AOS-W 8.7.1.8 Release Notes

Contents

Chapter 1
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 01	Initial release.

Chapter 2
Release Overview

This AOS-W release notes includes the following topics:

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

For a list of terms, refer Glossary.

Related Documents

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

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

Supported Browsers

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

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

Terminology Change

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

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

Contacting Support

Table 2: *Contact Information*

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

Chapter 3
New Features and Enhancements in AOS-W 8.7.1.8

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

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 8.7.1.8*

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 8.7.1.8*

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 8.7.1.8*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205

Table 5: *Supported AP Platforms in AOS-W 8.7.1.8*

AP Family	AP Model
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
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

Table 5: *Supported AP Platforms in AOS-W 8.7.1.8*

AP Family	AP Model
OAW-AP550 Series	OAW-AP555
OAW-AP560 Series	OAW-AP565, OAW-AP567
OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577

Chapter 5
Regulatory Updates in AOS-W 8.7.1.8

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

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

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at https://myportal.al-enterprise.com/.

The following DRT file version is part of this release:

- DRT-1.0_82868

Chapter 6
Resolved Issues in AOS-W 8.7.1.8

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in AOS-W 8.7.1.8*

New Bug ID	Description	Reported Version
AOS-229991	Clients were unable to connect to SSIDs that had the 802.11r option enabled. During this period, commands run in the CLI returned the error message, **Module AP STM Low Priority is busy. Please try later**. The fix ensures that SSIDs configured with 802.11r option service the client as expected. This issue was observed in APs running AOS-W 8.3.0.0 or later versions. **Duplicates:** AOS-230192, AOS-230290, AOS-230554, AOS-230604, AOS-230721, AOS-230871, AOS-229972, AOS-230416, and AOS-230725	AOS-W 8.3.0.0

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 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-125897 AOS-187598 AOS-189036 AOS-192082 AOS-192723 AOS-192731 AOS-192734 AOS-195746 AOS-198423 AOS-204676	151952	When a managed device reboots, APs and clients boot without IP addresses and other fields. This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.	AOS-W 8.0.1.0
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

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-153742 AOS-194948	188871	A stand-alone switch crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in OAW-4010 switches running AOS-W 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.	AOS-W 8.5.0.1
AOS-190071 AOS-190372	–	A few users are unable to access websites when WebCC is enabled on the user role. This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0. **Workaround:** Perform the following steps to resolve the issue: 1.Remove web category from the ACL rules and apply **any any any permit** policy. 2. Disable WebCC on the user role. 3. Change the VLAN of user role from trunk mode to access mode.	AOS-W 8.4.0.0
AOS-190621	–	WebUI does not filter the names of the APs that contain the special characters, + and %. This issue is observed in managed devices and Mobility Masters running AOS-W 8.2.0.0 or later versions.	AOS-W 8.4.0.2
AOS-193231 AOS-200101 AOS-207456	–	The **Dashboard > Infrastructure > Access Devices** page of the WebUI displays an error message, **Error retrieving information**. This issue is observed in Mobility Masters running AOS-W 8.5.0.3 or later versions.	AOS-W 8.5.0.3
AOS-196042 AOS-217995 AOS-221263	–	The output of the **show ucc dns-ip-learning** command displays **Unknown** for **Service Provider**. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
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 error messages, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_ Free: Bad state index 0 state 0x1.** This issue is observed in Mobility Masters running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-200515 AOS-219987	–	The **DDS** process crashes on managed devices running AOS-W 8.3.0.10 or later versions.	AOS-W 8.3.0.10
AOS-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

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201428	–	The **show log all** command does not display the output in a chronological order. This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-202552 AOS-203990	–	The **Dashboard > Traffic Analysis > AppRF** page of the WebUI displays **Unknown** for WLANs, Roles, and Devices. This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-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-205140	–	The AppRF ACLs using a voice role block WebRTC calls. This issue occurs when WebRTC audio and video ACLs are not part of the default **voip-applications-acl**. This issue is observed in Mobility Masters running AOS-W 8.6.0.8 or later versions.
		Workaround: Add WebRTC audio and video ACLs to the user role using the following command:
		`ip access-list session webrtc`
		`any any app alg-webrtc-audio permit`
		`any any app alg-webrtc-video permit`
			AOS-W 8.6.0.8

AOS-205192	–	The channels configured using in the **Configuration > System > Profiles > All Profiles > AP > Regulatory Domain** profile page of the WebUI does not take effect. This issue is observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-206541	–	The **Maintenance > Software Management** page does not display the list of all managed devices that are part of a cluster. This issue is observed in Mobility Masters running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-206752	–	The console log of OAW-4450 switches running AOS-W 8.5.0.9 or later versions displays the **ofald| |sdn| ERRS ofconn_rx:476 <10.50.1.26:6633> socket read failed, err:Resource temporarily unavailable(11)** message.	AOS-W 8.5.0.9
AOS-206795	–	A user is unable to rename a node from the Mobility Master node hierarchy. This issue is observed in Mobility Masters running AOS-W 8.3.0.7 or later versions. **Workaround:** Restart **profmgr** process to rename the node.	AOS-W 8.3.0.7
AOS-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

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
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-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	–	A few 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-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-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-209888 AOS-224884	–	The **Diagnostics > Tools > AAA Server Test** page of the WebUI displays the **Authentication** status as **0** instead of **Authentication Successful**. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-209977	–	An 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

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
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-210490	–	Some managed devices running AOS-W 8.5.0.8 or later versions display the error message, **Error: Tunnel is part of a tunnel-group** while deleting an L2 GRE tunnel which is not a part of any tunnel group.	AOS-W 8.5.0.8
AOS-211720	–	The **STM** process crashes on managed devices and hence, APs failover to another cluster. This issue is observed in managed devices running AOS-W 8.5.0.5 or later versions.	AOS-W 8.5.0.5
AOS-211863	–	Some APs do not come up on managed devices. This issue occurs when the forwarding mode is changed to bridge mode and when 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-212038	–	The **show memory <process-name>** command does not display information related to the **dpagent** process. This issue is observed in managed devices running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212255	–	Some APs are stuck in **Not in Progress** state during cluster live upgrade. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-215063	–	The output of the **show gsm debug channel cluster_aac** and **show gsm debug channel cluster_ap** commands is not filtered correctly. This issue is observed in Mobility Masters running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-215461 AOS-220709	–	Database synchronization fails between standby and stand-alone switches running AOS-W 8.6.0.9 or later versions. The log files list the reason for the event as **Standby switch did not acknowledge the WMS database restore request**.	AOS-W 8.6.0.9
AOS-215669	–	Some managed devices running AOS-W 8.6.0.7 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**.	AOS-W 8.6.0.7
AOS-215852	–	Mobility Masters running AOS-W 8.6.0.6 or later versions log the error message, **ofa: 07765|ofproto|INFO|Aruba-SDN: 1 flow_mods 28 s ago (1 modifications).** This issue occurs when openflow is enabled and when 35 seconds is configured as the UCC session idle timeout.	AOS-W 8.6.0.6

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
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-217890	–	Some managed devices running AOS-W 8.5.0.10 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (SOS Assert)**.	AOS-W 8.5.0.10
AOS-218795	–	Downloadable user roles are not downloaded and hence, user roles are not assigned to the tunnel-node users. This issue is observed in managed devices running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-219307 AOS-223234	–	Some managed devices running AOS-W 8.5.0.12 or later versions crash unexpectedly. The log files list the reason for the event as, **Reboot cause: Kernel Panic (Intent:cause:register 12:86:f0:2)**.	AOS-W 8.5.0.12
AOS-219376	–	Some users are unable to add VIA server details if the domain name exceeds 32 characters. This issue is observed in Mobility Masters running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-219379 AOS-221300	–	Some managed devices are unable to connect to Mobility Masters. The log files list the reason for the event as <WARN> |fpapps| handleMasterIpMsg: Ignoring duplicate Uplink update from CFGM: ip x.x.x.x sec_master_ip 0.0.0.0 role 3;. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions in a cluster setup.	AOS-W 8.7.1.1
AOS-219803	–	The XML query done on a non-existing user, results in an invalid response. This issue is observed in managed devices running AOS-W 8.7.1.2 or later versions.	AOS-W 8.7.1.2
AOS-219936	–	The stand-alone controller displays the error message, **Module Profile Manager is busy. Please try later** while configuring netdestination. This issue is observed in stand-alone controllers running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-220515	–	Some managed devices running AOS-W 8.0.0.0 or later versions display the error message, **|fpapps| filling up the default gateway configuration.**	AOS-W 8.5.0.12
AOS-220706	–	The Mobility Master assigns duplicate IP addresses to the managed devices. This issue occurs after a failover. This issue is observed in Mobility Masters running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220903	–	The **s** flag indicating LACP striping is not displayed in the output of the **show ap database long** command even if LLDP is enabled on two uplinks. This issue is observed in APs running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-220982	–	A few wireless clients are unable to pass traffic during a cluster failover. This issue is observed in managed devices running AOS-W 8.5.0.13 or later versions.	AOS-W 8.5.0.13
AOS-221307	–	Adding a new VLAN removes all the existing VLANs on the port channel. This issue occurs when the existing VLAN list exceeds 256 characters. This issue is observed in managed devices running AOS-W 8.5.0.8 or later versions.	AOS-W 8.5.0.8
AOS-221789 AOS-223052	–	The 802.1X authentication is initiated twice. This issue is observed in APs running AOS-W 8.6.0.3 or later versions.	AOS-W 8.6.0.9
AOS-222401 AOS-227191	–	Some clients are unable to perform WPA3 authentication. This issue occurs after a cluster failover. This issue is observed in stand-alone switches running AOS-W 8.6.0.13 or later versions.	AOS-W 8.6.0.13
AOS-222469	–	The number of APs in a network are higher than the number of licenses installed. This issue is observed in stand-alone switches running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-222499	–	Clients that perform only four-way handshake are unable to update their VSA role derived after machine and user authentication. This issue is observed in managed devices running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-222786	–	The logs downloaded using the WebUI are incomplete and have missing files. This issue is observed in Mobility Masters running AOS-W 8.7.1.3 or later versions.	AOS-W 8.71.3
AOS-223094 AOS-220190 AOS-223094 AOS-224240 AOS-224792	–	A few users are unable to login to the captive portal page that is hosted on ClearPass Policy Manager server. This issue occurs when the netdestination ID, which is added to the captive portal whitelist, is incorrectly changed to 0 after a reboot of the Mobility Master Virtual Appliance. This issue is observed in Mobility Master Virtual Appliance running AOS-W 8.5.0.10 or later versions. **Workaround:** Create a new user role with the same set of ACL rules, and replace the existing user role.	AOS-W 8.6.0.9
AOS-223273	–	The UBT users list is not available in the user table after a cluster failover. This issue is observed in Mobility Master running AOS-W 8.7.1.4 or later versions in a cluster setup.	AOS-W 8.7.1.4

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-223274	–	Packet drop is observed on LACP configured OAW-AP535 access points running AOS-W 8.7.1.4 or later versions. This issue occurs when the outer IP header TOS value is different than the original inner IP header in ICMP error frame since the switch sends the ICMP destination unreachable frames back to the sender.	AOS-W 8.7.1.4
AOS-223337	–	The clients added to the client match unsupported list are still considered for client match steers. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-223817	–	The **auth** process crashes on Mobility Masters running AOS-W 8.6.0.9 or later versions. **Duplicates:** AOS-225761, AOS-226316, AOS-226846, AOS-227879, and AOS-225878	AOS-W 8.6.0.9
AOS-223839	–	The output of the **show ap active** command does not display any value for **Outer IP**. This issue is observed in Mobility Masters running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-223945	–	A managed device is discovered by both primary and secondary Mobility Masters in a Layer 3 redundancy deployment. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-224019 AOS-226123	–	High controlpath memory utilization is observed and an error message, **Resource 'Controlpath Memory' has dropped below 85% threshold** is displayed. This issue is observed in managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-224081 AOS-224083 AOS-225940	–	The **Dashboard > Overview> WLANs** page of the WebUI displays incorrect **Usage** value. This issue is observed in managed devices running AOS-W 8.5.0.10 or later versions in a cluster setup.	AOS-W 8.5.0.10
AOS-224275 AOS-215206	–	The predefined v6-control policy does not allow DHCPv6 traffic. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions.	AOS-W 8.6.0.9
AOS-224326 AOS-226350	–	A few OAW-AP514 access points running AOS-W 8.7.1.5 or later versions crash unexpectedly. The log files list the reason for the event as **PC is at wlc_ratesel_set_link_bw+0x0**.	AOS-W 8.7.1.5
AOS-224961	–	The global user entries table is not updated when clients roam to a different AP. This issue occurs when 802.11r is enabled. This issue is observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-225070	–	The AirGroup server table incorrectly displays duplicate host names. This issue is observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-225135	–	Clients connected to APs are unable to send or receive data packets from APs. This issue occurs when the ACL changes are not updated on APs. This issue is observed in APs running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-225231	–	The captive portal redirection URL does not display the complete ESSID. This issue occurs when the ESSID has 32 characters. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-225268	–	Some OAW-RAPs are assigned to incorrect nodes. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions in a cluster setup.	AOS-W 8.7.1.3
AOS-225817	–	Some AP-315 access points running AOS-W 8.5.0.13 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Reason: Reboot caused by kernel panic: assert**.	AOS-W 8.5.0.13
AOS-226075	–	The logs generated by the stand-alone switch do not have source and destination port details and the logs also indicate that all TCP packets are fragmented. This issue is observed in stand-alone switches running AOS-W 8.6.0.12 or later versions.	AOS-W 8.6.0.12
AOS-226331	–	The MTU discovery does not work as expected when the OAW-RAP connects to the VRRP virtual IP of the switch. This issue is observed in stand-alone switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-226440	–	The **auth** process crashes on stand-alone switches running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-226455	–	The **show datapath netdest-id** command does not display any output. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-226475	–	A few APs display flag **D**, indicating **Dirty or no config** state while provisioned to an AP group. This issue is observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-226547	–	A few APs are stuck in the **pre-validating status** state. This issue occurs when the **ap convert pre-validate all-aps** command is executed. This issue is observed in APs running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4
AOS-226555 AOS-224165	–	The **WMS** process crashes on Mobility Masters running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3

Table 7: *Known Issues in AOS-W 8.7.1.8*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-226683	–	The **show running-config** command does not display information related to IP RADIUS source-interface loopback. However, the **show configuration effective detail** command displays information about the IP RADIUS source-interface loopback. This issue is observed in managed devices running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-226932	–	Some OAW-AP515 access points running AOS-W 8.7.1.5 crash unexpectedly. The log files list the reason for the event as **wlc_pktq_stats_free+0x48**.	AOS-W 8.7.1.5
AOS-227039	–	Some OAW-AP505H mesh access points running AOS-W 8.7.1.5 or later versions are stuck in D flag after an upgrade.	AOS-W 8.7.1.5
AOS-227081	–	DPI fails to classify traffic and hence, application traffic is categorized as Port 0. This issue is observed in managed devices running AOS-W 8.6.0.11 or later versions.	AOS-W 8.6.0.11
AOS-227324	–	The **ofc_cli_agent** process crashes on Mobility Masters running AOS-W 8.6.0.13 or later versions. This issue occurs when the **show openflow-controlller ports** command is executed.	AOS-W 8.6.0.13

Chapter 8
Upgrade Procedure

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

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

Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W runs on your managed device?
  - Are all managed devices running the same version of AOS-W?
  - What services are used on your managed device (employee wireless, guest access, OAW-RAP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-W images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Alcatel-Lucent Mobility Master Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Master, or two versions lower. For example multiversion is supported if a Mobility Master is running AOS-W 8.5.0.0 and the managed devices are running AOS-W 8.5.0.0, AOS-W 8.4.0.0, or AOS-W 8.3.0.0.

Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as

JPEG images for RF Plan can consume flash space quickly. Following are best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space inis 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 24 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 24 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 24 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 23.

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 24 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 24 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 24.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.

   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.

   b. From **Select destination file** drop-down list, select **Flash file system**, and enter a file name (other than default.cfg).

c. Click **Copy**.

2. Determine the partition on which your pre-upgrade AOS-W version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade AOS-W version is not stored on your system partition, load it into the backup system partition by performing the following steps:

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

a. Enter the FTP or TFTP server address and image file name.

b. Select the backup system partition.

c. Enable **Reboot Controller after upgrade**.

d. Click **Upgrade**.

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

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

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

In the CLI

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

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

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

or

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

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

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

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

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

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

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

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