AOS-W 8.10.0.15 Release Notes

Open Source Code

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

Contents

Chapter 1
Revision History

The following table 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

Important

- Upgrading from AOS-W.10.0.6 or earlier versions on OAW-41xx Series and 9200 Series switches will take longer than usual as we will be automatically upgrading the BIOS version to support additional functionality in the future. This upgrade is estimated to take up to 15 minutes and should not be interrupted for any reason. Power failures and interruptions during the upgrade may make the switch unusable. Please use caution and plan accordingly.

Cluster Rolling Upgrade is not supported when a BIOS upgrade is required. AOS-W must be manually upgraded for these controllers. In a (very rare) scenario where, post reload command, the unit does not come up in 15-20 minutes, apply power cycle only once and wait for a minimum of 15 minutes without re-applying power cycle again.

- As mandated by the Wi-Fi Alliance, AOS-W.10.0.0 and later versions require Hash-to-Element (H2E) for 6 GHz WPA3-SAE connections. H2E is supported on Android 12 or later versions, Linux wpa_ supplicant version 2.10 or later versions, macOS Catalina or later versions, Windows 11 or later versions. Users must upgrade their clients to support successful 6 GHz WPA3-SAE connections.
- The factory-default image of APs introduced in AOS-W.9.0.0 or later versions use **aruba-conductor** as the host name instead of **aruba-master** to identify a target managed device or stand-alone switch during DNS discovery. However, the factory-default image of APs that were introduced prior to AOS-W.9.0.0 still use **aruba-master** during DNS discovery. The usage of **aruba-conductor** is to align with the Inclusive Language Initiative.

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 ConductorLicensing 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:

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	■ Windows 10 or later ■ macOS
Firefox 107.0.1 or later	■ Windows 10 or later ■ macOS
Apple Safari 15.4 (17613.17.1.13) or later	■ macOS
Google Chrome 108.0.5359.71 or later	■ Windows 10 or later ■ 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

Contact Center Online

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
What's New in AOS-W.10.0.15

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

Luminosity Contrast Fixes

This release introduces improved contrast ratios throughout the WebUI to ensure better visibility and readability for users with visual impairments.

New Automatic Reboot upon TPM Communication Failure

The Trusted Platform Module (TPM) is a critical hardware component for secure operations of an access point. This version of AOS-W introduces a health check and an auto-reboot mechanism whenever an AP experiences an issue communicating with its TPM.

New WebCC Categories Available

AOS-W.10.0.15 adds Brightcloud's new WebCC categories: **self-harm (85)**, **dns-over-https (86)**, **low-thc-cannabis-products (87)**, and **generative-ai (88)**.

Behavioral Changes

This release does not introduce any changes in AOS-W behaviors, resources, or support that requires modifying the existing system configurations after updating to 8.10.0.15.

Supported Platforms in AOS-W.x

This section displays the supported platforms in AOS-W.x. The **minimum version supported** column displays the minimum AOS-W.x version that can be run on a platform. The **latest version supported** column displays the newest AOS-W.x version that can be run on a certain device. Patch releases do not affect platform support. For example, a device which **latest supported version** is 8.10.0.x can run on any 8.10.0.x version, such as 8.10.0.2 or 8.10.0.10.

Mobility Conductor Platforms

Mobility Conductor		AOS-W.x Versions Supported	
Conductor Family	**Conductor Model**	**Minimum**	**Latest**
Hardware Mobility Conductor	MCR-HW-1K, MCR-HW-5K, MCR-HW-10K	8.1.0.x	8.12.0.x
Virtual Mobility Conductor	MCR-VA-500, MCR-VA-1K, MCR-VA-5K, MCR-VA-10K	8.0.0.x	8.12.0.x
	MCR-VA-50	8.1.0.x	8.12.0.x

OmniAccess Mobility Controller Platforms

OmniAccess Mobility Controllers		AOS-W.x Versions Supported	
switch Family	**switch Model**	**Minimum**	**Latest**
9200 Series	9240	8.10.0.x	8.12.0.x
OAW-41xx Series	9012	8.7.0.x	8.12.0.x
	OAW-4104	8.5.0.x	8.12.0.x
OAW-4x50 Series	OAW-4850	8.3.0.x	8.12.0.x
	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM	8.0.0.x	8.12.0.x
OAW-40xx Series	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030	8.0.0.x	8.12.0.x
Virtual OmniAccess Mobility Controllers	MC-VA-50, MC-VA-250, MC-VA-1K	8.0.0.x	8.12.0.x
	MC-VA-10	8.4.0.x	8.12.0.x

Access Point Platforms

Access Points			AOS-W.x Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
6xx	670 Series	AP-675, AP-675EX, AP-677, AP-677EX, AP-679, AP-679EX	8.12.0.x	8.12.0.x
	OAW-AP650 Series	OAW-AP655	8.10.0.x	8.12.0.x
		AP-654	8.11.2.x	8.12.0.x
	OAW-AP630 Series	OAW-AP635	8.9.0.x	8.12.0.x
		AP-634	8.11.2.x	8.12.0.x
	OAW-AP610 Series	AP-615	8.11.0.x	8.12.0.x
	600 Series	AP-605H	8.12.0.x	8.12.0.x
5xx	OAW-AP580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX	8.10.0.x	8.12.0.x
	OAW-AP570 Series	OAW-AP574, OAW-AP575, OAW-AP577. AP-575EX, AP-577EX	8.7.0.x	8.12.0.x
	OAW-AP560 Series	OAW-AP565, OAW-AP567, AP-565EX, AP-567EX	8.7.1.x	8.12.0.x
	OAW-AP550 Series	OAW-AP555	8.5.0.x	8.12.0.x
	OAW-AP530 Series	OAW-AP534, OAW-AP535	8.5.0.x	8.12.0.x
	OAW-AP510 Series	OAW-AP518	8.7.0.x	8.12.0.x
		OAW-AP514, OAW-AP515	8.4.0.x	8.12.0.x
	OAW-AP500 Series	OAW-AP504, OAW-AP505	8.6.0.x	8.12.0.x
		OAW-AP505H, OAW-AP505HR	8.7.0.x	8.12.0.x
		OAW-AP503H, OAW-AP503HR	8.7.1.x	8.12.0.x
		AP-503	8.11.1.x	8.12.0.x

Access Points			AOS-W.x Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
3xx	380 Series	OAW-AP387	8.4.0.x	8.10.0.x
	OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377, OAW-AP375EX, OAW-AP377EX, OAW-AP375ATEX	8.3.0.x	8.12.0.x
	OAW-AP360 Series	OAW-AP365, OAW-AP367	8.3.0.x	8.12.0.x
	OAW-AP340 Series	OAW-AP344, OAW-AP345	8.3.0.x	8.10.0.x
	OAW-AP330 Series	OAW-AP334, OAW-AP335	8.1.0.x	8.10.0.x
	OAW-AP320 Series	OAW-AP324, OAW-AP325	8.0.0.x	8.10.0.x
	OAW-AP310 Series	OAW-AP318	8.3.0.x	8.12.0.x
		OAW-AP314, OAW-AP315	8.1.0.x	8.12.0.x
	OAW-AP300 Series	OAW-AP304, OAW-AP305	8.1.0.x	8.12.0.x
		OAW-AP303H, OAW-AP303HR	8.2.0.x	8.12.0.x
		OAW-AP303P	8.4.0.x	8.12.0.x
		OAW-AP303	8.3.0.x	8.12.0.x
2xx	OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277	8.0.0.x	8.10.0.x
	OAW-AP 220 Series	OAW-AP224, OAW-AP225, OAW-AP228	8.0.0.x	8.10.0.x
	OAW-AP210 Series	OAW-AP214, OAW-AP215	8.0.0.x	8.10.0.x
	OAW-AP200 Series	OAW-AP207	8.1.0.x	8.10.0.x
		OAW-AP204, OAW-AP205, OAW-AP205H	8.0.0.x	8.10.0.x
		OAW-AP203H, OAW-AP203R, OAW-AP203RP	8.2.0.x	8.10.0.x

Access Points			AOS-W.x Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
1xx	OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1	8.0.0.x	8.6.0.x
	OAW-AP130 Series	OAW-AP134, OAW-AP135	8.0.0.x	8.6.0.x
	OAW-AP110 Series	OAW-AP114, OAW-AP115	8.0.0.x	8.6.0.x
	OAW-AP100 Series	OAW-AP103, OAW-AP104, OAW-AP105	8.0.0.x	8.6.0.x
		OAW-AP103H	8.0.0.x	8.3.0.x
9x	OAW-AP90 Series	OAW-AP92, OAW-AP93, AP-93H	8.0.0.x	8.2.0.x

Chapter 5
Regulatory Updates

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_91171

Chapter 6
Resolved Issues in AOS-W.10.0.15

This chapter describes the resolved issues in this release.

Table 3: *Resolved Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-236543	Some switches unexpectedly crashed and rebooted. The log files listed the reason as **Reboot Cause: Datapath crash found after stressing CP with jumbo traffic**. The fix ensures the switches work as expected. This issue was observed in OAW-4x50 switches running AOS-W.11.0.0 or later versions.	AOS-W.11.0.0
AOS-236755 AOS-257767	Some OAW-AP535 access points randomly reduced the power level to 2 dBm and disabled the 2.4 GHz radio. The fix limits 5G-specific chainmask functions to the 5 GHz radio. This issue was observed in APs running AOS-W.10.0.6 or later versions.	AOS-W.10.0.6
AOS-245107	Some OAW-4750 switches running AOS-W.10.0.6 or later versions crashed on the datapath module. The log files listed the reason for the event as **Kernel panic with Reboot Cause: Soft Watchdog reset (Intent:cause:register de:86:70:2)**. The fix ensures that the datapath module works as expected.	AOS-W.10.0.6
AOS-246195	After enabling the TLS toggle in the **Managed Network node hierarchy > Configuration > System > Logging** page of the WebUI, traffic was not initiated on datapath sessions. This caused logs not to be sent to the syslog servers. The fix ensures that logging works as expected. This issue is observed in managed devices running AOS-W.10.0.7 or later versions.	AOS-W.10.0.7
AOS-247572	Some APs crashed and rebooted unexpectedly due to a memory leak. This issue occurred when the **add ssid-profile** and **delete ssid-profile** commands were used multiple times in a week. The fix ensures that the APs work as expected. This issue was observed in OAW-AP515 access points running AOS-W.10.0.11 or later versions.	AOS-W.10.0.11
AOS-247793	Some OAW-AP535 access points crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **AP crashed at ar_wal_vdev.c:3320 Assertion vdev_handle->type == WAL_VDEV_TYPE_STA**. The fix ensures the APs work as expected. This issue was observed in APs running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-249631	Cluster live upgrades failed while trying to upgrade to AOS-W.10.0.9. The log files listed the reason of the event as **Image copy failed on controller ip 172.21.7.12 ipv6 N/A, Incompatible file ArubaOS_72xx_8.10.0.9_88493**. The fix ensures that cluster live upgrades work as expected. This issue was observed in switches running AOS-W.10.0.7 or later versions.	AOS-W.10.0.9

Table 3: *Resolved Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-251950	Users were unable to connect to SSIDs with **Enterprise** security enabled. This issue occurred because the station sent a deauthentication request to the AP before the 802.1x authentication process was completed. The fix ensures that users are able to connect to the SSIDs with **Enterprise** security. This issue was observed on APs running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-252388 AOS-258834	The **AUTH** process crashed unexpectedly on some switches after a cluster live upgrade. The fix ensures that the **AUTH** process works as expected. This issue was observed in switches running AOS-W.10.0.13 or later versions in a cluster setup.	AOS-W.10.0.13
AOS-252701	The **show configuration effective detail** command displayed the CPPM password for a non-privileged account instead of displaying a string of **#** characters. The fix ensures the correct output is displayed. This issue was observed in gateways running AOS-W.10.0.0 or later versions.	AOS-W.10.0.7
AOS-253056	Devices running AOS-W.10.0.7 or later versions experienced memory leaks in the **arci-cli-helper** process when navigating the WebUI. The fix ensures that the **arci-cli-helper** process functions as expected.	AOS-W.10.0.7
AOS-253616 AOS-256571	Mobility Conductors did not update AirMatch optimization. The fix ensures that the AirMatch optimization works as expected. This issue was observed in Mobility Conductors running AOS-W.10.0.10 or later versions.	AOS-W.10.0.11
AOS-253850 AOS-259311	Clients experienced poor network performance when connecting to APs in a cluster. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W.10.0.12 or later versions.	AOS-W.10.0.12
AOS-253999 AOS-255991 AOS-257087 AOS-257689 AOS-258502	Some APs randomly crashed and turned off with an **MMC: MMC init failed** error message. The fix ensures the APs work as expected. This issue was observed in OAW-AP635 and OAW-AP655 access points running AOS-W.9.0.0 or later versions.	AOS-W.9.0.0
AOS-254784	When clients connected to an AP, the AP generated the following error log: **<ERRS> |AP KAKAO-AP-A03F-R16@172.20.4.104 stm| |ap| Unexpected stm (Station management) runtime error at handle_assoc_req, 7378, handle_assoc_req: sa-mac:a4:75:b9:d7:3d:d2, aid:59(LE:0xc03c) >= 60 or 1024, driver-val:60**. This issue occurred when the 6 GHz radio was enabled. The fix ensures that the logs are not generated. This issue was observed in APs running AOS-W.10.0.10 or later versions.	AOS-W.10.0.10
AOS-254923	The **profmgr** process crashed and rebooted unexpectedly on a switch due to a memory segmentation fault. This issue was observed in switches running AOS-W.10.0.7 or later versions. The fix ensures that the **profmgr** process works as expected.	AOS-W.10.0.7

Table 3: *Resolved Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-255194	Silex bridges in a mixed-mode SSID with TKIP encryption were unable to pass traffic due to TKIP decryption failures on OmniAccess Mobility Controllers. The fix ensures that the decryption process happens seamlessly. This issue was observed in 9240 OmniAccess Mobility Controllers running AOS-W.10.0.12 or later versions.	AOS-W.10.0.12
AOS-255636	Users were unable to monitor devices due to SNMP walk failure with a **Error: OID not increasing: WLSX-AUTH-MIB::authServerType** message. The fix ensures that the SNMP walk is successful. This issue was observed on devices running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-256177	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **FW assert count 1 collected 0 Send PC:0x00000000 to Wlan driver**. The fix ensures the APs work as expected. The issue was observed in OAW-AP535 and OAW-AP635 access points running AOS-W.10.0.9 or later versions.	AOS-W.10.0.9
AOS-256468	Some switches crashed unexpectedly due to the authentication process. After the crash, users were disconnected from the switch for a certain period of time. The fix ensures that the switches function as expected without crashing. This issue was observed in switches running AOS-W.10.0.10 or later versions.	AOS-W.10.0.10
AOS-256829 AOS-257029 AOS-257034 AOS-259321 AOS-259349	Some APs continuously switch between switches in a cluster, although no connectivity issues were observed. This issue occurred when the **Active AP Unbalanced Threshold** value is less than the **Active AP Rebalance AP Count** value. The fix ensures that the APs do not switch between switches unexpectedly. This issue was observed in APs in a cluster setup running AOS-W.10.0.10 or later versions.	AOS-W.10.0.13
AOS-257003	The ISAKMPD module unexpectedly crashed in 9240 switches running AOS-W.10.0.11 or later versions. The fix ensures that the ISAKMPD module functions as expected.	AOS-W.10.0.11
AOS-257019 AOS-257931	Fake rogue BSSIDs were listed in the output of the **show ap monitor ap-list** command. The fix ensures that the command displays the correct information. This issue was observed in APs running AOS-W.10.0.11 or later versions.	AOS-W.10.0.11
AOS-257057 AOS-258999	The HTTP module crashed on multiple gateways after upgrading to AOS-W.10.0.13 or later versions, affecting UBT clients. The fix ensures that the HTTP module does not crash on the gateways.	AOS-W.10.0.13
AOS-257095	Some APs failed to clear the loop status despite having the **Auto Recovery** and **the Loop Protect** configurations enabled in wired ports. The fix ensures the process works as expected. This issue was observed in OAW-AP505H access points running AOS-W.10.0.13 or later versions.	AOS-W.10.0.13
AOS-257192	Some clients experienced connectivity issues due to unstable mesh points. The fix ensures that the mesh points work as expected. This issue was observed in OAW-AP375 access points running AOS-W.10.0.7 or later versions.	AOS-W.10.0.7

Table 3: *Resolved Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-257196	Users were able to input invalid channel names when executing the **airmatch ap freeze** command. The fix ensures that an error message is displayed when users input incorrect information. This issue was observed in APs running AOS-W.10.0.11 or later versions.	AOS-W.10.0.11
AOS-257202	Some switches were displayed as **Down** in OmniVista 3600 Air Manager despite working normally. switch error logs displayed the message **|snmp| An internal system error has occurred at file../unix/aruba_main.c function snmpRequestProcessing line 747 error I cannot send a SNM response. errno:22 errstr:Invalid argument snmpdTI.fd:22 Destination**. This issue was related to the SNMP module of some switches being flooded with invalid requests, increasing memory usage. The fix optimizes memory management for switches to show their correct status and perform as expected. This issue was observed in switches running AOS-W.10.0.7 or later versions.	AOS-W.10.0.7
AOS-257229 AOS-258175	Whenever APs running AOS-W.12.0.2 or earlier versions had a kernel crash, they occasionally transferred an empty **kdump.tar.gz** file to their controller. This issue was related to special characters in the AP name conflicting with kdump file generation. The fix ensures APs will transfer the right kdump file as expected.	AOS-W.10.0.12
AOS-257295	When managed devices' software version was upgraded to AOS-W.10.0.8 or later, IDS incorrectly reported **Null-Probe-Response** events from some APs. This issue occurred when the driver sent a valid **Probe-Response** frame padded with extra bytes. The fix ensures that false events are not reported by IDS after software upgrades.	AOS-W.10.0.8
AOS-257534 AOS-259375	The mDNS process unexpectedly crashed in switches with an active Hidden Markov Model (HMM). The fix ensures the process works as expected. This issue was observed in switches running AOS-W.10.0.13 or later versions.	AOS-W.10.0.12
AOS-257560	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **Crash Internal error: Oops: 17 [#1] SMP ARM during weekend longevity**. The fix ensures the APs work as expected. The issue was observed in AP-615 access points running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-257640	A temporary OSPF blip caused an out-of-sync state issue between one cluster node and the UBT switch, resulting in some clients facing connectivity issues. The fix ensures UBT switches work as expected. This issue was observed in OmniAccess Mobility Controllers running AOS-W.10.0.12 or later versions.	AOS-W.10.0.2
AOS-257681	Some switches unexpectedly crashed due to the SNMP process. The fix ensures the process works as expected. This issue was observed in OAW-4650 switches running AOS-W.10.0.11 or later versions.	AOS-W.10.0.11

Table 3: *Resolved Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-257732	Some APs crashed and rebooted unexpectedly with reboot reason **BadPtr: 00000028 PC: anul_intf_init+0xb4/0x2b0 [anul] Warm-reset**. The issue was related to rare cases of pointers not obtaining proper memory assignment. The fix ensures APs work as expected. This issue was observed in APs running AOS-W.10.0.0 or later versions.	AOS-W.12.0.1
AOS-257826 AOS-258832 AOS-258938 AOS-259259 AOS-259303 AOS-259775	Some switches unexpectedly crashed and rebooted. The log files listed the reason as **Reboot Cause: Datapath timeout**. The fix ensures the switches work as expected. This issue was observed in 9240 switches running AOS-W.10.0.8 or later versions.	AOS-W.10.0.8
AOS-258089	Users were unable to form a UBT tunnel with the new switch in a cluster. This issue occurred when A-SAC was removed from the cluster. The fix ensures the UBT tunnels work as expected. This issue was observed in switches running AOS-W.10.0.5 or later versions.	AOS-W.10.0.5
AOS-258221	Some OAW-AP377 access points in a cluster did not broadcast SSIDs. The APs were flagged as inactive in the output of the **show ap database** command. The fix ensures the APs work as expected. This issue was observed in APs running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-258720 AOS-259805	Some switches unexpectedly crashed and rebooted. The log files listed the reason as **Reboot Cause: Datapath timeout**, which was caused by a packet with an invalid IP header reaching the controller. The fix ensures the switches work as expected. This issue was observed in 9240 switches running AOS-W.10.0.8 or later versions.	AOS-W.10.0.8
AOS-258874	Some OAW-4750XM switches crashed and rebooted multiple times. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the controllers do not crash and reboot. This issue was observed on OAW-4750XM switches running AOS-W.10.0.14 or later versions.	AOS-W.10.0.14
AOS-258924	Some OAW-AP535 and OAW-AP555 access points experienced high interference issues. The fix ensures APs work as expected. This issue was observed in APs running AOS-W.10.0.9 or later versions.	AOS-W.10.0.9
AOS-259293 AOS-260414	Some APs incorrectly reported high channel utilization in all 2.4 GHz radios after upgrading to AOS-W.10.0.14 or later versions, causing connectivity issues for clients. This issue was related to the adaptive Rx sensitivity adjustment feature, which was disabled. The fix enables the feature and ensures it works as expected.	AOS-W.10.0.14
AOS-259714 AOS-259725	Some clients experienced frequent disconnection from their SSID. This issue was related to a crash in the **auth** process of switches running AOS-W.10.0.14 or later versions. The fix ensures the **auth** module works as expected and client connection remains uninterrupted.	AOS-W.10.0.14

Table 3: *Resolved Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-245687 AOS-250956	VLAN configuration changes triggered a reconfiguration in all VAPs that caused transient issues at scale. The fix ensures the configuration works as expected. This issue was observed in APs running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-255909	Some APs crashed and rebooted with reason **AP rebooted caused by internal watchdog reset**. This error was related to the driver image on the device. The fix ensures that the APs function as expected. This issue was observed in OAW-AP535 and OAW-AP655 access points running AOS-W.10.0.11 or later versions.	AOS-W.10.0.11

Chapter 7
Known Issues in AOS-W.10.0.15

This chapter describes the known issues observed in this release.

Known Issues

Following are the known issues observed in this release.

Table 4: *Known Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-205650 AOS-231536	DHCP traffic from relay agent is not forwarded through the next-hop list configured in Layer 3 GRE tunnel. This issue is observed in managed devices running AOS-W.6.0.15 or later versions.	AOS-W.6.0.15
AOS-217948	Some APs experience issues with Wi-Fi uplink 802.1X authentication due to a conflict in certificate validity period verification. This issue is observed in APs running AOS-W.7.1.1 or later versions.	AOS-W.7.1.3
AOS-221308	The **execute-cli** command does not work as expected for a few show commands. This issue is observed in Mobility Conductors running AOS-W.7.1.4 or later versions.	AOS-W.7.1.4
AOS-229024	Some OAW-AP505 access points running AOS-W.7.1.5 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **PC is at wlc_mbo_parse_ie+0x15c/0x2b0 [wl_v6]**.	AOS-W.7.1.5
AOS-229770	switches do not display information on the 802.1X connection statuses if the 802.1X connection fails. This issue is observed in switches running AOS-W.7.1.8 or later versions.	AOS-W.7.1.8
AOS-232092	Some AP-305 and OAW-AP505 access points are not discoverable by Zigbee devices. The southbound traffic lists an **AP not found** error. This issue is observed in managed devices running AOS-W.8.0.1 or later versions.	AOS-W.8.0.1
AOS-232233	Some OAW-4104-LTE switches cache the LAN side MAC address during boot up. Thus, the gateway does not receive an IP address from the modem. This issue is observed in switches running AOS-W.7.0.0 or later versions.	AOS-W.7.1.4
AOS-232875 AOS-239469	The **mon_serv** process crashes in certain high-load scenarios, particularly with a large number of APs and users with high roaming rates. The issue occurs in OmniAccess Mobility Controllers running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-236471	Alcatel-Lucent OAW-4740 controllers running AOS-W.10.0.1 or later versions do not show the configured banner information in GUI login page.	AOS-W.10.0.1

Table 4: *Known Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-236852	The error **ofa: |ofa| ofa_gsm_ event_user_process: port not found:19, tnm50c4ddb3b194 end point is not configured or is down** is displayed when a client connects to an IAP-VPN tunnel. This issue is observed in Mobility Conductors running AOS-W.10.0.2 or later versions.	AOS-W.10.0.2
AOS-237174	Some 9240 switches record informational logs, even though the system log level is configured as **warning**. This issue is observed in 9240 switches running AOS-W.10.0.2 or later versions.	AOS-W.10.0.2
AOS-238407 AOS-236630 AOS-240428 AOS-241047	AppRF application or application category ACL does not block YouTube on devices connected to APs running AOS-W.6.0.16 or later versions.	AOS-W.6.0.16
AOS-238846	The **Exceeds the max supported vlans 128** error message is displayed when creating Layer 2 VLANs at folder level. This issue is observed in Mobility Conductors running AOS-W.6.0.15 or later versions.	AOS-W.6.0.15
AOS-239521	Users are unable to add a tunnel to a tunnel group and an error message is displayed: **Error: All tunnels must have same vlan membership**. This issue occurs when the VLANs are configured in a different order when compared to the order configured for other tunnels the same group. This issue is observed in managed devices running AOS-W.6.0.15 or later versions.	AOS-W.6.0.15
AOS-239724 AOS-239529	Some APs unexpectedly increase the response time when using DHCP configuration. This issue is observed in APs running AOS-W.10.0.2 or later versions.	AOS-W.10.0.2
AOS-241212 AOS-241537	Some OAW-4650 switches running AOS-W.10.0.4 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Nanny rebooted machine - low on free memory**.	AOS-W.10.0.4
AOS-241542	Some switches unexpectedly report crashes in the **flow_manager** module. This issue is observed in switches running AOS-W.10.0.0 or later versions.	AOS-W.10.0.11
AOS-242532	Some OAW-AP535 access points are not available on OAW-4550 switches post a power outage. This issue occurs when a USB converter and a console cable are used, which interrupt the boot up process and result in the AP not showing up on the switch. The issue is observed in switches running AOS-W.6.0.9 or later versions.	AOS-W.6.0.9
AOS-243266	Some APs upgraded through TFTP become stuck in **Upgrading** status due to an incorrect automatic change of UDP ports. This issue is observed in OmniAccess Mobility Controllers running AOS-W.6.0.20 or later versions.	AOS-W.6.0.20
AOS-243536	Some OmniAccess Mobility Controllers display incorrect values in **Discovery State** and **Transport State** for AirGroup services. This issue is observed in OmniAccess Mobility Controllers running AOS-W.0.0.0 or later versions.	AOS-W.0.0.0

Table 4: *Known Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-244193	Some OAW-AP655 access points frequently bootstrap. The issue occurs due to an interoperability issue of the AP firmware with certain third-party switches. The issue is observed in APs running AOS-W.10.0.6 or later versions.	AOS-W.10.0.6
AOS-244850	The CLI process crashes unexpectedly on 9240 switches running AOS-W.10.0.0 or later versions.	AOS-W.10.0.8
AOS-244965	An unnecessary debugging log appears as **Received ICMP (DEST_UNREACH, PROT_UNREACH) from X.X.X.X for heartbeat tunnel**. This issue is observed in switches running AOS-W.10.0.5 or later versions.	AOS-W.10.0.5
AOS-245367	In standalone switches, it is not possible to configure application speed limit under the **Dashboard > Traffic Analysis > Applications** tab. This feature works if the switch is in Conductor role, but this error is not reported properly. This issue is observed in switches running AOS-W.10.0.5 or later versions.	AOS-W.10.0.5
AOS-245600 AOS-252206 AOS-255808	Some switches crash unexpectedly due to a memory leak in the **DDS** process. This issue is observed in switches running AOS-W.6.0.17 or later versions.	AOS-W.10.0.8
AOS-246103 AOS-247433 AOS-240688 AOS-250837	Some OAW-AP635 and OAW-AP535 access points reboot randomly with reboot reason **Reboot caused by kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_send.c:11778 first**. This occurs due to issues with M3 switch recovery, to which the APs are connected. This issue is observed in APs running AOS-W.10.0.5 or later versions.	AOS-W.10.0.5
AOS-246170 AOS-245703	The **Dashboard > Overview > Wireless Clients** page of the WebUI does not show accurate information. For example, some column information like **IP ADDRESS** and **ROLE** might show as blank, and the **NAME** column might wrongly display other information like the **MAC ADDRESS** of the client. This issue is observed in Mobility Conductors running AOS-W.10.0.6 or later versions.	AOS-W.10.0.6
AOS-246606	The NVDA reader calls out only parameters that are not configured under the **Services > Firewall** page of the WebUI. This issue is observed in switches running AOS-W.10.0.0 or later versions.	AOS-W.10.0.0
AOS-246960	OmniAccess Mobility Controller upgrades trigger license changes, which cause the unintended loss of configured user-roles and ACLs in managed devices. This issue is observed in OAW-4010 switches running AOS-W.6.0.21 or later versions. **Workaround**: Reload the managed device or restart the **profmgr** process to fix the issue.	AOS-W.6.0.21
AOS-247721	Mobility Conductors in a standby setup failover and crash unexpectedly. The log files list the reason as **Datapath Exception**. This issue is observed in Mobility Conductors running AOS-W.10.0.7 or later versions.	AOS-W.10.0.7

Table 4: *Known Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-248466	The **switch discovery preference** field disappears when changing it from **ADP** to **Static** under the **Dashboard > Configuration > Access Point > Provision** page. This issue is observed in switches running AOS-W.10.0.8 or later versions.	AOS-W.10.0.8
AOS-248905	Clients are assigned the wrong role when reconnecting to WPA3 Enterprise (GCM) SSIDs, in both CNSA and non-CNSA modes. The issue is related to PMK caching as part of dot1x authentication. This issue is observed in switches running AOS-W.10.0.0 or later versions. **Workaround**: Since this is a PMK caching issue, clearing the cache by using the **aaa authentication dot1x key-cache clear <unk>station-mac>** command solves the problem.	AOS-W.10.0.0
AOS-248909	A few clients fail to connect to gateways running AOS-W.10.0.0 or later versions. This issue occurs because of an increased number of denied DHCP requests in UDP port 68 preventing clients from obtaining IP addresses, and user-based ACLs incorrectly blocking the gateway's DHCP requests.	AOS-W.10.0.0
AOS-250148	AirGroup's **Transport State** becomes stuck on **initializing** status. This issue is related to the current handling of OpenFlow flows in AOS SDN switches. This issue is observed in managed devices running AOS-W.0.0.0 or later versions.	AOS-W.0.0.0
AOS-250747	Mobility Conductors with RBTree elements reach the maximum allowed value due to an age out issue in WMS, which causes WIDS to function incorrectly. This issue is observed in Mobility Conductors running AOS-W.10.0.7 or later versions.	AOS-W.10.0.7
AOS-251605 AOS-241347	Wired AirGroup servers disappear from the AirGroup server table when GE/PC ports are deactivated. This issue is observed on OmniAccess Mobility Controllers running AOS-W.10.0.0 or later versions.	AOS-W.10.0.9
AOS-252538	The **IKE XAuth** process fails on OAW-RAPs, causing them to reboot and appear as **Down** on switches. The issue occurs when users do not modify the password in the WebUI while provisioning multiple RAPs. This issue is observed in APs running AOS-W.6.0.17 or later versions.	AOS-W.6.0.17
AOS-252798	The **OFA** process crashes on switches running AOS-W.10.0.10 or later versions after a RAP deployment. The issue occurs due to a segmentation fault while deleting a client object from the OFML library.	AOS-W.10.0.10
AOS-253146 AOS-254328	WLANs with any upper-case characters created from the CLI or WebUI cannot be edited through the **Configuration > WLANs** section of the WebUI. This issue is observed in Mobility Conductors running AOS-W.10.0.11 or later versions.	AOS-W.10.0.11
AOS-254363	The **switch_manager** process crashes on some switches running AOS-W.10.0.8 or later versions.	AOS-W.10.0.8
AOS-254700	Users are unable to delete stale AP entries through the WebUI or CLI. This issue is observed in Mobility Conductors running AOS-W.10.0.11 or later versions in a cluster setup.	AOS-W.10.0.11

Table 4: *Known Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-255529 AOS-256450	The **Delete** option is missing for the first four WLANs listed in the WebUI of the Mobility Conductor. This issue is observed in managed devices running AOS-W.10.0.8 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W.10.0.8
AOS-255629	The bandwidth contract profile reference is not updated correctly when used in other profiles, such as role or user. This issue is observed in managed devices running AOS-W.10.0.7 or later versions.	AOS-W.10.0.7
AOS-255648 AOS-255929	Some clients experience MAC authentication issues when attempting to connect to an SSID. This issue is related to RadSec server connectivity. This issue is observed in OAW-4550 switches running AOS-W.10.0.6 running or later versions.	AOS-W.10.0.6
AOS-256292	switches display an error message when the user attempts to access the managed network node through the **Dashboard > Configuration > Services** page. This issue occurs when the cluster profile is configured with a space in the profile name. This issue is observed in switches running AOS-W.10.0.8 or later versions in a cluster setup.	AOS-W.10.0.12
AOS-256471	Some Mobility Conductors running AOS-W.10.0.12 or later versions experience slow loading times when trying to configure any profiles through the WebUI.	AOS-W.10.0.12
AOS-256745	In the **Configuration > System > Profiles** page of the WebUI, the landscape scroll bar cannot be dragged. This issue is observed in switches running AOS-W.10.0.13 or later versions.	AOS-W.10.0.13
AOS-256821	The BLE relay process crashes unexpectedly in OAW-4650 switches running AOS-W.10.0.11 or later versions. This issue occurs when the main BLE relay thread and the thread for the WebSocket connection are not synchronized. This causes the connection state to be removed by the main BLE thread while the WebSocket thread accesses the packet queue.	AOS-W.10.0.11
AOS-257285	When 13 or more VAPs are configured on a single radio, the APs become stuck in **Dirty** state. This issue results in a continuous flood of configuration messages that overwhelms the STM process, causing client association to fail. This issue is observed in switches running AOS-W.10.0.13 or later versions in a cluster setup.	AOS-W.10.0.13
AOS-257588	Some APs do not age out clients although the **station ageout timer** parameter is configured to the default value of 1000 seconds. This issue is observed in OAW-AP535 access points running AOS-W.10.0.10 or later versions.	AOS-W.10.0.12
AOS-257760	The authentication server name appears duplicated with the duplicate text overlapping the existing text. This issue occurs sometimes when a new server is configured on the WLAN profile during asynchronous operations. This issue is observed in switches running AOS-W.10.0.0 or later versions.	AOS-W.10.0.12

Table 4: *Known Issues in AOS-W.10.0.15*

New Bug ID	Description	Reported Version
AOS-258090	Some Mobility Conductors unexpectedly display the **imudp: error receiving on socket: Broken pipe: Broken pipe [v8.2102.0]** error in the rsyslogs. This issue is observed in Mobility Conductors running AOS-W.10.0.13 or later versions.	AOS-W.10.0.13
AOS-258103	Some APs experience packet loss when receiving pings with packet size over 497 bytes from Cisco's fast ping protocol. This issue is observed in OAW-AP515 access points running AOS-W.10.0.13 or later versions.	AOS-W.10.0.13
AOS-258212 AOS-258932	Cluster live upgrade preloads only some APs in a cluster with 9240 switches that have gold capacity licenses. This issue is observed in switches running AOS-W.10.0.9 or later versions in a cluster setup.	AOS-W.10.0.11
AOS-259138	The **ofa** process crashes unexpectedly with the error message **ofserver_handle_connection_down_event**. This issue is observed in switches running AOS-W.10.0.7 or later versions.	AOS-W.10.0.7
AOS-259603 AOS-260283 AOS-260347	The ZMQ threads of the **nbapi_helper** process crash randomly. This issue is observed in Mobility Conductors after upgrading the software to AOS-W.10.0.14 or later versions.	AOS-W.10.0.14
AOS-259719 AOS-259734	Clients do not receive an IP address when reconnecting to the AP after upgrading the software version. This issue occurs when the ACL is configured to deny user traffic from UDP port 68. This issue is observed in managed devices running AOS-W.10.0.14 or later versions.	AOS-W.10.0.14
AOS-259788	In the **Access Point** tab of the WebUI, some APs incorrectly display the **UPTIME** as **0**. This issue is observed in APs running AOS-W.10.0.14 booted at the same time as the switch.	AOS-W.10.0.14
AOS-260012	Under the **Dashboard > Configuration > Roles & Policies > Roles** page, the **RULES** field incorrectly displays **--** when **Policy-Based Routing** is enabled. This issue occurs because of a case mismatch between the policy names received from the API. This issue is observed in managed devices running AOS-W.10.0.14 or later versions.	AOS-W.10.0.14

Chapter 8
Limitations in AOS-W.10.x

This section includes the known limitations in 8.10.x.x releases.

Title	Description
Port-Channel Limitation in OAW-4850 switches	The OAW-4850 hardware architecture consists of two Network Acceleration Engines (NAEs). The ethernet ports are split between the NAEs according to this mapping: ■ NAE 0: Ports 0/0/4 to 0/0/7 and 0/0/12 to 0/0/15 ■ NAE 1: Ports 0/0/0 to 0/0/3 and 0/0/8 to 0/0/11 When configuring a port-channel, it is recommended that member ports are distributed between the two different NAEs (e.g., 0/0/0 and 0/0/4) . This is to ensure hitless operation if one of the member ports experiences a link flap either due to a network event or a user-driven action. If member ports are on the same NAE, a link flap will be observed for less than a second. It is not recommended to form a 10 Gbe based port-channel larger than 2x 10 Gbe due to this hardware limitation.
No Support for Airtime Fairness Mode	Airtime Fairness Mode is not supported in 802.11ax access points.

6 GHz Channel Information in Regulatory Domain Profile	AOS-W does not display the 6 GHz channel information in the existing regulatory domain profile of Wi-Fi 6E APs by default.
	To include 6 GHz channel information, ensure that you change the country code to a different country code, apply the change, and then revert it to the original country code. Another option is to create a new regulatory domain profile that includes the 6 GHz channel information by default, or copy the existing regulatory domain profile into a new regulatory domain profile to save the configuration.
	The following example configures a regulatory domain profile and specifies a valid 6 GHz band.
	`(host) [mynode](config) #ap regulatory-domain-profile reg-635`
	`(host) [mynode] (Regulatory Domain profile "reg-635") #country-code US`
	`(host) [mynode] (Regulatory Domain profile "reg-635") #valid-6ghz-channel 165`

Limitations in OAW-AP650 Series and OAW-AP630 Series Access Points	■ No spectrum analysis on any radio ■ No Zero-Wait DFS ■ No Hotspot and Air Slice support on the 6 GHz radio ■ No 802.11mc responder and initiator functionality on any radio ■ Only 4 VAPs on the 6 GHz radio instead of 16 ■ Maximum of 512 associated clients on any radio, instead of 1024
Air Slice is partially enabled on some OAW-AP500 Series APs	Air Slice is partially enabled on OAW-AP500 Series access points and OAW-AP510 Series access points. However, WMM boost will be functional even if Air Slice high-priority queuing is disabled.

Title	Description
cpboot command in OAW-40xx Series and OAW-4x50 Series switches	The **cpboot** command does not upgrade the AOS-W software version of OAW-40xx Series and OAW-4x50 Series controllers.

Chapter 9
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 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*.
- With the introduction of the Long Supported Release (LSR) and Short Supported Release (SSR) terminology in AOS-W.10.0.0, a Mobility Conductor running an LSR release supports managed devices running the same release and the three preceding releases. This is considered as N-3 support. This allows a customer to run the latest LSR, the previous SSRs and the previous LSR simultaneously. A Mobility Conductor running an SSR release supports managed devices running the same release and the two preceding releases. This would be considered N-2 support and is the same behavior as the pre-AOS-W.10.0.0 MultiVersion support.

- Only for the AOS-W.10.0.0 LSR release, AOS-W.6.0.0 is treated as an LSR despite being beyond N-3. As such a Mobility Conductor running AOS-W.10.0.0 supports managed devices running AOS-W.10.0.0, AOS-W.9.0.0, AOS-W.8.0.0, AOS-W.7.0.0 and AOS-W.6.0.0.

Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. Following are best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your 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 32 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 32 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 32 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 Conductor, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups.

In the CLI

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

Low Free Flash Memory

Sometimes, after extended use, the flash memory might get used up for logs and other files. The AOS-W image has increased in size and this may cause issues while upgrading to newer AOS-W images without cleaning up the flash memory.

Prerequisites

Before you proceed with the freeing up the flash memory:

- Ensure to always backup the configuration and flash memory. Issue the **backup configuration** and **backup flash** commands to backup the configuration and flash.
- Copy the **flashbackup.tar.gz** and **configbackup.tar.gz** files out of the switch. Then delete the **flashbackup.tar.gz** and **configbackup.tar.gz** files from the flash memory of the switch.
- Use only one partition for the upgrade activity and keep the other partition unchanged.

If you use the WebUI to perform an upgrade, a banner on the **Maintenance** page provides the following reminder to have sufficient free flash memory before initiating an upgrade.

For a healthy and stable system it requires free space of 360 MB for AOS v8.3 and 8.5, 570 MB for AOS 8.6 and 8.7 and 450 MB for AOS 8.8 and higher version in the /flash directory. Please make sure minimum required memory is available in /flash before upgrading to newer version.

Freeing up Flash Memory

The following steps describe how to free up the flash memory before upgrading:

1. Check if the available memory in **/flash** is greater than the limits listed in Table 5 for all supported switch models:
   Table 5: *Flash Memory Requirements*

Upgrading from	Upgrading to	Minimum Required Free Flash Memory Before Initiating an Upgrade
8.3.x	8.10.x	360 MB
8.5.x	8.10.x	360 MB
8.6.x	8.10.x	570 MB
8.7.x	8.10.x	570 MB
8.8.x	8.10.x	450 MB
8.9.x	8.10.x	450 MB
8.10.x	8.10.x	450 MB

   To check the available free flash memory, issue the **show storage** command. Following is the sample output from a switch with low free flash memory:

```
(host) [mynode] #show storage
Filesystem              Size    Available       Use     %       Mounted on
/dev/usb/flash3         1.4G    1014.2M         386.7M  72%     /flash
```

2. If the available free flash memory is less than the limits listed in Table 5, issue the following commands to free up more memory.
   - **tar crash**
   - **tar clean crash**
   - **tar clean logs**
   - **tar clean traces**

3. Issue the **show storage** command again to check if the available space in **/flash** is more than the minimum space required for AOS-W upgrade as listed in Table 5
4. **If you are unable to free up sufficient flash memory, contact Technical Support. Do not reboot the switch.**
5. If sufficient flash memory is available, proceed with the standard AOS-W upgrade. See Upgrading AOS-W.
6. If a reboot was performed, you may see some of the following errors. Follow the directions below:
   - Upgrade using standard procedure. You may see some of the following errors:

     Error upgrading image: Ancillary unpack failed with tar error (tar: Short header).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Ancillary unpack failed with tar error (tar: Invalid tar magic).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Need atleast XXX MB space in /flash for image upgrade, please clean up the /flash and try upgrade again.

     Failed updating: [upgradeImageNew.c] extractAncTar (dev: /dev/usb/flash1 imgLoc: /flash/config/ArubaOS_70xx_8.8.0.0-mm-dev_78066
   - If any of the above errors occur, issue the **show image version** command to check for the default boot partition. The partition which was upgraded should become the default partition. Following is the sample output of the **show image version** command:

```
(host) [mynode] #show image version
---------------------------------
Partition               : 0:0 (/dev/usb/flash1) **Default boot**
Software Version        : AOS-W.9.0.0 (Digitally Signed SHA1/SHA256 - Production
Build)
Build number            : 81046
Label                   : 81046
Built on                : Thu Aug 5 22:54:49 PDT 2021
---------------------------------
Partition               : 0:1 (/dev/usb/flash2)
Software Version        : AOS-W.7.0.0-2.3.1.0 (Digitally Signed SHA1/SHA256 -
Developer/Internal Build)
Build number            : 0000
Label                   : arpitg@sdwan-2.3_arpitg-3-ENG.0000
Built on                : Tue Aug 10 15:02:15 IST 2021
```

   - If the default boot partition is not the same as the one where you performed the upgrade, change the default boot partition. Issue the **boot system partition <part_number>** command to change the default boot partition. Enter **0** or **1** for **part_number** representing partition 0:0 or partition 0:1, respectively.
   - Reload the switch. If any of the errors listed in step 4 were observed, the following errors might occur while booting AOS-W.9.0.0.

```
Sample error:
[03:17:17]:Installing ancillary FS                    [ OK ]
Performing integrity check on ancillary partition 1   [ FAIL : Validating new
ancillary partition 1...Image Integrity check failed for file
/flash/img1/mswitch/sap/arm32.ari. Digest Mismatch]
Extracting Webui files..tar: Short read
chown: /mswitch/webui/*: No such file or directory
chmod: /mswitch/webui/wms/wms.cgi: No such file or directory
```

   - After the switch reboots, the login prompt displays the following banner:

```
*****************************************************************
```

```
* WARNING:  An additional image upgrade is required to complete the *
* installation of the AP and WebUI files. Please upgrade the boot   *
* partition again and reload the controller.                        *
*********************************************************************
```

- Repeat steps 1 through 5. If sufficient free flash memory is available, proceed with the standard AOS-W upgrade procedure. See Upgrading AOS-W.
- If sufficient free flash memory is not available, issue the **dir** and **dir flash** commands to identify large files occupying the flash memory.

- Exercise caution while deleting files. Contact Technical Support if you are not sure which large files in the **/flash** directory could be safely deleted to free up the required space.

  Issue the **delete filename <filename>** command to delete large files to free more flash memory.
- Check if sufficient flash memory is free as listed in Table 5.
- Proceed with the standard AOS-W upgrade procedure in the same partition. See Upgrading AOS-W.

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.

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 29.

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 32 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 32 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 32.
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:

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
```

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.