running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-206801	—	A managed device running AOS-W 8.2.2.3 or later versions contacted the Activate server more than once during ZTP. The fix ensures that the managed device work as expected. This issue was observed in managed devices running AOS-W 8.2.2.3 or later versions.	AOS-W 8.2.2.3
AOS-206888	—	A few APs took up to 30 minutes to be operational and join the managed device, when they were provisioned for the first time in a native IPv6 deployment. This issue was observed in OAW-AP515 and OAW-AP555 access points running AOS-W 8.7.0.0 in a cluster setup. The fix ensures that APs work as expected.	AOS-W 8.7.0.0
AOS-207337	—	After upgrading from AOS-W 8.2.x.x to AOS-W 8.5.0.0- FIPS or later versions, a few managed devices were stuck in the **LAST SNAPSHOT** state. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.0
AOS-207664 AOS-213842	—	The login banner text was not displayed after upgrading the managed device to AOS-W 8.5.0.0 or later versions. The fix ensures that the login banner is displayed.	AOS-W 8.5.0.0
AOS-207701 AOS-218006	—	The RADIUS request packets did not have the state attribute value and hence, clients faced connectivity issue. This issue occurred due to a race condition. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.	AOS-W 8.4.0.0
AOS-207780	—	Some managed devices running AOS-W 8.5.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (sp_sbeth_poe_map_age).** The fix ensures that the managed devices work as expected. **Duplicates:** AOS-203049, AOS-208611, AOS-210394, AOS-212485, AOS-214564, AOS-214917, /AOS-215657	AOS-W 8.5.0.5
AOS-207795	—	Users were unable to access the WebUI of the Mobility Master. The fix ensures that users are able to access the WebUI. This issue was observed in Mobility Masters running AOS-W 8.2.2.6 or later versions.	AOS-W 8.2.2.6

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-208515	—	The radio usage graph in OmniVista 3600 Air Manager got reset to zero. This issue occurred while downloading large files. The fix ensures that the radio usage graph does not reset to zero. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-209069	—	The control plane security configuration, **auto-cert-allowed-addrs** pushed from a Mobility Master to the managed devices was not visible in the **Configuration > System > CPSec** page of the WebUI. The fix ensures that the control plane security configuration, **auto-cert-allowed-addrs** is visible in the WebUI. This issue is observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-209127	—	Internal server timeout was observed during an authentication request. The fix ensures successful authentication. This issue was observed in stand-alone switches with master-redundancy setup using VRRP environment, where the stand-alone switches were running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209196 AOS-213746	—	Some APs rebooted unexpectedly. The fix ensures that the APs work as expected. The issue occurred when tunnel forwarding modes, **dot11k**, and **WPA3** were enabled in AP. This issue was observed in OAW-AP345 access points running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-209323	—	The **Server Group Match Rules** option for **Internal** server in the **Authentication > Auth Servers** page of the WebUI was not available in Mobility Masters running AOS-W 8.7.0.0 or later versions. The fix ensures that WebUI displays the **Server Group Match Rules** option for **Internal** server.	AOS-W 8.7.0.0
AOS-209352	—	Some managed devices terminating VIA connection displayed the error message, **httpd[30106]: Reached session limit: 64**. The fix ensures that all VPNC and VIA sessions are considered during session count. This issue was observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-209402	—	A few clients experienced dot1x timeout in split tunnel mode. This issue occurred when multiple wired clients were connected to an AP. The fix ensures that the clients don't experience a timeout. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-209640	—	A few clients were unable to receive IP addresses from the VLAN configured on LLDP-MED network policy profile. The fix ensures that clients receive IP addresses. This issue was observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-209748 AOS-215172 AOS-217181	—	Some users were unable to make configuration changes to the existing RADIUS server profile at the device level. The log file listed the reason for the event as **Reference retrieval error**. The fix ensures that **profmgr** process does not get stuck if it's unable to retrieve a profile reference and the devices work as expected. This issue was observed in Mobility Master running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209783	—	After a reload of the Mobility Master, OAW-RAPs and VIA clients with ECDSA Suite B certificates overloaded the **ISAKMPD** process. As a result, the **ISAKMPD** process became unresponsive. The fix ensures that IKE exchanges are throttled at the beginning of the tunnel establishment and it is restricted only to a certain maximum number of exchanges at a time. This reduces the load on the **ISAKMPD** process. Issue the **show crypto-local isakmp max-allowed-negotiations** command to check the default maximum number of exchanges allowed at a time. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-210065 AOS-213825	—	A few users were unable to connect to an AP. The fix ensures seamless connectivity. This issue was observed in APs running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210122 AOS-215655	—	Clients were unable to receive the IP addresses from their respective VLANs. This issue occurred when clients were connected to a OAW-RAP. The fix ensures that clients receive IP addresses. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-210342	—	The VRRP authentication password was not encrypted in the output of the **show running config** command. The fix ensures that the password is encrypted. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-210404	—	The **Pending Changes** option did not appear in the WebUI. This issue occurred when there were too many unsaved nodes and the **show configuration unsaved-nodes** command had on output of more than 1024 characters. The fix ensures that the **Pending Changes** option appear in the WebUI. This issue was observed in Mobility Masters running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-210481	—	The **Dashboard > Infrastructure > Clusters** page of the WebUI did not list all the clusters. The fix ensures that the WebUI displays the list of all the clusters. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-210484	—	Some managed devices running AOS-W 8.0.0.0 or later versions do not display the 802.11k measurements from clients. The fix ensures that the managed devices display the 802.11k measurements from clients.	AOS-W 8.3.0.6
AOS-210896	—	Hotspot 2.0 IEs were not present in beacons frames. The fix ensures that the Hotspot 2.0 IEs are present in beacons frames. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-211256	—	The SFP J8177D, JD089B, and Cisco GLC-TE transceivers did not work with OAW-4450 switches running AOS-W 8.6.0.3. The fix ensures that the SFP J8177D, JD089B, and Cisco GLC-TE transceivers work with OAW-4450 switches.	AOS-W 8.6.0.3

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-211324	—	Some iPads were unable to connect to SSIDs. The log file listed the reason for the event as **STA Requesting Association without authentication**. The fix ensures seamless connectivity. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-211389	—	Users were unable to install evaluation licenses. This issue occurred when the Mobility Master displayed an expired installation date. The fix ensures that the users are able to install evaluation licenses. This issue was observed in Mobility Masters running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-211430	—	The WebUI did not display the list of APs and clients. This issue occurred when VRRP IPv4 / IPv6 dual stack was used to form an IPsec tunnel between the Mobility Master and managed device. The fix ensures that the WebUI displays the list of APs and clients. This issue was observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-211472	—	Captive portal failed to send mails to guest accounts. This issue occurred when the SMTP server failed to validate the host. The fix ensures that the captive portal works as expected. This issue was observed in stand-alone switches running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-211782	—	Users were unable to delete a policy assigned to a role and the error message, **No Changes Done** was displayed. The fix ensures that users are able to delete a policy assigned to a role. This issue was observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-211841	—	The **Dashboard > Infrastructure** page of the WebUI displayed the client status as **Unknown**. The fix ensures that the WebUI displays the correct status of clients. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-211878 AOS-214377	—	Some APs failed to come up as OAW-RAPs. This issue occurred when the MTU size was not adjusted automatically. The fix ensures that APs come up as OAW-RAPs. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212039	—	User debug logging information was not available in **Configuration > System > Logging > Logging Levels** page of the WebUI. The fix ensures that the WebUI displays the user debug logging information . This issue was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-212063 AOS-216153	—	Licenses got installed with incorrect dates in Mobility Masters running AOS-W 8.5.0.10 or later versions. The fix ensures that licenses are installed using correct dates.	AOS-W 8.5.0.10
AOS-212203 AOS-213878 AOS-213879 AOS-212560	—	Some users experienced poor network performance. This issue occurred due to 2.4G beacon power fluctuations in OAW-AP505 access points running AOS-W 8.6.0.5 or later versions. The fix ensures optimal network performance.	AOS-W 8.6.0.5

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212432 AOS-212634 AOS-212958	—	The **Datapath** process crashed on a stand-alone controller. This issue occurred in a cluster setup during a switchover. The fix ensures that the controller works as expected. . This issue was observed in OAW-4750XM controllers running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-212458 AOS-215059 AOS-215163	—	Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Take care of the TARGET ASSERT first at NOC_error**. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points and OAW-AP555 access points running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-212486 AOS-216471	—	L2TP IP address was observed and VLAN pool was exhausted. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-212530	—	Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as, **reboot Intermittently-suspecting scb or rrm cubby corruption.** This issue was observed in OAW-AP515 access points running AOS-W 8.5.0.10 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-212554	—	VIA connection failed and high **ISAKMP CPU** usage was observed. The fix ensures that the managed device works as expected. This issue was observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-212568	—	The **aaa / certmgr / cpsec** security categories in the **Configuration > System > Logging > Logging Levels** page of the WebUI displayed **None** even if values were configured. The fix ensures that the WebUI displays the correct **aaa / certmgr / cpsec** values. This issue was observed in Mobility Masters running all AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.13
AOS-212576	—	Some APs running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: rcu_sched detected stalls (pc is at __ schedule+0x78/0x360).** The fix ensures that the APs work as expected.	AOS-W 8.6.0.5
AOS-212599 AOS-211699 AOS-212564 AOS-212567 AOS-215978 AOS-217452	—	Some APs running AOS-W 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: jiffies stall (pc is at __ schedule+0x78/0x360).** The fix ensures that the APs work as expected.	AOS-W 8.6.0.5

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212656 AOS-212696 AOS-215107	—	The custom captive portal page did not load completely. This issue occurred when the **use http authentication option** was enabled. The fix ensures that the captive portal works as expected. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-212686	—	Some APs sent higher SAP MTU frames than the configured value. The fix ensures that APs work as expected. This issue was observed in APs running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-212707	—	Some Mobility Masters running AOS-W 8.5.0.10 logged the error message, **Fri Oct 16 23:58:53 2020, 0, 0, 0, 0, 0, 0, 0**. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.5.0.10
AOS-212843	—	Some users were randomly assigned the default role. This issue occurred when 802.11r feature was enabled. The fix ensures that users are not assigned incorrect roles. This issue was observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-212861 AOS-215350 AOS-215522 AOS-216305	—	Some OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first.** The fix ensures that the APs work as expected.	AOS-W 8.6.0.6
AOS-212885 AOS-214735	—	Some APs rebooted unexpectedly. The log file listed the reason for the event as, **BUG in aruba_wlc.c:4527/aruba_radio_update()**. This issue occurred after the APs were upgraded. The fix ensures that the AP works as expected. This issue was observed in OAW-AP345 access points running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-212980 AOS-217034 AOS-217127 AOS-218636	—	Some managed devices did not execute complete commands and displayed incorrect outputs. The fix ensures that the correct output is displayed for each command. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-213089	—	Some managed devices running AOS-W 8.3.0.0 or later versions crashed and rebooted 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 managed devices work as expected. **Duplicates:** AOS-213044, AOS-213295, AOS-214238, AOS-214431, AOS-214678, AOS-215123, AOS-215572, AOS-216951, AOS-217734	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213099	—	The **dpagent** process crashed on managed devices running AOS-W 8.5.0.10 or later versions. The fix ensures that the managed devices work as expected. **Duplicates:** AOS-214123, AOS-215367, AOS-216451, AOS-216612, AOS-217647, AOS-217960, AOS-217721, AOS-217942, AOS-217943, AOS-218204	AOS-W 8.5.0.10
AOS-213132 AOS-216300	—	Users were unable to upload server certificates in PEM or DER format. The fix ensures that users are able to upload server certificates. This issue is observed in Mobility Masters running AOS-W 8.6.0.6-FIPS.	AOS-W 8.6.0.6-FIPS
AOS-213242 AOS-215607 AOS-218659	—	Some APs did not connect to the network. The fix ensures that the APs work as expected. This issue occurred due to high noise level and channel utilization on the 2.4 GHz band. This issue was observed in OAW-AP535 access points and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-213305 AOS-213310	—	Some APs crashed and rebooted unexpectedly. The log file lists the reason for the event as **PC is at wlc_nar_dotxstatus+0x88/0x7d8: AOS-200674 instrumentation kicks in (wlc_nar_validate_cubby).** The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.7.0.0 or later versions	AOS-W 8.7.0.0
AOS-213308	—	Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **PC is at asap_ap_dev_xmit+0x118/0x4d0**. The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-213309	—	Some OAW-AP515 access points running AOS-W 8.7.0.0 or later versions crash and reboot unexpectedly. The log file listed the reason for the event as **PC is at wlc_ratesel_clr_cache+0x2c/0xa0.** The fix ensures that the APs work as expected.	AOS-W 8.7.0.0
AOS-213558	—	Users were unable to add a new node to an existing cluster of eight nodes. The fix ensures that users are able to add new nodes. This issue was observed in managed devices running AOS-W 8.5.0.6 or later versions.	AOS-W 8.5.0.6
AOS-213856	—	The **show ap remote debug heartbeat-miss-trace** command displayed only UTC time in **Time** field. The fix ensures that the command works as expected. This issue was observed in managed devices running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-213865	—	The WebUI displayed the message, **one or more settings have been overridden at bottling** and displays the older folder name after an override. The fix ensures that the WebUI does not displays the older folder name. This issue was observed in Mobility Masters running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-214255	—	Some older 802.11b clients were unable to connect to a few APs. This issue occurred when VAPs on 2.4 GHz radio were configured with different basic rates and when few VAPs did not include 802.11b CCK rates. The fix ensures seamless connectivity. This issue was observed in OAW-AP203R, OAW-AP203RP, OAW-AP203H, and OAW-AP207 access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-214261	—	Some clients experienced connectivity issues while roaming. The fix ensures seamless connectivity. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-214714	—	A stand-alone controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the controller works as expected. This issue was observed in stand-alone controllers running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-214835 AOS-218512	—	Some wireless clients connected to APs experienced slow network speed. Enhancements to the driver resolved the issue. This issue was observed in APs running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-214916	—	The value of **wlanAPRxDataBytes64** was displayed as 0. The fix ensures that the correct value is displayed. This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-215022	—	Clients authenticated using wpa3-sae-aes with MAC authentication were disconnected from the network. This issue occurred when a 4-way handshake was not initiated. The fix ensures that clients are not disconnected from the network. This issue was observed in managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-215641 AOS-215642 AOS-217268 AOS-217362 AOS-217640	—	The **ISAKMPD** process crashed on managed devices running AOS-W 8.6.0.0 or later versions in a PSK-RAP setup. The fix ensures that the managed devices work as expected.	AOS-W 8.7.1.1
AOS-216204	—	Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as, **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. The fix ensures that the APs work as expected. This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

Table 6: *Resolved Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216281	—	Some APs did not display any information related to crash. This issue occurred when the APs crashed twice. The fix ensures that the APs displays information related to crash and APs work as expected. This issue was observed in APs running AOS-W 8.6.0.0 or later versions.	AOS-W 8.7.1.1
AOS-216752 AOS-217439 AOS-217893	—	The **impystart** process crashed on a Mobility Master Virtual Appliance. The fix ensures that the Mobility Master Virtual Appliance works as expected. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-217035	—	A few APs were down and were unable to connect to the managed device. This issue occurred when UDP traffic was sent without establishing IPsec tunnels. This issue was observed in APs running AOS-W 8.3.0.0 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.6.0.7

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 8.7.1.3*

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-153742 AOS-194948	188871	A stand-alone switch crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in OAW-4010 switches running AOS-W 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.1

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
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-193701 AOS-209485	—	The **Rx Data Bytes** value in the **show ap debug radio-stats** command was lower than the actual value. The fix ensures that the correct number of data bytes are received. This issue was observed in stand-alone switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.0
AOS-197210	—	WebUI takes a long time to display data. 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-199545 AOS-212851	—	Some APs report low noise floor after upgrading the cluster to AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-199884	—	Mobility Master logs the following error message, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-201166 AOS-207939 AOS-209042	—	A switch crashes and reboots unexpectedly when the **HTTPD** process is restarted. The log files list the reason for the event as **Reboot cause: Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c)**. This issue is observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.5.0.2
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-203077 AOS-203232	—	Configurations committed using the **firewall cp** command are not synchronized on the standby Mobility Master. This issue occurs when static firewall entries are deleted. This issue is observed in Mobility Masters running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.3
AOS-203115 AOS-217219	—	The IAP-VPN tunnel goes down and the error message, **Failed to create internal-iap IP user entry and user entry due to too many user entries 128** is displayed. This issue occurs when the user table has 128 entries. This issue is observed in stand-alone switches running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203517 AOS-204709	—	The **Datapath** process crashes on managed devices unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).** This issue occurs when data packets undergo multiple GRE encapsulation. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-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-204187	—	The command, **vpn-peer peer-mac** does not support Suite-B cryptography for custom certificates. This issue is observed in Mobility Masters running AOS-W 8.2.2.8 or later versions.	AOS-W 8.2.2.8
AOS-204241	—	Managed devices log spurious DHCP DBUG messages. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-204892	—	The upgrade of AOS-W switches is delayed due to slow uplink speed. This issue is observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.	AOS-W 8.2.0.0
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 listed the reason 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 had 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-206537	—	The **H** flag indicating standby tunnel is not displayed in the output of the **show datapath tunnel-table** command and this results in a network loop. 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-206765 AOS-208978	—	A few show commands fail to display any output. This issue is observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
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-206890	—	The **body** field in the **Configuration > Services > Guest Provisioning** page of the WebUI does not allow users to add multiple paragraphs for email messages. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-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-206907	—	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 **Kernel panic - not syncing: assert**.	AOS-W 8.5.0.5
AOS-206929	—	The **show global-user-table** command does not provide an IPv6 based filtering option. This issue is observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-206930	—	Some Mobility Masters running AOS-W 8.7.0.0 or later versions allow to configure the same IPv6 address twice. This issue occurs when the user enters the same IPv6 address in a different format.	AOS-W 8.7.0.0
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
AOS-207303	—	Users are unable to add a managed device to an existing cluster of managed devices configured with rap-public-ip address. This issue is observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
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-207691	—	CLI displays incorrect IP address for a TACACS server. This issue is observed in managed devices running AOS-W 8.3.0.8 or later versions. **Workaround:** Restart the **profmgr** process for CLI to display the correct IP address.	AOS-W 8.3.0.8

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207692	—	Some managed devices running AOS-W 8.6.0.4 or later versions log multiple authentication error messages.	AOS-W 8.6.0.4
AOS-207775 AOS-215946	—	The **auth** process crashes on managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-207915	—	Some OAW-AP500 Series access points running AOS-W 8.6.0.4 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **AP Reboot reason: BadAddr:ecf47526bb436b6e PC:wlc_mutx_bw_policy_update+0x156c/0x2938 [wl_v6] Warm-reset.** **Duplicates:** AOS-208119, AOS-209128, AOS-210182, AOS-210217, AOS-211247, AOS-211252, AOS-211715, AOS-211774, AOS-212111, AOS-212235, AOS-212557, AOS-212741, AOS-212930, AOS-212961, and AOS-214656	AOS-W 8.6.0.4
AOS-208337 AOS-209348 AOS-212655 AOS-213442	—	The **airmatch_recv** process crashes on Mobility Controller Virtual Appliances running AOS-W 8.5.0.7 or later versions.	AOS-W 8.5.0.7
AOS-208420	—	Users are unable to log in to CLI of a switch. This issue occurs when the password has special characters, < and/or >. This issue is observed in switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.5
AOS-208421	—	Some managed devices running AOS-W 8.5.0.10 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Soft Watchdog reset**. **Duplicates:** AOS-209367, AOS-209509, AOS-209606, AOS-211577, AOS-211772, AOS-211879, and AOS-212502.	AOS-W 8.5.0.10
AOS-208696	—	The **profmgr** process crashes after configuring LACP and the error message, **Module profmgr is busy** is displayed. This issue is observed in Mobility Masters running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-208740 AOS-213754	—	The **profmgr** process crashes on Mobility Masters running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-208846	—	Clients connected to bridge mode SSIDs are unable to receive IP addresses and pass traffic. This issue is observed in stand-alone switches running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209130	—	Stale user entries are not removed from the user-table and hence, new users cannot connect to the managed device. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209273	—	The **Dashboard > Infrastructure** page of the WebUI does not display the data in graphical charts for mesh APs. This issue is observed in Mobility Masters running AOS-W 8.7.0.0 or later versions	AOS-W 8.7.0.0
AOS-209276	—	The **show datapath crypto counters** command displays the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. This issue is observed in Mobility Masters running AOS-W 8.5.0.0 or later versions.	AOS-W 8.5.0.10
AOS-209626	—	A few clients experience connectivity issue. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-209797	—	Some Mobility Master Hardware Appliances running AOS-W 8.6.0.4 or later versions intermittently return high values for SNMP walk for OID, **ifOutDiscards.**	AOS-W 8.6.0.4
AOS-209936 AOS-215097	—	Mobility Masters running AOS-W 8.6.0.6 or later versions display some BSSIDs as rouge BSSIDs even after manually white-listing the BSSIDs.	AOS-W 8.6.0.6
AOS-209977	—	SNMP query with an incorrect string fails to record the offending IP address in the trap or log information. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-209996	—	Some APs running AOS-W 8.5.0.9 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: __bug**.	AOS-W 8.5.0.9
AOS-210416 AOS-210480	—	The **show ap client trail-info** command display incorrect **VLAN(s)** values. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
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-210638	—	The **ARM** process crashes on managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-210845 AOS-217214 AOS-217871	—	OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions crash and reboot unexpectedly. The log file lists the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first.**	AOS-W 8.6.0.6
AOS-210922	—	The **auth** process crashes on stand-alone switches and APs reboot unexpectedly. The log file lists the reason for the reboot as **Unable to set up IPSec tunnel, Error:RC_ERROR_IKEV2_TIMEOUT.** This issue is observed in stand-alone switches running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210990	—	Some managed devices send BPDUs when STP is globally disabled. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
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-211437 AOS-218454	—	It takes a long time to synchronize configurations between stand-alone switch and standby switch running AOS-W 8.6.0.8.	AOS-W 8.6.0.8
AOS-211545 AOS-217654	—	Some APs running AOS-W 8.5.0.10 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **kernel panic: Fatal exception in interrupt.**	AOS-W 8.5.0.10
AOS-211587 AOS-216068	—	High CPU utilization is observed in **udbserver** and **postgres** processes. This issue is observed in managed devices running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-211658	—	A few clients are unable to connect to OAW-AP535 access points running AOS-W 8.6.0.5 or later versions in a cluster setup. This issue occurs when WMM and HT configurations are enabled.	AOS-W 8.6.0.5
AOS-211730	—	Users are unable to map server certificate as switch certificate on a secondary Mobility Master running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-211863	—	Some APs do not come up on managed devices. This issue occurs when ■ the forwarding mode is changed to bridge mode. ■ the name of the ACL reaches the maximum size of 64 bytes. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212123	—	The SNMP trap **wlsxNUserAuthenticationFailed** is not generated upon failed authentication in a termination-enabled dot1x configuration. This issue occurs in stand-alone switches running AOS-W 8.0.0.0 or later versions.	AOS-W 8.3.0.0
AOS-212198	—	Some OAW-RAP3WN OAW-RAPs running AOS-W 8.5.0.8 or later versions reboot unexpectedly. This issue occurs when time between the controller and the OAW-RAP is not in synchronization. **Workaround:** Reboot the OAW-RAP.	AOS-W 8.5.0.8
AOS-212255	—	Some APs are stuck in **Not in Progress** state during cluster live upgrade. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-212591	—	Some managed devices running AOS-W 8.7.1.0 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**.	AOS-W 8.7.1.0

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212935	—	Temporary ACL is still applied to user roles even if the disaster-recovery mode is disabled. This issue occurs when configuration changes in disaster recovery mode are not submitted using the **write memory** command. This issue is observed in managed devices running AOS-W 8.3.0.6 or later versions. **Workaround:** Ensure to submit the configuration changes made in the disaster-recovery mode.	AOS-W 8.3.0.6
AOS-212991	—	The **use-ip-for-calling-station** parameter of the **aaa authentication-server radius** command does not work as expected for VIA clients. This issue is observed in stand-alone switches running AOS-W 8.6.0.6.	AOS-W 8.6.0.6
AOS-213011	—	Packet loss is observed for clients during a cluster failover. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.5.0.10
AOS-213115	—	Some managed devices running AOS-W 8.5.0.10 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first.**	AOS-W 8.5.0.10
AOS-213307	—	L2 GRE ICMP keepalive response is sent outside the tunnel and hence, gets dropped by the firewall. This issue is observed in managed devices running AOS-W 8.5.0.1 or later versions.	AOS-W 8.6.0.6
AOS-213924 AOS-217233	—	Mobility Controller Virtual Appliance running AOS-W 8.7.0.0 or later versions displays incorrect VLAN ID details for some wired users.	AOS-W 8.7.0.0
AOS-214243 AOS-215775	—	A managed device running AOS-W 8.7.1.0 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**. This issue occurs due to a race condition.	AOS-W 8.7.1.0
AOS-214391 AOS-217130 AOS-217832	—	The STM process crashes on OAW-4750XM switches running AOS-W 8.4.0.0 or later versions.	AOS-W 8.5.0.11
AOS-214416	—	Some stand-alone switches running AOS-W 8.6.0.6 or later versions display the error message, **An internal system error has occurred at file main.c function rx_handler line 1517 error sxdr_read_str_safe szFunctionName failed**.	AOS-W 8.6.0.6
AOS-214434	—	Some APs are unable to come up on a managed device running AOS-W 8.5.0.8 or later versions. This issue occurs when UDP 8209 traffic is sent without establishing IPsec tunnels.	AOS-W 8.5.0.8
AOS-214963	—	Some APs running AOS-W 8.5.0.11 or later versions detect false radar.	AOS-W 8.5.0.11

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-215012 AOS-215567	—	The AP debug counters, **Total Bootstraps** and **Reboots** are not reset after upgrading the managed devices to AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-215021	—	**Channel Width Capability** configured on OmniVista 3600 Air Manager is not available in the **Dashboard > Overview > Wireless Clients** page of the WebUI. This issue is observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-215073	—	Some OAW-AP515 access points running AOS-W 8.5.0.8 or later versions go down and keep rebooting.	AOS-W 8.5.0.8
AOS-215546	—	The CLI does not trigger session timeout if paging is enabled. This issue is observed in Mobility Masters and managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.5
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 when 35 seconds is configured as UCC session idle timeout.	AOS-W 8.6.0.6
AOS-216133	—	Clients are unable to connect to APs on A-band channels. This issue is observed in APs running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0
AOS-217106	—	The **no valid** parameter of the ap regulatory-domain-profile command does not work while creating a new regulatory profile. This issue is observed in switches running AOS-W 8.0.0.0 or later versions. **Workaround:** Configure and save an ap regulatory-domain-profile and then issue the **no valid** commands.	AOS-W 8.6.0.7
AOS-217382	—	VRRP flapping is observed in Mobility Masters running AOS-W 8.6.0.5 or later versions. This issue occurs when the VRRP master could not send periodic advertisements.	AOS-W 8.6.0.5
AOS-217539	—	The **auth** process crashes on managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-217678 AOS-218131	—	Some APs do not honour the user alias route src-nat ACL and tunnels the traffic to managed devices. The issue occurs when a netdestination alias is configured in the ACL. This issue is observed in APs running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7
AOS-217694 AOS-218525	—	Some APs running AOS-W 8.7.1.1 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel Panic: Take care of the TARGET ASSERT first**.	AOS-W 8.7.1.1

Table 7: *Known Issues in AOS-W 8.7.1.3*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-217703	—	Some managed devices running AOS-W 8.6.0.7 or later versions take a long time to boot up after an upgrade.	AOS-W 8.6.0.7
AOS-218117	—	The **show ntp servers** and **show ntp status** commands display the error message, **Address family for hostname not supported**. However, the WebUI displays the NTP servers. This issue is observed in managed devices running AOS-W 8.6.0.7 or later versions.	AOS-W 8.6.0.7
AOS-218277 AOS-214428	—	The **auth** process crashes on managed devices running AOS-W 8.5.0.11 or later versions. Hence, the OAW-RAPs reboot and VIA users face connectivity issues.	AOS-W 8.5.0.11

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 35 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 35 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 35 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 34.

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 35 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 35 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 35.
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.