AOS-W 8.10.0.0 Release Notes

Contents

Contents 3

Revision History 4

Release Overview 5
- Related Documents 5
- Supported Browsers 5
- Important 5
- Terminology Change 5

Contacting Support 6

What's New 7
- New Features and Enhancements in AOS-W 8.10.0.0 7
- Behavioral Changes 13

Supported Platforms 14
- Mobility Conductor Platforms 14
- OmniAccess Mobility Controller Platforms 14
- AP Platforms 14

End-of-Support 17

Regulatory Updates 18

Resolved Issues 19

Known Issues 23
- Limitations 23
- Known Issues 23

Upgrade Procedure 27
- Important Points to Remember 27
- Memory Requirements 27
- Low Free Flash Memory 28
- Backing up Critical Data 31
- Upgrading AOS-W 32
- Verifying the AOS-W Upgrade 33
- Downgrading AOS-W 34
- Before Calling Technical Support 36

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 04	Updated the maximum MTU size to 2500 bytes in **Support for Jumbo Lite Frames** under the **What's New** chapter.
Revision 03	The following bugs were added to the list of Known Issues: ■ AOS-227404 ■ AOS-228058 ■ AOS-228284 ■ AOS-232181
Revision 02	This revision introduces the following changes: ■ Added limitation on **IP Default-Gateway Management Address** in Known Issues. ■ Updated the statement in **End-of-Support** chapter.
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

Related Documents

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

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

Supported Browsers

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

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

Important

As mandated by the Wi-Fi Alliance, AOS-W 8.10.0.0 requires Hash-to-Element (H2E) for 6 Ghz WPA3-SAE connections. H2E is supported only on Windows 11, Linux wpa_supplicant version 2.10 and later versions. Hence, users must upgrade their Windows and Linux software for successful 6 Ghz WPA3-SAE connections.

Terminology Change

As part of advancing Alcatel-Lucent Enterprise's commitment to racial justice, we are taking a much-needed step in overhauling ALE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against

specific groups of people. Such content is not representative of our ALE culture and moving forward, ALE will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

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

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

New Features and Enhancements in AOS-W 8.10.0.0

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

9240 Controller Platform

The Alcatel-Lucent 9240 controller is a wireless LAN controller that connects, controls, and intelligently integrates wireless Access Points (APs) and Air Monitors (AMs) into a wired LAN system. The controller has advanced IDS functionality and mobility services that is integrated with per user based enforcement policies for better security. The controller has the following port configurations:

- 4 x SFP28 1G/10G/25G data ports
- 1 x RJ45 serial console access port
- 1 x USB Type-C console port for direct local access
- 1 x out-of-band management port
- 2 x USB 3.0 interfaces
- 1 x expansion slot reserved for future use

The Alcatel-Lucent 9240 switch supports capacity licensing. The license types are as follows:

- **Base model** - Base license
- **Silver** - Mid-range license
- **Gold** - Top range license

The following table lists the major differences in the license types supported on the Alcatel-Lucent 9240 switch:

Table 3: *License Types*

Feature	Base Model	Silver	Gold
Number of Access Points	512	1024	2048
Number of Devices	16,384	24,576	32,768
GRE Tunnels	8,704	17,408	34,816
Concurrent IPsec sessions	16,384	24,576	32,768
Route Cache Entries	23,764	65,532	119,343
Wired throughput (Gbps)	20	30	40

For complete technical details and installation instructions, see Alcatel-Lucent 9240 controller Installation Guide.

Support for 580 Series Outdoor AP Platforms

The Alcatel-Lucent 580 Series access points (AP-584, AP-585, AP-585EX, AP-587, and AP-587EX) are high performance, dual-radio, outdoor access points that can be in either controller-based (AOS-W) or controller-less (Aruba Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi functionality with MIMO radios (4x4 in 2.4 GHz and 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Additional features include:

- Support for high power BLE.
- Support for 10G SFP+ (SX and LX) and 1G (SX and LX).
- Support for 1G PSE Out.
- Support for GPS.
- Support for AC power over new Molex connector kit.
- AP-584 access points with external antennas.
- AP-585 and AP-585EX access points with internal omni-directional antennas.
- AP-587 and AP-587EX access points with internal directional antennas.
- Mesh.
- Wi-Fi uplink.

For complete technical details and installation instructions, see Alcatel-Lucent 580 Series *Access Points Installation Guide*.

Support for 650 Series OAW-AP Platforms

The Alcatel-Lucent 650 Series access points (AP-655) are high performance, tri-radio, indoor access points that can be deployed in either switch-based (AOS-W) or switch-less (Aruba Instant) network environments. These APs deliver high performance concurrent 2.4 GHz, 5 GHz, and 6 GHz 802.11ax Wi-Fi (Wi-Fi 6E) functionality with MIMO radios (4x4 in 2.4 GHz, 5 GHz, and 6 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services.

Additional features include:

- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point
- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor
- Two Ethernet ports, ENET0 and ENET1, each capable of data rates up to 5 Gbps
- Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports
- Mesh
- Thermal management

The 650 Series access points have the following limitations:

- No spectrum analysis
- No Zero-Wait DFS
- Maximum number of associated clients is 512
- Maximum of 4 virtual APs for 6 GHz radio

For complete technical details and installation instructions, see Alcatel-Lucent *650 Series Access Points Installation Guide*.

Support for New Alcatel-Lucent USB LTE Modem

AOS-W supports a new Alcatel-Lucent USB LTE modem for OAW-RAPs. The USB modem plugs directly into the USB port of the OAW-RAPs, and supports plug-and-play to provision the modem for both 3G and 4G networks on the OAW-RAPs as backup or primary WAN uplink.

Advertise Wide Bandwidth Information Element in Neighbor Report Responses

A new setting called **Advertise Wide Bandwidth IE in Neighbor Report Responses** is added to the 802.11k profile configuration to include wide channel bandwidth information element in the neighbor report responses. This setting is enabled by default in the WebUI. This feature can be configured in the CLI by using the **nb-resp-wide-band-ie** parameter in the **wlan dot11k-profile** command.

Command Support for AP Antenna Detection on Wi-Fi 6E APs

AOS-W supports the **show ap antenna status** command for Wi-Fi 6E APs (630 Series and 650 Series access points).

Command Support for U-Blox GPS Receiver

AOS-W supports the **gps** command to enable or disable the U-Blox GPS receiver in APs and the **show ap gps** command to view the status of the GPS receiver.

Configuring IoT Antenna Gain Value

The following CLI parameters are introduced to configure an antenna gain value for IoT devices:

- A new CLI parameter **iot-ant-gain** is introduced in the **provision-ap** command to configure an antenna gain value for APs with external antennas.
- A new parameter called **action iot-ant-gain** is introduced in the **ap provisioning-rule** command. This command is available only in the Mobility Conductor.

Display Client Kickout Occurrences on APs

The **show ap debug client-kickout-logs** command is introduced to display detailed information on the last 12 occurrences of the client deauthentication logs. This occurs due to consecutive Tx failures in 530 Series, 550 Series, 630 Series, and 650 Series access points.

Display LLDP Neighbor Chassis ID / Port ID during AP Provisioning

The WebUI now displays LLDP Neighbor Chassis ID / Port ID while provisioning an AP.

DRT support for BLE and 802.15.4 Introduced in New Access Points

The output of the **show ap debug received-reg-table** command will now display the DRT information for BLE and 802.15.4 standard for 580 Series access points.

Enhancements to AirGroup

Starting with AOS-W 8.10.0.0, AirGroup version 2 is enabled by default and AirGroup version 1 is not available. AirGroup version 2 introduces the following changes:

- Auto-associate AP name is enabled by default. Any configuration related to auto-associate AP name that was done before the upgrade to AOS-W 8.10.0.0 will be retained. But, if auto-associate is not configured before the upgrade to AOS-W 8.10.0.0, then auto-associate AP name will be enabled automatically after the upgrade to AOS-W 8.10.0.0. An AirGroup user will see AirGroup servers only in the vicinity of the AP name.
- Wired servers are added to managed device-tagged, cluster-tagged, or untagged list. Wired servers in the untagged list cannot be discovered. Wired servers in the untagged list do not have a unique managed device or cluster location and:
  - If a ClearPass Policy Manager policy is present, it will be applied.
  - A managed device-tagged wired server will be visible to AirGroup users connected the same managed device.
  - A cluster-tagged wired server will be visible to AirGroup users connected to the same cluster.

Enhancements to Default Gateway for dedicated OOB Management

The **ip default-gateway** command is modified to configure the default gateway for dedicated OOB management Ethernet port on OAW-40xx Series switches.

Enhancements to Dump Collection

The AOS-W WebUI is modified to allow users to regulate the core dump files sent to the managed device. The **transfer-enable** sub-parameter was added to the **dump-collection-profile** parameter to enable APs to transfer the core dump.

Enhancements to IPM

Additional reduction steps are introduced in the **ap-system profile <name>ipm-power-reduction-step-prio ipm-step** command to reduce the power consumption and the operating temperature of the AP when IPM is enabled.

Exporting IDS Logs from WebUI

Starting with AOS-W 8.10.0.0, user has the option of exporting IDS logs as a CSV file from the WebUI for Detected Clients, Detected Radios, Events, and Denylist tables.

Enhancement to Multiversion Support

Multiversion is now supported for a Mobility Conductor that is running AOS-W 8.10.0.0 version and the managed devices are running either AOS-W 8.6.0.0, AOS-W 8.7.0.0, AOS-W 8.8.0.0, AOS-W 8.9.0.0, or AOS-W 8.10.0.0 version.

Enhancements to the show mon-serv-mesh-tbl-entry command

The **6G** parameter has been added to the **show mon-serv-mesh-tbl-entry** command to display the entries of 6 GHz radio band.

Enhancements to RRE IM Profile configuration

The **Import** option in the **Configuration > System > Profiles > All Profiles > RF Management > 6 GHz radio > RRM IE Settings for 6GHz** page of the WebUI allows you to copy the configuration parameters of an existing WLAN RRM IE profile.

Enhancement to Tx Power Value for IoT BLE or Zigbee Radio Profile

The maximum configurable value of Tx power for BLE and Zigbee-based radio profiles is increased from -40 to 20.

Ghost Tunnel Attack Detection

AOS-W allows detection of ghost tunnel attacks on both the server side and client side. A ghost tunnel attack is a backdoor transmission method that can be used in an isolated environment. A ghost tunnel attack does not use 802.11 probe request packets or beacon packets to communicate and does not need to establish a Wi-Fi connection.

Grouping Firewall Sessions for Managed Devices

AOS-W allows grouping of policy enforcement firewall visibility sessions for managed devices based on the same BSSID.

Handling Over Current in AP's USB Port

Starting from AOS-W 8.10.0.0, the AP's USB port will now automatically shut down if the temperature of the port reaches 125°C. This helps to prevent short circuits on USB ports. This feature is available by default on all Alcatel-Lucent 500 Series, 500H Series, 510 Series, 530 Series, 550 Series, 630 Series , 650 Series access points.

Increase in the RADIUS server authentication timeout value

Starting from AOS-W 8.10.0.0, the maximum timeout value for RADIUS server authentication has been increased from 30 seconds to 120 seconds.

Increase in the Username and Password Character Limit for Management Authentication

Currently, the maximum character count for username and password in management authentication is 32. Starting from AOS-W 8.10.0.0. the character count has been increased to 128.

Long Supported Release

AOS-W 8.10.0.0 is now a Long Supported Release (LSR). The WebUI, CLI, and SNMP commands reflect this update. An LSR extends support for patches up to five years. A Short Supported Release (SSR) extends support for patches up to two years.

Postquantum Preshared Key (PPK)support for IKEv2

Postquantum Preshared Key (PPK) support is added to IKEv2. It is limited to site-to-site VPNs.

VIA Client Count in WebUI

Starting with AOS-W 8.10.0.0, count of VIA clients is displayed in the **Dashboard > Overview** page.

Revised Scaling Capacity of Alcatel-Lucent OAW-4750 switches

Starting from AOS-W 8.10.0.0, the scaling capacity of Alcatel-Lucent OAW-4750 switches has been reduced to that of Alcatel-Lucent OAW-4650 switches. The scaling capacity of Alcatel-Lucent OAW-4750XM switches has not been revised.

Allow Search Based on Special Characters in Device Name

Starting from AOS-W 8.10.0.0, you will be able to search, sort, and filter APs, switches, and client devices even when they have special characters such as +, *, &, %, $, #, etc.

Separate Band-Steer for 5 GHz and 6 GHz Radios

ClientMatch supports separate band-steer for 5 GHz and 6 GHz capable clients on Wi-Fi 6E APs. If band-steer to 5 GHz radio fails multiple times for a client that is both 5 GHz and 6 GHz capable, the client is marked as unsteerable for band-steer to 5 GHz radios only.

SES-Imagotag and Wi-Fi Co-Existence Support for Wi-Fi 6 and Wi-Fi 6E Access Points

AOS-W now supports SES-Imagotag and Wi-Fi Co-existence for Wi-Fi 6 and Wi-Fi 6E access points.

Support for 802.11mc Fine Timing Measurement on Wi-Fi 6E APs

AOS-W supports 802.11mc Fine Timing Measurement feature on Wi-Fi 6E APs (630 Series and 650 Series access points).

Support for AirMatch Mode Aware

AOS-W supports AirMatch mode aware to optimize the use of 2.4 GHz radios in dense RF environment. In a high-density RF environment, multiple 2.4 GHz radios may cause interference. With the mode aware feature, AirMatch converts some of the 2.4 GHz radios to monitoring mode keeping coverage for all the bands at priority. The mode aware feature allows dynamic optimization of the RF environment.

Support for BSC Computer Version of the EnOcean USB Dongle

AOS-W Instant now supports the BSC computer version of the EnOcean USB dongle.

Support for Alcatel-Lucent Certification

A new parameter **Aruba Certified** is introduced in the output of the **show interface gigabitethernet <slot/module/port> transceiver** command. This parameter shows if the Small Form-factor Pluggable (SFP) transceiver is certified by Alcatel-Lucent.

Support for DigiCert Global G2 root CA certifications

AOS-W now supports DigiCert Global G2 root CA certifications for Azure IoTHub and DPS connection.

Support for EN302502 and EN301893 in UNI3 Bands

The AP-374 outdoor access point supports EN302502 and EN301893 for DFS in UNI3 bands. Support for EN302502 allows the usage of higher power in the UNI3 band in ETSI and support for EN301893 allows radar detection.

Support for Flash EIRP Limit on 6 GHz bands

AOS-W supports the Flash EIRP limit for U-NII channels of 6 GHz bands on Wi-Fi 6E APs.

Support for Higher Cipher for SSH

Starting with AOS-W 8.10.0.0, support for rsa-sha2-256 and higher ciphers is added for the SSH protocol.

Support for Hypervisor Version 7.0

AOS-W can now be installed using VMware ESXi version 7.0.

Support for Jumbo Lite Frames

Starting from AOS-W 8.10.0.0, the Jumbo Lite frames are now supported in IPv4 and IPv6 networks. IPsec site-to-site tunnels for the virtual mobility controllers (VMC)s now support the Jumbo Lite frames that allow the VMCs to forward data frames over IPsec site-to-site tunnels that are larger than 1500 bytes without fragmentation. In IPv6 site-to-site tunnels, the minimum MTU size is 1280 bytes. When a user configures the MTU size with a value less than 1280 bytes, the IPv6 tunnels will use an MTU size of 1280 bytes. For non-VMC platforms, the maximum MTU size is limited to 2500 bytes.

Support for Wi-Fi Uplink on Wi-Fi 6E APs

AOS-W supports Wi-Fi uplink feature on Wi-Fi 6E APs (630 Series and 650 Series access points) for 2.4 GHz and 5 GHz radio bands only.

Support Sort and Filter Capabilities in Detected Radios

AOS-W supports sorting and filtering capabilities on the following columns in the **Dashboard > Security > Detected Radios** page.

- Bandwidth
- Secondary Channel
- Confidence Level
- Encryption
- Discovered Time
- Match Time
- Match AP/Rule

Telemetry Manager Process

Starting from AOS-W 8.10.0.0, a new process named Telemetry Manager(TM) has been introduced to offload the management interfaces, AMON and MON from the station management process(STM).

VLAN support for Wireless Clients

A new parameter **VLAN** is introduced in the **Customize Column** for the Wireless Clients on **Dashboard > Overview** page.

ZBOSS Database

The ZigBee Open Source Stack (ZBOSS) database in AOS-W is upgraded to version 3.5.1.0.

Behavioral Changes

This release does not introduce any changes in AOS-W behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.10.0.0.

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 4: *Supported Mobility Conductor Platforms*

Mobility Conductor Family	Mobility Conductor Model
Hardware Mobility Conductor	MCR-HW-1K, MCR-HW-5K, MCR-HW-10K
Virtual Mobility Conductor	MCR-VA-50, MCR-VA-500, MCR-VA-1K, MCR-VA-5K, MCR-VA-10K

OmniAccess Mobility Controller Platforms

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

Table 5: *Supported OmniAccess Mobility Controller Platforms*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
OAW-41xx Series OmniAccess Mobility Controllers	OAW-4104, 9012
9200 Series OmniAccess Mobility Controllers	9240
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 6: *Supported AP Platforms*

AP Family	AP Model
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H

Table 6: *Supported AP Platforms*

AP Family	AP Model
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, AP-303HR
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, 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
370EX Series	AP-375EX, AP-377EX, AP-375ATEX
OAW-AP387	OAW-AP387
500 Series	OAW-AP504, OAW-AP505
500H Series	AP-503H, AP-503HR, AP-505H, AP-505HR
510 Series	OAW-AP514, OAW-AP515, AP-518
518 Series	AP-518
530 Series	OAW-AP534, OAW-AP535
550 Series	OAW-AP555

Table 6: *Supported AP Platforms*

AP Family	AP Model
560 Series	AP-565, AP-567
570 Series	AP-574, AP-575, AP-577
580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX
630 Series	AP-635
650 Series	AP-655

Chapter 5
End-of-Support

This chapter provides information on the Alcatel-Lucent products that are not supported for a particular release.

AOS-W 8.10.x.x is the last release that supports the following AP platforms:

- 200 Series
- OAW-AP203H Series
- OAW-AP203R Series
- OAW-AP205H Series
- OAW-AP207 Series
- 210 Series
- 220 Series
- OAW-AP228 Series
- 270 Series
- 320 Series
- 330 Series
- OAW-AP340 Series
- OAW-AP387

Chapter 6
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_83672

Chapter 7
Resolved Issues

This chapter describes the resolved issues in this release.

Table 7: *Resolved Issues in AOS-W 8.10.0.0*

New Bug ID	Description	Reported Version
AOS-210845 AOS-217214 AOS-219154 AOS-220187 AOS-221165 AOS-226266	OAW-AP535 and OAW-AP555 access points running AOS-W 8.6.0.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.6
AOS-211699 AOS-212564 AOS-212567 AOS-212599 AOS-215978 AOS-217452 AOS-229376	A few APs running AOS-W 8.5.0.10 or later versions crashed unexpectedly. The log file listed the reason for the crash as **Kernel panic - not syncing: jiffies stall (pc is at __ schedule+0x78/0x360)**. The fix ensures that the APs work as expected.	AOS-W 8.5.0.10
AOS-218873 AOS-230672	High SAPD memory utilization was observed and hence, APs dropped DHCP packets. This issue was observed in non-6GHz APs. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.9.0.1 or later versions.	AOS-W 8.9.0.1
AOS-220107 AOS-220109 AOS-223713	The PHY link was unusable and Tx CRC error was displayed on Eth1. This issue occurred when the Eth1 link speed was changed from auto to 1000 or 100 when Eth0 was working at 2.5 Gbps. This issue was observed in AP-635 access points running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-220190 AOS-223094 AOS-224240 AOS-224792 AOS-226989 AOS-228434	A few users were unable to login to the captive portal page that was hosted on ClearPass Policy Manager server. This issue occurred when the netdestination ID, which was added to the captive portal allowlist, was incorrectly changed to 0 after a reboot of the Mobility Conductor Virtual Appliance. This issue was observed in Mobility Conductor Virtual Appliances running AOS-W 8.5.0.10 or later versions.	AOS-W 8.6.0.9
AOS-220748	In CLI, when you search for `config`, the first character did not appear until the next character was typed. This issue was observed in Mobility Master and managed devices running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-221126 AOS-224948	Users were unable to upgrade the switch when the **Local File** option was selected for the **Upgrade Using** field in the **Maintenance > Software Management > Upgrade** page of the WebUI. The fix ensures that the WebUI allows for an upgrade using the local file. This issue was observed in Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0

Table 7: *Resolved Issues in AOS-W 8.10.0.0*

New Bug ID	Description	Reported Version
AOS-221676 AOS-221961 AOS-222865 AOS-224926	A few clients connected on the 6 GHz channel were deauthenticated. The log file listed the reason for the event as **Wlan driver wireless client out of range (seq num 0)**. This issue was observed in AP-635 and AP-655 access points running AOS-W 8.9.0.0 or later versions. The fix ensures that the APs work as expected.	AOS-W 8.9.0.0
AOS-221798	A few Mobility Controller Virtual Appliances running AOS-W 8.4.0.0-FIPS or later versions were unable to route jumbo data packets even though the jumbo frames were enabled. This issue was observed in vSphere Hypervisor running 6.7 or later versions. The fix ensures that the Mobility Controller Virtual Appliances are able to route the jumbo data packets.	AOS-W 8.8.0.0-FIPS
AOS-222152	A few clients faced connectivity issues. This issue occurred due to a race condition where the PHY mode of the initially configured virtual AP was incorrectly applied to all the other virtual APs. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-W 8.6.0.10 or later versions.	AOS-W 8.6.0.10
AOS-222203 AOS-228442	OAW-AP505 access points running AOS-W 8.6.0.8 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the crash as **Panic: Out of memory Warm-reset during throughput test in Lab environment**. The fix ensures that the APs work as expected.	AOS-W 8.6.0.8
AOS-222885	The **show datapath frame** counters and **show datapath error counters** commands did not display the **Jumbo Discards** counter even when the jumbo packets were dropped. Issue the **show port stats debug xstats** command to view all the NIC counter related details. This issue was observed in OAW-4104 switches running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-222971	The configuration commands **airgroup active-domain**, **airgroup cppm-server aaa**, **airgroup cppm-server query-interval**, and **airgroup domain** did not work as expected. The commands **show airgroup cppm-server aaa**, **show airgroup effective profiles** and **show airgroup policy-entries** failed to display any output. The fix ensures that the commands are removed and the CLI message **This command is deprecated** is displayed only on the specific and applicable node paths for which the command is valid. This issue was observed in managed devices running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-223903	A Mobility Conductor did not accept applying a valid XML file that was generated in Python for IPv6 relay-option and IPv4 option 82. The Mobility Conductor displayed the error message, **Filename <sample.xml> has invalid keywords**. This issue was observed in a Mobility Conductor running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-224081 AOS-224083 AOS-225940	The **Dashboard** > **Overview** > **WLANs** page displayed incorrect value under **Usage** column in the WebUI. The fix ensures that the WebUI displays the correct value under **Usage** column. 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

Table 7: *Resolved Issues in AOS-W 8.10.0.0*

New Bug ID	Description	Reported Version
AOS-224632 AOS-231802	The AirGroup server table did not display the list of wired servers. This issue occurred after enabling the multicast aggregation. The fix ensures that the AirGroup feature works as expected. This issue was observed in Mobility Conductors running AOS-W 8.9.0.0 or later versions.	AOS-W 8.9.0.0
AOS-224688	The HE enabled APs were incorrectly displayed as HTT None in OmniVista 3600 Air Manager. The fix ensures that the status of the APs are correctly updated in OmniVista 3600 Air Manager. This issue was observed in APs running AOS-W 8.7.1.1 or later versions.	AOS-W 8.7.1.1
AOS-224867	A rsync failure occurred on a managed device. This issue occurred during boot when the DHCP process wrongly derived the switch IP as IP address of the Mobility Conductor. The IP address of the Mobility Conductor was subsequently configured as a FQDN in configuration. This issue was observed in a managed device running AOS-W 8.9.0.0.	AOS-W 8.9.0.0
AOS-225174	In addition to BGP control frames and other routing control packets, when the Alcatel-Lucent VPNC 7240XM switch running AOS-W 8.6.0.4 received high number of TTL=1 packets, the cumulative rate of these frames exceeded the policed rate in the bandwidth contract and resulted in frame drops. These dropped frames were seen on the VPNC port, but not in the control path capture. This issue was observed in Alcatel-Lucent 7240XM controllers running AOS-W 8.6.0.4 or later versions.	AOS-W 8.6.0.4
AOS-225508	A few managed devices running AOS-W 8.6.0.16 or later versions in a Mobility Conductor-Managed Device topology sent ARP requests with an incorrect MAC address. The fix ensures that the managed devices do not send ARP requests with an incorrect MAC address.	AOS-W 8.7.1.4
AOS-225704	A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c) (nanny memory leak).** This issue occurred when the **Nanny** process leaked memory. The fix ensures that the **Nanny** process does not leak memory and works as expected. This issue was observed in Managed Devices running AOS-W 8.8.0.0.	AOS-W 8.8.0.0
AOS-226320	Some users were unable to perform 802.1X authentication when a few host IP addresses were removed from the netdestination list. This issue was resolved by enabling EAP-TLS fragmentation in the 802.1X authentication profile. This issue was observed in managed devices running AOS-W 8.6.0.10 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.6.0.10
AOS-227016 AOS-229420	The VIA application took longer time to download a VPN profile. The fix ensures that the VIA application downloads the VPN profile over non-blocking PAPI sockets. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.6.0.9

Table 7: *Resolved Issues in AOS-W 8.10.0.0*

New Bug ID	Description	Reported Version
AOS-228319	Some OAW-AP535 access points running AOS-W 8.7.1.6 or later versions crashed unexpectedly. The log file listed the reason for the event as **FW Exception :Excep :0 Exception detected, Thread ID: 0x00000069 Thread name : WLAN BE**. The fix ensures that the APs work as expected.	AOS-W 8.7.1.6
AOS-229351	Users were unable to disable the AirGroup profile. This issue occurred when the AirGroup profile was disabled in the parent node and then was disabled again in the child node. The fix ensures that the AirGroup feature works as expected. This issue was observed in Mobility Conductors running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-229901	The VIA web authentication welcome page displayed incorrect Windows OS processor. The fix ensures that the VIA web authentication page displays the correct Windows OS processor. This issue occurred because the VIA web authentication welcome page incorrectly detected 32-bit Windows OS processor whereas the user had 64-bit Windows OS processor and web browser. This issue was observed in managed devices running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-230210	A managed device did not cache the entries and displayed the **Module DPAGENT_PORT is busy. Please try later** error when the **show datapath web-cc https-deny-cache** command was issued. The fix ensures that the **show datapath web-cc https-deny-cache** command works as expected. This issue was observed in a managed device running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-232176	Some OAW-4104 switches running AOS-W 8.7.1.9 experienced datapath timeout. This issue occurred when the tunnel MTU was configured with a value lesser than 1280 for IPv6 managed devices. The fix ensures that the OAW-4104 switches work as expected.	AOS-W 8.7.1.9
AOS-230563	The proxy configuration of the Azure-IoTHub did not work as expected. The fix ensures that the proxy configuration works as expected. This issue was observed in Mobility Conductors running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0

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

Limitations

Following are the limitations observed in this release.

IP Default-Gateway Management Address

Alcatel-Lucent recommends to not configure the IP default-gateway management address for 7010, 7024, 7205, and OAW-4850 switches running AOS-W 8.10.0.0.

AP-635 and AP-655 Access Points

AP-635 and AP-655 access points do not support Wi-Fi uplink on the 6 GHz radio channel.

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
```

No Support for 6 GHz Radio Band and WPA3-PSK-H2E in Wi-Fi Uplink

The Wi-Fi Uplink feature does not support 6 GHz radio band and WPA3-PSK-H2E encryption type for Wi-Fi 6E APs (630 Series and 650 Series access points).

AirSlice

AirSlice is disabled for 500 Series and 510 Series access points and enabled for 530 Series, 550 Series, and 630 Series access points.

Known Issues

Following are the known issues observed in this release.

Table 8: *Known Issues in AOS-W 8.10.0.0*

New Bug ID	Description	Reported Version
AOS-218844 AOS-222351 AOS-227400 AOS-231009	Mobility Conductor picks only 43% of the APs for cluster CRU. This issue is observed in Mobility Conductor running AOS-W 8.8.0.0 or later versions.	AOS-W 8.8.0.0
AOS-227404	After a reboot of the Mobility Conductor Virtual Appliance, the route cache entries for IPsec tunnel display the MAC address as 0. This issue is observed in L3 connected Mobility Conductor Virtual Appliances running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-227804	The AirMatch mode-aware feature takes all the APs, including dual-band and tri-band APs, into consideration, but post computation it considers only the dual-band APs and excludes the tri-band APs. This issue is observed in a managed device running AOS-W 8.10.0.0	AOS-W 8.10.0.0
AOS-228058	AOS-W WebUI does not allow users to configure MTU size as 2500 for IPsec tunnels. This issue is observed in Mobility Conductors running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-228065	The **Dashboard** > **Overview** page of the WebUi display 0 for VLAN. This issue is observed in Mobility Conductors running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-228149	When the number of wired devices tagged to the managed device is more than 100, the wired devices are not flagged after activating the cluster. This issue is observed in a managed device running AOS-W 8.10.0.0 in a cluster setup.	AOS-W 8.10.0.0
AOS-228284	IPv6 reassembly failure is observed when packet size is greater than the tunnel MTU. This issue is observed in Mobility Conductors running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-228764	A few AP-655 access points running AOS-W 8.10.0.0 crash and reboot unexpectedly. The log files list the reason for the event as **PC is at cnss_wait_for_cold_boot_cal_done+0xe0/0x124**.	AOS-W 8.10.0.0
AOS-229094	A few wired servers are incorrectly marked with more than one flag in the output of the show---command. This issue occurs when ADP table does not get updated with the details of the VLAN. This issue is observed in managed devices running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-229559	A wrong policy may be enforced when a combination of DPI application-based rules and WebCC-based policies are used. This issue is observed in a managed device running AOS-W 8.7.0.0.	AOS-W 8.7.0.0
AOS-229758	Clients are unable to obtain the IP address or forward traffic. This issue occurs when WPA2-PSK-AES and WPA-PSK-TKIP opmodes are used in decrypt-tunnel mode. This issue is observed in APs running AOS-W 8.10.0.0.	AOS-W 8.10.0.0

Table 8: *Known Issues in AOS-W 8.10.0.0*

New Bug ID	Description	Reported Version
AOS-231206	The **wpa3_sae process** crashes or is stuck in **PROCESS_NOT_ RESPONDING_CRITICAL** state. This issue occurs due to timer corruption. However, this issue does not affect the connectivity of already connected clients. This issue is observed in managed devicesrunning AOS-W 8.6.0.17 or later versions.	AOS-W 8.6.0.17
AOS-231454	The show commands display an error message, **auth module busy**. This issue occurs when large number of netdestination configurations are added. This issue observed in OmniAccess Mobility Controllers running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-231490	Dynamic packet capture fails to generate the pcap file. This issue occurs when WPA3-SAE encryption is used. This issue is observed in OAW-AP505 and OAW-AP515 access points running AOS-W 8.7.1.9 or later versions.	AOS-W 8.7.1.9
AOS-231769	The downlink MU-MIMO transmission with negative gains are observed for Samsung S21 devices in 160 MHz channel. This issue is observed in APs running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-231849	Mesh Portal APs do not change channels even after AirMatch changes the channels. This issue is observed in APs that have only mesh vaps configured. This issue is observed in APs running AOS-W 8.6.0.16 or later versions. **Workaround:** Configure a **wlan virtual-ap profile <name>** to resolve the issue.	AOS-W 8.6.0.16
AOS-232049	AirGroup traffic fails to reach the **MDNS** process on Mobility Conductors running AOS-W 8.10.0.0 in a Mobility Conductor-Managed Device topology. This issue occurs when the AirGroup traffic hits the **any any any permit** datapath ACL that appears before the OpenFlow ACL.	AOS-W 8.10.0.0
AOS-232181	Some APs do not form GRE tunnels with the Mobility Conductor Virtual Appliances on ESXi hypervisor and the MTU size falls back to 1578 bytes. This issue occurs when the MTU size of the jumbo tunnels is set to 9000 bytes. This issue is observed in APs running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-232331	The AP multicast aggregation tunnel packets on managed devices do not reach the **MDNS** process on Mobility Conductors running AOS-W 8.10.0.0. This issue occurs when the reboot of **STM** process on the **managed devices** changes the AP multicast aggregation tunnel ID, and the change is not detected by OpenFlow.	AOS-W 8.10.0.0
AOS-232463	The **Remote Clients** table under **Dashboard** > **Overview** > **Clients** page in the WebUI displays incorrect value of client age under the **Age** column. This issue is observed in managed devices running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-232503	A few APs do not accept action messages and this results in random channel and power assignments. This issue occurs when the opmode is changed from Dual-band to Dual-5G. This issue is observed in APs running AOS-W 8.10.0.0.	AOS-W 8.10.0.0

Table 8: *Known Issues in AOS-W 8.10.0.0*

New Bug ID	Description	Reported Version
AOS-232606	The WebCC classification fails in centralized mode in a native IPv6 deployment. This issue is observed in Mobility Conductors and managed devices running AOS-W 8.9.0.1 or later versions in a Mobility Conductor-Managed Device topology.	AOS-W 8.10.0.0
AOS-232614	The multicast aggregation message, **stm_send_split_tunnel_status_to_mdns** is not sent to the **OFA** process. This issue occurs due to incorrect endianness. This issue is observed in OAW-41xx Series switches running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-232623	Multiple APs are incorrectly marked as forwarder on the same VLAN. This issue is observed in APs running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-232699	A mesh portal is converted into AAM mode and the radios in mesh points are disabled. This issue occurs when the AirMatch mode-aware feature is enabled. This issue is observed in APs running AOS-W 8.10.0.0	AOS-W 8.10.0.0
AOS-232757	A BLE southbound API connection is terminated when the characteristic discovery is interrupted. This issue is observed in a managed device running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-233010	The 2.4 GHz radio of an AP does not turn off in accordance with the AirMatch mode-aware decision. The log on the OmniAccess Mobility Controller shows that the AP is in AAM mode but the log on the managed device shows that the AP has not moved into AAM mode. This issue is observed in APs running AOS-W 8.10.0.0.	AOS-W 8.10.0.0
AOS-233098	Controller-generated traffic is always forwarded through the management port instead of the data port. This issue occurs when the IP default-gateway management address is configured in switches. This issue is observed in 7010, 7024, 7205, and OAW-4850 switches running AOS-W 8.10.0.0. **Workaround:** Alcatel-Lucent recommends to not configure the IP default-gateway management address for 7010, 7024, 7205, and OAW-4850 switches running AOS-W 8.10.0.0.	AOS-W 8.10.0.0

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 Master, managed device, or stand-alone switch.

Important Points to Remember

To upgrade your managed device or Mobility Master:

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

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 31 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 31 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 31 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

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 9 for all supported switch models:

   Table 9: *Flash Memory Requirements*

Upgrading from	Upgrading to	Minimum Required Free Flash Memory Before Initiating an Upgrade
8.3.x	8.9.x	360 MB
8.5.x	8.9.x	360 MB
8.6.x	8.9.x	570 MB
8.7.x	8.9.x	570 MB
8.8.x	8.9.x	450 MB
8.9.x	8.9.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 9, 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 9
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        : ArubaOS 8.9.0.0 (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        : ArubaOS 8.7.0.0-2.3.1.0 (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 8.9.0.0.

```
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 9.

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading AOS-W

Upgrade AOS-W using the WebUI or CLI.

CAUTION

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

NOTE

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

In the WebUI

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

1. Download the AOS-W image from the customer support site.
2. Upload the AOS-W image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-W image:
   a. Download the **Alcatel.sha256** file from the download directory.
   b. Load the AOS-W image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the customer support site.

NOTE

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

4. Log in to the AOS-W WebUI from the Mobility Master.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

NOTE

The upgrade does not take effect until reboot. If you chose to reboot after upgrade, the Mobility Master or managed device reboots automatically.

9. Select **Save Current Configuration**.
10. Click **Upgrade**.
11. Click **OK**, when the **Changes were written to flash successfully** message is displayed.

In the CLI

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

1. Download the AOS-W image from the customer support site.
2. Open an SSH session to your Mobility Master.
3. Execute the **ping** command to verify the network connection between the Mobility Master and the SCP server, FTP server, or TFTP server.

```
(host)# ping <ftphost>
```

or

```
(host)# ping <tftphost>
```

or

```
(host)# ping <scphost>
```

4. Execute the **show image version** command to check if the AOS-W image is loaded on the flash partition. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

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

5. Execute the **copy** command to load the new image to the non-boot partition.

```
(host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

6. Execute the **show image version** command to verify that the new image is loaded.

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

7. Reboot the Mobility Master.

```
(host)#reload
```

8. Execute the **show version** command to verify that the upgrade is complete.

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

Verifying the AOS-W Upgrade

Verify the AOS-W upgrade in the WebUI or CLI.

In the WebUI

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

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

2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 31 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the AOS-W image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 31 for information on creating a backup.

Downgrading AOS-W

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

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 31.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade AOS-W version.

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

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

Downgrade AOS-W version using the WebUI or CLI.

In the WebUI

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

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. From **Select destination file** drop-down list, select **Flash file system**, and enter a file name (other than default.cfg).
   c. Click **Copy**.
2. Determine the partition on which your pre-upgrade AOS-W version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade AOS-W version is not stored on your system partition, load it into the backup system partition by performing the following steps:

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot Controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, and click **Reboot**.

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

In the CLI

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

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

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

   or

   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the Mobility Master or managed device to boot with your pre-upgrade configuration file.

   (host) # boot config-file `<backup configuration filename>`
3. Execute the **show image version** command to view the partition on which your pre-upgrade AOS-W version is stored.

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

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

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

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