AOS-W 8.7.1.5 Release Notes

Alcatel·Lucent
Enterprise

Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

https://www.al-enterprise.com/en/legal/trademarks-copyright

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2021)

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

Contents

The following table 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.

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 Conductor 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://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

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

BLE Relay Process

Starting from AOS-W 8.7.1.5, all HTTP traffic of Meridian Beacons Management, Meridian Asset Tracking, and Telemetry Websocket are verified by the BLE Relay process.

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 8.7.1.5*

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 8.7.1.5*

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 8.7.1.5*

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

Table 5: *Supported AP Platforms in AOS-W 8.7.1.5*

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 8.7.1.5*

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

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_81131

The following issues are resolved in this release.

Table 6: *Resolved Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203517 AOS-204709 AOS-213765 AOS-221056	—	The **datapath** process crashed on managed devices running AOS-W 8.3.0.7 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.3.0.7
AOS-204187	—	The command **vpn-peer peer-mac** did not support Suite-B cryptography for custom certificates. The fix ensures that the command supports Suite-B cryptography for custom certificates. This issue was observed in Mobility Masters running AOS-W 8.2.2.8 or later versions.	AOS-W 8.2.2.8
AOS-206765 AOS-208978	—	A few show commands failed to display any output. The fix ensures that the commands display the output. This issue was observed in managed devices running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-207691	—	CLI displayed an incorrect IP address for a TACACS server. The fix ensures that the CLI displays the correct IP addresses for TACACS servers. This issue was observed in managed devices running AOS-W 8.3.0.8 or later versions.	AOS-W 8.3.0.8
AOS-208420	—	Users were unable to log in to the CLI of a switch. This issue occurred when the password had special characters, < and/or >. This issue is resolved by allowing special characters in the CLI password. This issue was observed in switches running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.5
AOS-209136	—	A few clients were disconnected due to the **Tx fail reached maximum** error. This issue occurred due to an incorrect state of variables in the AP while peer STA was in power save state, which lead to the packets being sent out when the peer STA was also in power save state. Since the peer STA was in power save state, it did not acknowledge the packets and the AP exhausted the maximum retries and disconnected the clients. The fix ensures that the state of variables in APs power save state machine is updated correctly. This issue was observed in AP-315 access points running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0

Table 6: *Resolved Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209879 AOS-220470	—	The **trusted vlan add** command removed all the existing trusted VLANs. The fix ensures that the **trusted vlan add** command does not remove all the existing trusted VLANs. This issue was observed in managed devices running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-209936 AOS-215097	—	Mobility Masters running AOS-W 8.6.0.6 or later versions displayed some BSSIDs as rouge BSSIDs even after manually whitelisting the BSSIDs. The fix ensures that the Mobility Masters work as expected.	AOS-W 8.6.0.6
AOS-210638	—	The **ARM** process crashed on managed devices running AOS-W 8.6.0.5 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.5
AOS-211578 AOS-219595	—	The bucketmap was not updated for a specific BSSID of an AP. The fix ensures that the bucketmap is updated. This issue was observed in APs running AOS-W 8.6.0.5 or later versions.	AOS-W 8.6.0.5
AOS-212310 AOS-219441	—	The **WebCC** and **NTPd** processes were in busy state in stand-alone switches running AOS-W 8.5.0.12 or later versions. This issue occurred when a DNS server or an NTP server was not reachable. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.5.0.12
AOS-212605 AOS-218721	—	Some APs running AOS-W 8.6.0.9 or later versions crashed unexpectedly. The log files listed the reason for the event as **wlc_key_get_info+0x4/0x60 [wl_v6]**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-215303	—	Users were unable to view file names in the **Diagnostic > Technical Support > Copy Files** page of the WebUI. This issue occurred when **Flash file system** was selected as the source file. The fix ensures that the users are able to view the file names. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-216512	—	The DHCP client/station related AMON message sent the mask, server IP address, and client IP address in the reverse order to the AirWave server. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-216764	—	Users were not redirected to the captive portal page. The fix ensures that the captive portal works as expected. This issue was observed in managed devices running AOS-W 8.7.1.0 or later versions in a cluster setup.	AOS-W 8.7.1.0

Table 6: *Resolved Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216766	—	Some APs generated sapd coredump. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-217184 AOS-218026 AOS-220562 AOS-220985	—	Some OAW-4750XM switches running AOS-W 8.7.1.1 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the events as, **Kernel Panic (Intent:cause:register 12:86:b0:4)**. This issue occurred due to socket buffer corruption. The fix ensures that the OAW-4750XM switches work as expected.	AOS-W 8.7.1.1
AOS-217807	—	Some OAW-RAPs took a long time to come up on a managed devices running AOS-W 8.6.0.5 or later versions in a cluster setup. This issue occurred due to a delay in whitelist-db synchronization between the Mobility Master and managed devices, and when external authentication was enabled for OAW-RAPs. The fix ensures that the OAW-RAPs do not take a long time to come up on a managed device.	AOS-W 8.6.0.5
AOS-218404 AOS-212330	—	Some APs were unable to ping a few clients. The fix ensures that the APs are able to ping clients. This issue was observed in APs running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-218621	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as **AP Reboot reason: BadAddr:6c0094119461 PC:wlc_ampdu_recv_ addba_resp+0x240/0x838 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-218622	—	Some APs running AOS-W 8.6.0.6 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC:aruba_wlc_ratesel_ getcurrate+0x24/0xd0 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-218642	—	Some iPads and other clients were unable to access the internet. This issue occurred when client entries were not removed by the managed devices even when CoA disconnect was triggered for the clients. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-218646	—	Ascom i63 phones connected to OAW-AP515 access points running AOS-W 8.6.0.7 or later versions experienced degraded audio quality. The fix ensures that the clients do not experience degraded audio quality.	AOS-W 8.6.0.7

Table 6: *Resolved Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219034	—	Clients connected to HT-enabled SSIDs connected as non-HT clients. The fix ensures that the APs work as expected. This issue is observed in APs running AOS-W 8.6.0.6 or later versions.	AOS-W 8.6.0.6
AOS-219178	—	Clients connected to the anchor controller were unable to receive IP addresses. The fix ensures that the clients are able to receive IP addresses. This issue is observed in managed devices running AOS-W 8.3.0.7 or later versions.	AOS-W 8.3.0.7
AOS-219214	—	The validuser acl list was reordered in stand-alone controllers running AOS-W 8.6.0.8 or later versions. The fix ensures that the validuser acl list is not reordered.	AOS-W 8.6.0.8
AOS-219355 AOS-223755 AOS-224270	—	Some OAW-AP515 access points running AOS-W 8.7.1.3 or later versions crashed unexpectedly. The fix ensures that the APs work as expected.	AOS-W 8.7.1.3
AOS-219384	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at wlc_nar_dotxstatus+0x450**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219725	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at wlc_nar_detach+0x8c**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-219879	—	The **show iap subnet** command did not display the **Allocated BID Branch List**. The fix ensures that the command displays the **Allocated BID Branch List**. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.	AOS-W 8.3.0.0
AOS-219894 AOS-220122	—	The BLE server displayed incorrect **Last Sync Time**. The fix ensures that the BLE server displays the correct **Last Sync Time**. This issue was observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-220053	—	Some OAW-RAPs went down on managed devices running AOS-W 8.6.0.5 or later versions. This issue occurred after a failover. The fix ensures that the OAW-RAPs work as expected.	AOS-W 8.6.0.5
AOS-220183	—	The user table did not list the PUTN users and the error message, **Dropping bridge miss rcvd for dormant PUTN user** was displayed. The fix ensures that the user table lists the PUTN users. This issue was observed in managed devices running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0

Table 6: *Resolved Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220251	—	Some users experienced connectivity issue. This issue occurred when APs did not respond to the authentication frames in MultiZone networks that have non-cluster zones and 802.11r enabled Virtual APs. The fix ensures seamless connectivity. This issue was observed in stand-alone switches running AOS-W 8.5.0.4 or later versions.	AOS-W 8.5.0.4
AOS-220293	—	Some APs running AOS-W 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as **aruba_wlc_ratesel_ getmaxrate+0x34**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1
AOS-220398	—	A few clients in bridge mode were unable to connect to WPA2-PSK SSIDs. The fix ensures that the clients in bridge mode are able to connect to WPA2-PSK SSIDs. This issue was observed in stand-alone switches running AOS-W 8.6.0.8 or later versions.	AOS-W 8.6.0.8
AOS-220552	—	The **Configuration > Services > Clusters** page of the WebUI did not display the status of live upgrade. This issue occurred when the cluster profile name had blank spaces. The fix ensures that the WebUI displays the status of live upgrade. This issue was observed in Mobility Masters running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-221005	—	Some stand-alone switches running AOS-W 8.7.1.2 or later versions were stuck in reboot loop. The log files listed the reason for the event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.7.1.2
AOS-221047 AOS-221813 AOS-223756	—	Some OAW-AP515 access points running AOS-W 8.7.1.3 or later versions crashed unexpectedly. The log files listed the reason for the event as, **AP Reboot reason: Panic:Ktrace core monitor: cpu2 hung for 36893488 seconds, hung cpu count: 3 Warm-reset.** The fix ensures that the APs work as expected.	AOS-W 8.7.1.3
AOS-221064	—	Some OAW-AP515 access points running AOS-W 8.7.1.3 or later versions crashed unexpectedly. The log files listed the reason for the event as, **AP Reboot reason: InternalError: : 96000210 1 SMP PC:phy_ utils_write_phyreg_nopi+0x70/0x130 [wl_v6] Warm-reset.** The fix ensures that the APs work as expected.	AOS-W 8.7.1.3
AOS-221225	—	Some OAW-AP387 access points running AOS-W 8.7.1.1 or later versions rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.1

Table 6: *Resolved Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-221352	—	Some mesh links reported incorrect RSSI values. The fix ensures that the mesh links report correct RSSI values. This issue was observed in APs running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-221429	—	Downloadable user roles were not applied correctly in the split tunnel mode. This issue was observed in stand-alone switches running AOS-W 8.6.0.9 or later versions. The fix ensures that the stand-alone switches work as expected.	AOS-W 8.6.0.9
AOS-221478 AOS-221569 AOS-221572	—	The **auth** process crashed on managed devices running AOS-W 8.5.0.9 or later versions. This issue occurred when the **show auth-tracebuf mac** command was executed. The fix ensures that the managed devices work as expected.	AOS-W 8.5.0.9
AOS-221507	—	Some OAW-AP515 access points running AOS-W 8.7.1.3 or later versions crashed unexpectedly. The log files listed the reason for the event as **BadAddr:ffffffc12c30ca80 PC:_alloc_ skb+0x110/0x1c8 Warm-reset**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.3
AOS-221726	—	Some managed devices running AOS-W 8.7.1.1 or later versions were unable to form L2 clusters with its peers. The fix ensures that the managed devices are able to form L2 clusters.	AOS-W 8.7.1.1
AOS-221743 AOS-212229	—	Some APs running AOS-W 8.5.0.10 or later versions rebooted unexpectedly. The log files listed the reason for the events as, **skb_release_ data+0xa0/0xc8/neigh_flush_dev+0x60**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-221856 AOS-222034 AOS-222201	—	A few APs running AOS-W 8.7.1.3 or later versions displayed negative counters. This issue occurred in APs that used ESDK version 6.2.1.2. The fix ensures that the APs work as expected.	AOS-W 8.7.1.3
AOS-222051	—	The **IAPMGR** process crashed on managed devices running AOS-W 8.6.0.4 or later versions. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.4
AOS-222540 AOS-224221	—	Some APs dropped EAPOL packets from the bridge mode wired port. The fix ensures that the APs do not drop the EAPOL packets. This issue was observed in APs running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-222787	—	Some OAW-AP535 access points running AOS-W 8.7.1.3 or later versions rebooted unexpectedly. The log file lists the reason for the event as, **kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.3

Table 6: *Resolved Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-223434 AOS-223579	—	Some OAW-AP515 access points running AOS-W 8.7.1.4 displayed the error log, **wl0: 802.11 reinit reason[2]**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.4
AOS-224090 AOS-225043	—	Some managed devices running AOS-W 8.6.0.10 or later versions were stuck in the **Last Snapshot** state. This issue occurred when tunnel MTU was set to a value lesser than 1500. The fix ensures that the managed devices work as expected.	AOS-W 8.6.0.10
AOS-224296	—	A few clusters got disconnected from the network. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-225590	—	Some users experienced connectivity issues. The fix ensures seamless connectivity. This issue was observed in managed devices running AOS-W 8.5.0.10 or later versions in a cluster setup.	AOS-W 8.5.0.10

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 8.7.1.5*

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 8.7.1.5*

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-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-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 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-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-201428	—	The **show log all** command does not display 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

Table 7: *Known Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
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-205693 AOS-204926	—	The **auth** process crashes on managed devices running AOS-W 8.5.0.9 or later versions. This issue occurs while configuring bandwidth contract.	AOS-W 8.5.0.9
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
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	—	APs go down and UDP 8209 traffic is sent without UDP 4500 traffic. This issue is observed in managed devices running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-207245	—	Some managed devices running AOS-W 8.5.0.8 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 53:86:0:802c).**	AOS-W 8.5.0.8

Table 7: *Known Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
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-208597	—	The **show ap mesh monitor stats** command returns 0 for output. This issue is observed in Mobility Masters running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
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-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-210416 AOS-210480	—	The **show ap client trail-info** command displays 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-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-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

Table 7: *Known Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
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-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
AOS-213507	—	Some managed devices running AOS-W 8.5.0.10 or later versions crash unexpectedly. The log files list the reason for the event as, **Reboot Cause: Soft Watchdog reset**. Duplicates: AOS-210240, AOS-214964, AOS-215393, AOS-215421, AOS-215628, AOS-215765, AOS-215827, AOS-216087, AOS-216315, AOS-216420, AOS-216888, AOS-217041, AOS-218007, AOS-218021, AOS-218907, AOS-219588, AOS-219597, AOS-220471, AOS-220981, AOS-221390, AOS-221642, and AOS-222036	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-215712	—	Mobility Masters running AOS-W 8.7.0.0 or later versions forward all syslog messages with severity level marked as debug. This issue occurs when CEF format is enabled on the Mobility Master.	AOS-W 8.7.0.0

Table 7: *Known Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
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-216145	—	Mobility Masters running AOS-W 8.5.0.8 or later versions send continuous DNS requests to the managed devices. This issue occurs when a folder that is not available on the /mm node is trying to get synchronized on the managed devices. **Workaround:** Perform the following steps to resolve the issue: 1.Issue the **show memory debug | include rsync** command to identify the name of the folder that is trying to get synchronized on the managed devices. 2. Ensure that the folder is not present in the /flash/upload/custom/ path of the Mobility Master and then issue the **no sync files <folder name>** command to stop synchronization.	AOS-W 8.5.0.8
AOS-216536 AOS-220630	—	Some managed devices running AOS-W 8.5.0.11 or later versions are unable to come up on the Mobility Master. This issue occurs when the managed devices get the branch IP address as the switch IP address in a VPNC deployment.	AOS-W 8.5.0.11
AOS-216622	—	A few APs incorrectly display the restricted flag, **p = Restriction mode in POE-AF/AT** in the AP database even if the Ethernet port is disabled. This issue is observed in APs running AOS-W 8.7.0.0 or later versions.	AOS-W 8.7.0.0
AOS-217653 AOS-224031	—	Some OAW-AP535 access points running AOS-W 8.7.1.4 or later versions do not respond to the fragmented ping requests from a few clients. This issue occurs when the APs operate in tunnel mode.	AOS-W 8.7.1.4
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-218162	—	The wired Ethernet port does not form GRE tunnel with the managed device. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1

Table 7: *Known Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218254 AOS-218875	—	Some managed devices running AOS-W 8.7.1.0 or later versions crashes unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2).**	AOS-W 8.7.1.0
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-219112	—	A few UBT clients hop between VLANs. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
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-219383	—	The **Configuration > License > License Usage** tab does not display the license details. This issue is observed in stand-alone controllers running AOS-W 8.5.0.12 or later versions.	AOS-W 8.5.0.12
AOS-219385	—	Some APs take a long time to come up on the backup data center after the primary data center failover. This issue is observed in APs running AOS-W 8.5.0.10 or later versions.	AOS-W 8.5.0.10
AOS-219894 AOS-220122	—	The BLE server displays incorrect **Last Sync Time**. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
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-220108	—	The **OFA** process crashes on Mobility Master Virtual Appliances running AOS-W 8.6.0.6 or later versions. This issue occurs when the **show openflow debug ports** command is executed.	AOS-W 8.6.0.6
AOS-220183	—	The user table does not list the PUTN users and the error message, **Dropping bridge miss rcvd for dormant PUTN user** is displayed. This issue is observed in managed devices running AOS-W 8.7.1.0 or later versions.	AOS-W 8.7.1.0

Table 7: *Known Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220293	—	Some APs running AOS-W 8.7.1.1 or later versions crash unexpectedly. The log files list the reason for the event as **aruba_wlc_ratesel_getmaxrate+0x34**.	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-220704	—	Some APs are incorrectly displayed under different clusters. This issue is observed in managed devices running AOS-W 8.5.0.11 or later versions.	AOS-W 8.5.0.11
AOS-221144	—	ARP packets are not forwarded to the uplink switch when bcmc-optimization is enabled on the switches. This issue is observed in Mobility Masters and managed devices running AOS-W 8.5.0.9 or later versions.	AOS-W 8.5.0.9
AOS-221666 AOS-222708	—	Some OAW-RAPs running AOS-W 8.6.0.9 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Kernel panic - not syncing**.	AOS-W 8.6.0.9
AOS-221726	—	Some managed devices running AOS-W 8.7.1.1 or later versions are unable to form L2 clusters with its peers.	AOS-W 8.7.1.1
AOS-221883 AOS-221884	—	Users are unable to add ACLs using the **firewall cp** command and an error message, **Error: Max CP firewall limit (97) reached** is displayed. This issue is observed in managed devices running AOS-W 8.7.1.3 or later versions.	AOS-W 8.7.1.3
AOS-222578	—	L2TP IP address leak is observed and the VLAN pool is exhausted. This issue is observed in managed devices running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-222754	—	The SNMP walk to managed devices fails when the SNMP requests have the IPv6 address of the switch. This issue occurs when the primary managed device has VRRP IPv6 address configured. This issue is observed in managed devices running AOS-W 8.4.0.1 or later versions.	AOS-W 8.4.0.1
AOS-222771	—	Some managed devices running AOS-W 8.5.0.12 or later versions do not send SNMPv3 information to the OmniVista 3600 Air Manager server.	AOS-W 8.5.0.12
AOS-222931	—	Some APs do not form active tunnels with the AAC. This issue is observed in managed devices running AOS-W 8.7.1.4 or later versions.	AOS-W 8.7.1.4

Table 7: *Known Issues in AOS-W 8.7.1.5*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-223669	—	Some users are unable to complete captive portal authentication. This issue occurs when ipv6-user snmpwalk populates IPv4 user details. This issue is observed in managed devices running AOS-W 8.6.0.0 or later versions.	AOS-W 8.6.0.4
AOS-223797	—	The **show ap remote auth-trace-buf** command does not display any output. This issue is observed in stand-alone switches and managed devices running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9
AOS-223807	—	Some OAW-4850 switches running AOS-W 8.7.1.5 generates multiple kernel messages.	AOS-W 8.7.1.5
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-223848	—	The **+** symbol in the **Configuration > Services > AirGroup > Service-Based Policy** page of the WebUI does not allow users to create an AirGroup profile. Users can create an AirGroup profile only by navigating to the **Configuration > System > Profiles > AirGroup** page of the WebUI. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	AOS-W 8.7.1.4
AOS-224186	—	The **show tech-support** command does not display any information about the kernel crash and displays the message, **No kernel crash information available**. This issue is observed in stand-alone switches running AOS-W 8.6.0.9 or later versions.	AOS-W 8.6.0.9

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 Conductor, managed device, or stand-alone switch.

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- 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 Conductor Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Conductor, or two versions lower. For example multiversion is supported if a Mobility Conductor 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 29 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.

  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 29 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.

  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 29 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

⚠️ **CAUTION**

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

From the Mobility Conductor, 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 Conductor 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 Conductor or managed device. For details, see Memory Requirements on page 28.

NOTE When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message is displayed ccurs when you upgrade using the WebUI and navigate to the **Configuration** tab after the managed device reboots. This message disappears after clearing the Web browser cache.

In the WebUI

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

1. Download the AOS-W image from the customer support site.

2. Upload the AOS-W image to a PC or workstation on your network.

3. Validate the SHA hash for the AOS-W image:

    a. Download the **Alcatel.sha256** file from the download directory.

    b. Load the AOS-W image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.

    c. Verify that the output produced by this command matches the hash value found on the customer support site.

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

4. Log in to the AOS-W WebUI from the Mobility Conductor.

5. Navigate to the **Maintenance > Software Management > Upgrade** page.

    a. Select the **Local File** option from the **Upgrade using** drop-down list.

    b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.

6. Select the downloaded image file.

7. Choose the partition from the **Partition to Upgrade** option.

8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

NOTE The upgrade does not take effect until reboot. If you chose to reboot after upgrade, the Mobility Conductor 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 Conductor.

3. Execute the **ping** command to verify the network connection between the Mobility Conductor 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 Conductor.

```
(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 Conductor is functioning as expected:

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the AOS-W image version.

2. Verify if all the managed devices are up after the reboot.

3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.

4. Verify that the number of APs and clients are as expected.

5. Test a different type of client in different locations, for each access method used.

6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 29 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.

2. Execute the **show version** command to verify the AOS-W image version.

3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.

4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.

5. Test a different type of client in different locations, for each access method used.

6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 29 for information on creating a backup.

Downgrading AOS-W

A Mobility Conductor or managed device has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the Mobility Conductor or managed device from the other partition.

Pre-requisites

Before you reboot the Mobility Conductor or managed device with the pre-upgrade AOS-W version, perform the following steps:

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 29.

2. Verify that the control plane security is disabled.

3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.

4. Set the Mobility Conductor 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 Conductor 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 Conductor 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 Conductor or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.

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

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

c. Click **Copy**.

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

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

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

b. Select the backup system partition.

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

d. Click **Upgrade**.

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

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

4. When the boot process is complete, verify that the Mobility Conductor 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 Conductor 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 Conductor 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 Conductor or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Conductor 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.