HPE Aruba Networking Wireless Operating System 8.10.0.16 Release Notes

Hewlett Packard Enterprise

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

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-8 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-8.10.0.6 or earlier versions on 9000 Series and 9200 Series controllers 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 controller unusable. Please use caution and plan accordingly.

Cluster Rolling Upgrade is not supported when a BIOS upgrade is required. AOS-8 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-8.10.0.0 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-8.9.0.0 or later versions use **aruba-conductor** as the host name instead of **aruba-master** to identify a target managed device or stand-alone controller during DNS discovery. However, the factory-default image of APs that were introduced prior to AOS-8.9.0.0 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 Aruba user-centric network:

- *AOS-8 Getting Started Guide*
- *AOS-8 User Guide*
- *AOS-8 CLI Reference Guide*
- *AOS-8 API Guide*
- *Aruba Mobility ConductorLicensing Guide*
- *Aruba Virtual Appliance Installation Guide*

- *Aruba AP Software Quick Start Guide*

Supported Browsers

The following browsers are officially supported for use with the AOS-8 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 HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE 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 HPE culture and moving forward, Aruba 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*

Main Site	arubanetworking.hpe.com
Support Site	networkingsupport.hpe.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200

International Telephone	arubanetworks.com/support-services/contact-support
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins Email: aruba-sirt@hpe.com

Chapter 3
What's New in AOS-8.10.0.16

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

Chapter 4
Supported Platforms

This section displays the supported platforms in AOS-8.x. The **minimum version supported** column displays the minimum AOS-8.x version that can be run on a platform. The **latest version supported** column displays the newest AOS-8.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-8.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

Mobility Controller Platforms

Mobility Controllers		**AOS-8.x Versions Supported**	
Controller Family	**Controller Model**	**Minimum**	**Latest**
9200 Series	9240	8.10.0.x	8.12.0.x
9000 Series	9012	8.7.0.x	8.12.0.x
	9004	8.5.0.x	8.12.0.x
7200 Series	7280	8.3.0.x	8.12.0.x
	7205, 7210, 7220, 7240, 7240XM	8.0.0.x	8.12.0.x
7000 Series	7005, 7008, 7010, 7024, 7030	8.0.0.x	8.12.0.x
Virtual 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-8.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
	650 Series	AP-655	8.10.0.x	8.12.0.x
		AP-654	8.11.2.x	8.12.0.x
	630 Series	AP-635	8.9.0.x	8.12.0.x
		AP-634	8.11.2.x	8.12.0.x
	610 Series	AP-615	8.11.0.x	8.12.0.x
	600 Series	AP-605H	8.12.0.x	8.12.0.x
5xx	580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX	8.10.0.x	8.12.0.x
	570 Series	AP-574, AP-575, AP-577. AP-575EX, AP-577EX	8.7.0.x	8.12.0.x
	560 Series	AP-565, AP-567, AP-565EX, AP-567EX	8.7.1.x	8.12.0.x
	550 Series	AP-555	8.5.0.x	8.12.0.x
	530 Series	AP-534, AP-535	8.5.0.x	8.12.0.x
	510 Series	AP-518	8.7.0.x	8.12.0.x
		AP-514, AP-515	8.4.0.x	8.12.0.x
	500 Series	AP-504, AP-505	8.6.0.x	8.12.0.x
		AP-505H, AP-505HR	8.7.0.x	8.12.0.x
		AP-503H, AP-503HR	8.7.1.x	8.12.0.x
		AP-503	8.11.1.x	8.12.0.x

Access Points			AOS-8.x Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
3xx	380 Series	AP-387	8.4.0.x	8.10.0.x
	370 Series	AP-374, AP-375, AP-377, AP-375EX, AP-377EX, AP-375ATEX	8.3.0.x	8.12.0.x
	360 Series	AP-365, AP-367	8.3.0.x	8.12.0.x
	340 Series	AP-344, AP-345	8.3.0.x	8.10.0.x
	330 Series	AP-334, AP-335	8.1.0.x	8.10.0.x
	320 Series	AP-324, AP-325	8.0.0.x	8.10.0.x
	310 Series	AP-318	8.3.0.x	8.12.0.x
		AP-314, AP-315	8.1.0.x	8.12.0.x
	300 Series	AP-304, AP-305	8.1.0.x	8.12.0.x
		AP-303H, AP-303HR	8.2.0.x	8.12.0.x
		AP-303P	8.4.0.x	8.12.0.x
		AP-303	8.3.0.x	8.12.0.x
2xx	270 Series	AP-274, AP-275, AP-277	8.0.0.x	8.10.0.x
	220 Series	AP-224, AP-225, AP-228	8.0.0.x	8.10.0.x
	210 Series	AP-214, AP-215	8.0.0.x	8.10.0.x
	200 Series	AP-207	8.1.0.x	8.10.0.x
		AP-204, AP-205, AP-205H	8.0.0.x	8.10.0.x
		AP-203H, AP-203R, AP-203RP	8.2.0.x	8.10.0.x

Access Points			AOS-8.x Versions Supported	
AP Family	**AP Series**	**AP Model**	**Minimum**	**Latest**
1xx	170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1	8.0.0.x	8.6.0.x
	130 Series	AP-134, AP-135	8.0.0.x	8.6.0.x
	110 Series	AP-114, AP-115	8.0.0.x	8.6.0.x
	100 Series	AP-103, AP-104, AP-105	8.0.0.x	8.6.0.x
		AP-103H	8.0.0.x	8.3.0.x
9x	90 Series	AP-92, AP-93, 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 controller 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 networkingsupport.hpe.com.

The following DRT file version is part of this release:

- DRT-1.0_91868

Chapter 6
Resolved Issues in AOS-8.10.0.16

This chapter describes the resolved issues in this release.

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-236852	The error log **ofa: |ofa| ofa_gsm_ event_user_process: port not found:19, tnm50c4ddb3b194 end point is not configured or is down** was displayed when clients connected to an IAP-VPN tunnel. The fix ensures such error log is not displayed. This issue was observed on Mobility Conductors running AOS-8.10.0.2 or later versions.	AOS-8.10.0.2
AOS-238545 AOS-260378	Some controllers running AOS-8.10.0.3 or later versions experienced unexpected crashes due to an issue related to the OSPF protocol. The crashes occurred when the LSA re-origination happened within a shorter-than-expected interval, preventing the sequence number from being incremented. This resulted in the database entry being set to **NULL** in **LsaUpdateReceived**. The fix ensures that **LsaUpdateReceived** calls **LsaReOriginate** with a **NULL** interface structure pointer in cases where **LSA** regeneration is unnecessary. Additionally, it implements a **NULL** check in **LsaOrgNetwork** to handle scenarios where a **NULL** interface structure pointer is passed from the caller.	AOS-8.10.0.3
AOS-241212 AOS-241537	Some 7220 controllers running AOS-8.10.0.4 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Nanny rebooted machine - low on free memory**. The fix ensures the controllers perform as expected.	AOS-8.10.0.4
AOS-241338 AOS-245793	The **show openflow ports** command did not show any physical port information, leading to issues with AirGroup server functionality. The fix ensures the command works as expected. This issue was observed in Mobility Conductors running AOS-8.11.1.0 or later versions.	AOS-8.11.1.0
AOS-241542 AOS-259771	Some controllers reported unexpected crashes in the **flow_ manager** module. The fix ensures controllers work as expected. This issue was observed in controllers running AOS-8.10.0.0 or later versions.	AOS-8.10.0.11
AOS-243536 AOS-248711	Some Mobility Controllers running AOS-8.0.0.0 or later versions displayed incorrect values in **Discovery State** and **Transport State** for AirGroup services, after running the **show airgroup switches** command. This occurred due to a race condition. Therefore, users connected to the affected APs were unable to use AirGroup services. The fix ensures the correct values are displayed.	AOS-8.10.0.6
AOS-244965	An unnecessary debugging log appeared as **Received ICMP (DEST_UNREACH, PROT_UNREACH) from X.X.X.X for heartbeat tunnel**. The fix deletes this unnecessary log. This issue was observed in controllers running AOS-8.10.0.5 or later versions.	AOS-8.10.0.5

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-250148	AirGroup's **Transport State** was stuck on initializing status. The issue was related to the current handling of OpenFlow flows in AOS-8 SDN controllers. The fix ensures the managed devices work as expected. This issue was observed in managed devices running AOS-8.0.0.0 or later versions.	AOS-8.10.0.9
AOS-250747 AOS-255302 AOS-256513	AP radio count information in Mobility Conductors was not consistent with AirWave's count. This issue occurred due to an age-out issue in the station hash table, causing WIDS to function improperly. The fix ensures that AirWave's information is consistent with the Mobility Conductor. This issue was observed in Mobility Conductors running AOS-8.10.0.7 or later versions.	AOS-8.10.0.7
AOS-251605 AOS-241347	Wired AirGroup servers disappeared from the AirGroup server table when GE/PC ports were deactivated. The fix ensures that wired AirGroup servers display as expected. This issue was observed on Mobility Controllers running AOS-8.10.0.0 or later versions.	AOS-8.10.0.9
AOS-252114 AOS-259088	In some 9240 controllers, egress packets were not properly load-balanced across all LAG members; thus, the receive rate at the far end was significantly lesser than the total ingress packets. This occurred due to an endian issue. The fix ensures that the traffic is balanced among all LAG members. This issue was observed in x86-based controllers running AOS-8.10.0.9 or later versions.	AOS-8.10.0.9
AOS-252689 AOS-256126	AirGroup servers randomly disappeared from the topology. The issue was related to OpenFlow connections flapping unexpectedly due to TCP read/write failures not being handled properly in OFA and OFC software. The fix ensures the servers appear as expected. This issue was observed in controllers running AOS-8.11.2.2 or later versions.	AOS-8.11.2.2
AOS-252798	The **OFA** process crashed on controllers running AOS-8.10.0.10 or later versions after a RAP deployment. The issue occurred due to a segmentation fault while deleting a client object from the OFML library. The fix ensures the **OFA** process works as expected.	AOS-8.10.0.2
AOS-254363	The **switch_manager** process crashed on some controllers running AOS-8.10.0.8 or later versions. The fix ensures the process works as expected.	AOS-8.10.0.8
AOS-254431 AOS-259912	Users experienced disconnections on handheld devices while attempting to renew the PMK cache. The issue was caused by the AP sending an unencrypted EAP identity request after receiving the start message from the user, which resulted in the user being disconnected for several minutes. The fix ensures that when the client initiates a new EAP session while being already connected, the EAP packets from the AP are sent encrypted using the current PTK, preventing disconnections. This issue was observed in APs running AOS-8.10.0.0 or later versions.	AOS-8 8.10.0.8
AOS-254700	Users were unable to delete stale AP entries through the WebUI or CLI. The fix ensures that the users are able to do so. This issue was observed in Mobility Conductors running AOS-8.10.0.11 or later versions in a cluster setup.	AOS-8.10.0.11

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-255626	When uploading a **.pem** certificate with the same name in different hierarchy locations, no error message was displayed and the user was able to save the configuration. In both the CLI and WebUI, if either certificate was deleted, both of them would get deleted. The fix ensures only the intended certificate is deleted. This issue was observed in controllers running AOS-8.10.0.11 or later versions.	AOS-8.10.0.11
AOS-255648 AOS-255929	Some clients experienced MAC authentication issues when attempting to connect to an SSID. This issue was related to RadSec server connectivity. The fix ensures that connection to the RadSec server is established successfully, and authentication works as expected. This issue was observed in 7210 controllers running AOS-8.10.0.6 running or later versions.	AOS-8.10.0.6
AOS-256180	After a software upgrade, Branch Gateways failed to reestablish a connection with peer VLANs when PAPI enhanced security was enabled. The fix ensures the Branch Gateway works as expected. This issue was observed in Central-managed gateways running AOS-8.6.0.4-2.2.0.7 or later versions.	AOS-8.6.0.15
AOS-256292	Controllers displayed an error message when the user attempted to access the managed network node through the **Dashboard > Configuration > Services** page. This issue occurred when the cluster profile was configured with a space in the profile name. The fix ensures the controllers work as expected. This issue was observed in controllers running AOS-8.10.0.8 or later versions in a cluster setup.	AOS-8.10.0.8
AOS-256406	In some controllers, the output of the **show crypto isakmp timers** command displayed a **Module IKE is busy. Please try later** error message. The controllers were dedicated to VIA clients only and the issue was observed when the number of VPN users exceeded one hundred. The fix ensures the controllers work as expected. This issue was observed in devices running AOS-8.10.0.9 or later versions.	AOS-8.10.0.9
AOS-256514 AOS-258728 AOS-260113 AOS-260395 AOS-260647	Some AP-635 access points crashed and rebooted unexpectedly. The log files listed the reason for the crash as **ar_wal_tx_ send.c:8479 Assertion**. The issue was related to the AP image found in previous versions of AOS-8.10.x. The fix contains a patch for the AP image that resolves the error. This issue was observed in APs running AOS-8.10.0.10 or later versions.	AOS-8.10.0.10
AOS-256547	Some devices running AOS-8.10.0.9 or later versions crashed and rebooted. The log files listed the reason for the event as **mem_ mon process died (Intent:cause: 86:34)**. The fix ensures that the devices work as expected.	AOS-8.10.0.9
AOS-256714	Mobility Conductors unexpectedly displayed the AP's IP instead of Client's IP in user authentication **success authmgr** logs. The fix ensures that the Mobility Conductors work as expected. This issue was observed in Mobility Conductors running AOS-8.10.0.11 or later versions.	AOS-8.10.0.11

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-256821	The BLE relay process crashed unexpectedly in 7220 controllers running AOS-8.10.0.11 or later versions. This issue occurred when the main BLE relay thread and the thread for the WebSocket connection were not synchronized. This caused the connection state to be removed by the main BLE thread while the WebSocket thread accessed the packet queue. The fix ensures the controllers work as expected in this scenario.	AOS-8.10.0.11
AOS-256825	Some AP-635 access points crashed unexpectedly. The log file listed the reason for the event as **Warn: trap[645]: Trapped: Thread: 5, reason: 00000800, PC: 4004FF98, previous PC: 4004FF94**. The fix ensures that the crash does not happen. The issue was observed in AP-635 access points running AOS-8.10.0.0 or later versions.	AOS-8.10.0.0
AOS-256916	Some Werfen Medical devices got disconnected when another WME-QoS-capable client connected to an AP-635 access point. The issue occurred after HE MU EDCA updated WME QoS Info. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-8.10.0.0 or later versions.	AOS-8.10.0.0
AOS-257285 AOS-260818	When 13 or more VAPs were configured on a single radio, the APs got stuck in **Dirty** state. This issue resulted in a continuous flood of configuration messages that overwhelmed the STM process, causing client association to fail. The fix ensures the APs work as expected. This issue was observed in controllers running AOS-8.10.0.13 or later versions in a cluster setup.	AOS-8.10.0.13
AOS-257760	The authentication server name was duplicated with the duplicate text overlapping the existing text. This issue occurred randomly when configuring a new server on the WLAN profile during asynchronous operations. The fix ensures the authentication server name is displayed as expected. This issue was observed in controllers running AOS-8.10.0.0 or later versions.	AOS-8.10.0.12
AOS-257808	Customers experienced leakage of per-user bandwidth contracts in controllers in a cluster setup over a period of months. This issue occurred because bandwidth contracts were not applied to connected clients. The fix ensures bandwidth contracts do not leak in cluster setups. This issue was observed in 7240XM controllers running AOS-8.10.0.11 or later versions.	AOS-8.10.0.11
AOS-257871	Controllers displayed an error message when users tried to configure the **Wireless Intrusion Protection (WIP)** policy through the **Configuration** > **Tasks** page of the WebUI. The error message was displayed as **Exception raised while processing requests**. The fix ensures that the users can configure the WIP policy successfully. This issue was observed in controllers running AOS-8.10.0.12 or later versions.	AOS-8.10.0.12
AOS-258055	Some AP-514 access points displayed an incorrect **Antenna Radio** status when external antennas were connected and disconnected. The fix ensures that the APs work as expected. This issue was observed in APs running AOS-8.10.0.10 or later versions.	AOS-8.10.0.10

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-258074 AOS-257910	Some wireless clients were unable to discover AirGroup servers although they were on the AirGroup server list. The issue was related to OpenFlow's data input/output handling being exceeded. The fix improves OpenFlow's data count handling, ensuring that AirGroup servers are discoverable, as expected. This issue was observed in managed device running AOS-8.10.0.12 or later versions.	AOS-8.12.0.1
AOS-258090	Some Mobility Conductors unexpectedly displayed an **imudp: error receiving on socket: Broken pipe: Broken pipe [v8.2102.0]** error in the rsyslogs. The fix ensures that the error does not display in the rsyslogs. This issue was observed in Mobility Conductors running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-258103	Some APs experienced packet loss when receiving pings with packet size over 497 bytes from Cisco's fast ping protocol. The fix ensures that data loss does not occur. This issue was observed in AP-515 access points running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-258212 AOS-258932	In clusters with varying capacity license types, cluster live upgrade preloads only some APs. The fix ensures that live upgrades preload all APs as expected. This issue was observed in 9240 controllers running AOS-8.10.0.9 or later versions.	AOS-8.10.0.11
AOS-258272	In the **show ap database** command, some AP flags were not synchronized to **SAAC**. The fix ensures that the AP synchronize as expected. This issue was observed in APs running AOS-8.10.0.3 or later versions.	AOS-8.10.0.3
AOS-258305	Some AP-635 access points crashed unexpectedly. The log files listed the reason for the reboot as **Kernel panic: Take care of the TARGET ASSERT**. The fix ensures the APs work as expected. This issue was observed in APs running AOS-8.10.0.8 or later versions.	AOS-8.10.0.8
AOS-258558	In some Mobility Conductors, the total throughput usage did not match with the throughput of the individual managed devices. The sum of the managed devices was significantly higher than the one reported in the **Dashboard > Overview > USAGE** page of the conductor's WebUI. At the same time, the portion of the graph was concave, representing the lesser throughput. This issue was caused by the data type used in the backend to store these values. The fix ensures the **USAGE** data is congruent. This issue was observed in Mobility Conductors running AOS-8.10.0.7 or later versions.	AOS-8.10.0.7
AOS-258579	Some 7240XM controllers failed to reach default gateway due to an **INCOMPLETE** or **FAILED** ARP resolution. The fix enhances the ability to debug the failures and helps in easier identification of issues. This issue was observed in 7240XM controllers running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-258777	Some users experienced synchronization issues between controllers and RAPs after updating the RAPs' allowlist. The issue occurred when modifying the **AP-Group** or **AP-Name**, which was correctly updated on the RAP but not on the controller. The fix ensures that inconsistencies between RAPs and controllers will no longer occur. This issue was observed in 7220 controllers running AOS-8.10.0.11 or later versions.	AOS-8.10.0.13

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-259138	The **ofa** process crashed unexpectedly with the error message **ofserver_handle_connection_down_event**. The fix ensures that the process works as expected. This issue was observed in controllers running AOS-8.10.0.7 or later versions.	AOS-8.10.0.7
AOS-259231	Some AP-635 access points randomly crashed and the log files listed the error **Reboot caused by kernel panic with whal_sring.c:1403**. The fix ensures the APs perform as expected. This issue was observed in APs running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-259355	After failover to a redundant controller, updates to the denylist were not synchronized. This issue occurred due to denylist database synchronization problems. The fix ensures that the denylist is synchronized accurately. This issue was observed in controllers running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-259428 AOS-261205	When NAT was enabled on user VLANs, there was an issue where WebCC ACL rule hits were incremented even if there was no traffic matching the rule. The fix ensures that only the matching traffic increments ACL hits instead of all web traffic. This issue was observed on controllers running AOS-8.10.0.0 or later versions.	AOS-8.12.0.3
AOS-259603 AOS-260283 AOS-260347	The ZMQ threads of the **nbapi_helper** process crashed randomly. The fix ensures the ZMQ threads of the **nbapi_helper** process work as expected. This issue was observed in Mobility Conductors after upgrading the software to AOS-8.10.0.14 or later versions.	AOS-8.10.0.14
AOS-259719 AOS-259734	Clients did not receive an IP address when reconnecting to the AP after upgrading the software version. This issue occurred when the ACL was configured to deny user traffic from UDP port 68. This issue was observed in managed devices running AOS-8.10.0.14 or later versions.	AOS-8.10.0.14
AOS-259780	Some wireless clients experienced reduced download speeds when LACP striping was enabled on AP-655 access points. The fix ensures accurate download speeds when LACP striping is enabled. This issue was observed in AP-655 access points running AOS-8.10.0.14 or later versions.	AOS-8.12.0.0
AOS-259788	In the **Access Point** tab of the WebUI, some APs incorrectly displayed the **UPTIME** as **0**. This issue occurred whenever the AP and the controller boot up at the same time. The fix ensures the APs work as expected. This issue was observed in APs running AOS-8.10.0.14 or later versions.	AOS-8.10.0.14
AOS-259808 AOS-258120	WebSocket connection requests to the CPPM server failed. The issue occurred whenever username and password combinations exceeded a length of 28 characters, causing credentials to get truncated internally, leading to SSL failure. The fix ensures that the WebSocket connection is successful in this scenario. This issue was observed in controllers running AOS-8.10.0.12 or later versions.	AOS-8.10.0.0
AOS-259810	Some APs became unreachable when **MultiZone** was enabled. This occurred because APs created a **default route entry** that pointed to the **DataZone** tunnel after controller failover, which caused packet drops. The fix ensures that APs do not create this entry and are reachable in this scenario. This issue was observed in APs running AOS-8.0.0.0 or later versions.	AOS-8.10.0.12

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-259860 AOS-260730 AOS-261328	Some AP-655 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot after internal watchdog dump saved**. The fix ensures that the APs work as expected. The issue was observed in APs running AOS-8.10.0.14 or later versions.	AOS-8.10.0.14
AOS-260074	Server-derivation rule was not updated accurately in the **running config** command output of some managed devices. The fix ensures that the server derivation rule is updated accurately in all managed devices. This issue was observed in controllers running AOS-8.10.0.7 or later versions.	AOS-8.10.0.7
AOS-260100 AOS-260111 AOS-260811 AOS-260961 AOS-261010 AOS-261165 AOS-261318 AOS-261464 AOS-261559	Some AP-577 access points running AOS-8.10.0.9 or later versions rebooted unexpectedly. The log files listed the reason for the reboot as **BUGSoftLockup:CPU#1 stuck for 22s! [kworker/1:3:27856] PC:wlc_bmac_suspend_mac_and_ wait+0x21c/0x440 [wl_v6]**. The fix ensures that the APs work as expected.	AOS-8.10.0.14
AOS-260317 AOS-261156	Some access points crashed and rebooted unexpectedly when multiple users were connected, and the power-saving mode was activated. The issue arose from dropped packets due to insufficient capacity in the power save queue, resulting in AP crashes. The fix ensures the APs work as expected. This issue was observed in APs running AOS-8.10.0.14 or later versions.	AOS-8.10.0.14
AOS-260437	Some users connected to an SSID configured with WPA3-AES-CCM-128 encryption experienced intermittent traffic issues after roaming between APs. The issue persisted until users roamed to another AP, at which point traffic resumed. The fix ensures that user traffic is able to pass after a station roams. This issue was observed on access points running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-260441	Some AP-635 access points randomly rebooted with the reason, **Kernel panic: Fatal exception in interrupt**. This issue occurred in an IPsec environment, where a tunneled device was deleted after IPsec encryption. The fix ensures proper validations are made, preventing the AP crash. This issue was observed in AP-635 access points running AOS-8.10.0.0 or later versions.	AOS-8.10.0.0
AOS-260491	Some controllers running AOS-8.12.0.3 or later versions experienced multiple mDNS process crashes. This issue was observed when managed devices were present under a different island. The fix ensures that the mDNS works as expected.	AOS-8.12.0.3
AOS-260527	In non-CPsec environments, obtaining technical support logs either via the WebUI or the **show ap tech-support** command took a long time, sometimes resulting in the process being aborted or an **Unable to save..!!** error message being displayed. The issue was related to the **show memory ap rapper** command taking too long to run whenever CPsec was disabled, delaying the request. The fix ensures the expected behavior when checking rapper memory in a non-CPsec environment, expediting the generation of technical support logs. This issue was observed in managed devices running AOS-8.10.0.0 or later versions.	AOS-8.12.0.1

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-260788 AOS-259548	Some 9240 controllers reported incorrect bandwidth contract numbers that did not match the supported numbers for each license type. The fix ensures controllers work as expected. This issue was observed in controllers running AOS-8.10.0.0 or later versions.	AOS-8.10.0.0
AOS-260852	VAPs were turned off and could not be turned back on after adding a new controller to the cluster. The issue occurred due to an incorrect configuration of the node limit in the MultiZone profile. The fix ensures that the VAPs can be successfully turned on even after adding a new controller. This issue was observed in AP-655 access points running AOS-8.10.0.0 or later versions.	AOS-8.10.0.0
AOS-261118 AOS-261119	During a cluster failover, AP-635 and AP-535 access points went down and did not come back up. The issue occurred in a two-node cluster where the AP's Standby Active Access Controller (SAAC) was slow to be assigned. The node that would become the SAAC initially acted as the Unicast Access Controller (UAC) for the AP. If the AP failed over to this node as the Active Access Controller (AAC), the node continued to consider itself the UAC. Upon failover completion, the node attempted to exit the UAC role, mistakenly deleting the AP's tunnel and causing the AP to go offline. The fix ensures that APs recover and come back online automatically after a cluster failover. This issue was observed on devices running AOS-8.10.0.12 or later versions.	AOS-8.10.0.12
AOS-261520	Some APs crashed and rebooted unexpectedly after a VAP was removed. The log files listed the reason for the crash as **BadPtr:0000030c PC:wl_pktc_tx+0x1d8/0x798 [wl_v6] Warm-reset**. The fix ensures there will be no crashes associated with removing VAPs. This issue was observed in AP-505 access points running AOS-8.10.0.6 or later versions.	AOS-8.10.0.6
AOS-261623 AOS-261987 AOS-261992 AOS-262042	Some AP-555 access points randomly crashed and rebooted. The log files listed the reason for the crash as **Kernel panic - not syncing: Take care of the TARGET ASSERT**. The fix ensures APs work as expected. This issue was observed in APs running AOS-8.10.0.12 or later versions.	AOS-8.10.0.12
AOS-262403 AOS-261409 AOS-261914	Some clients connected to 500 Series access points experienced latency and performance issues. The fix brings back the latency and performance to the expected level for these clients. This issue was observed in access points running AOS-8.10.0.14 or later versions.	AOS-8.10.0.14
AOS-259007	The SSID profile configuration was not correctly applying multiple changes simultaneously in the configuration management system, resulting in incorrect information being broadcast in the beacon. The fix ensures APs work as expected. This issue was observed in access points running AOS-8.12.0.2 or later versions.	AOS-8.12.0.2

Table 3: *Resolved Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-260486	After upgrading to AOS-8.10.0.11, some users experienced connection issues on devices connected to APs due to the AirMatch optimization process. The issue occurred in rare cases during the initial optimization runs, when AirMatch failed to read previously optimized radio data. As a result, the optimization process was triggered the following day, displaying a **New radios optimized** message, which led to unnecessary deployments, particularly when the quality-threshold value was not met. The fix ensures that the AirMatch optimization process correctly reads the optimized radio data from prior runs during the initial optimization process and ensures deployment according to the quality-threshold. This issue was observed in AP-315 and AP-515 access points running AOS-8.10.0.11 or later versions.	AOS-8.10.0.11

Known Issues in AOS-8.10.0.16

This chapter describes the known issues observed in this release.

Table 4: *Known Issues in AOS-8.10.0.16*

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-8.6.0.15 or later versions.	AOS-8.6.0.15
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-8.7.1.1 or later versions.	AOS-8.7.1.3
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-8.7.1.4 or later versions.	AOS-8.7.1.4
AOS-229024	Some AP-505 access points running AOS-8.7.1.5 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-8.7.1.5
AOS-229770	Controllers do not display information on the 802.1X connection statuses if the 802.1X connection fails. This issue is observed in controllers running AOS-8.7.1.8 or later versions.	AOS-8.7.1.8
AOS-232092	Some AP-305 and AP-505 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-8.8.0.1 or later versions.	AOS-8.8.0.1
AOS-232233	Some 9004-LTE controllers 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 controllers running AOS-8.7.0.0 or later versions.	AOS-8.7.1.4
AOS-232875 AOS-239469 AOS-247974	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 Mobility Controllers running AOS-8.10.0.0 or later versions.	AOS-8.10.0.0

Table 4: *Known Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-237174	Some 9240 controllers record informational logs, even though the system log level is configured as **warning**. This issue is observed in 9240 controllers running AOS-8.10.0.2 or later versions.	AOS-8.10.0.2
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-8.6.0.16 or later versions.	AOS-8.6.0.16
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-8.6.0.15 or later versions.	AOS-8.6.0.15
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 in the same group. This issue is observed in managed devices running AOS-8.6.0.15 or later versions.	AOS-8.6.0.15
AOS-239724 AOS-239529 AOS-263428	Some APs unexpectedly increase the response time when using DHCP configuration. This issue is observed in APs running AOS-8.10.0.2 or later versions.	AOS-8.10.0.2
AOS-239814 AOS-239815	In some controllers running AOS-8.6.0.11 or later versions, IPv4 and IPv6 accounting messages use the same session ID with Passpoint. This causes multiple accounting messages to be sent repeatedly.	AOS-8.6.0.11
AOS-242404	The reason and timestamp of APs in a **DOWN** status is not displayed in the Mobility Conductor dashboard under **Infrastructure > Access Devices**. The information displayed is **AP is down since - because of the following reason: None**, or similar. This issue is observed in AOS-8.10.0.4 or later versions.	AOS-8.10.0.4
AOS-242532	Some AP-535 access points are not available on 7210 controllers 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 controller. The issue is observed in controllers running AOS-8.6.0.9 or later versions.	AOS-8.6.0.9
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 Mobility Controllers running AOS-8.6.0.20 or later versions.	AOS-8.6.0.20
AOS-244193	Some AP-655 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-8.10.0.6 or later versions.	AOS-8.10.0.6
AOS-244850 AOS-255408	The CLI process crashes unexpectedly on 9240 controllers running AOS-8.10.0.0 or later versions.	AOS-8.10.0.8

Table 4: *Known Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-245367	In standalone controllers, it is not possible to configure application speed limit under the **Dashboard > Traffic Analysis > Applications** tab. This feature works if the controller is in Conductor role, but this error is not reported properly. This issue is observed in controllers running AOS-8.10.0.5 or later versions.	AOS-8.10.0.5
AOS-246103 AOS-247433 AOS-240688 AOS-250837	Some AP-635 and AP-535 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 controller recovery, to which the APs are connected. This issue is observed in APs running AOS-8.10.0.5 or later versions.	AOS-8.10.0.5
AOS-246170 AOS-245703 AOS-245763 AOS-254175 AOS-254868 AOS-258612	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-8.10.0.6 or later versions.	AOS-8.10.0.6
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 controllers running AOS-8.10.0.0 or later versions.	AOS-8.10.0.0
AOS-246960	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 7010 controllers running AOS-8.6.0.21 or later versions. **Workaround**: Reload the managed device or restart the **profmgr** process to fix the issue.	AOS-8.6.0.21
AOS-247721 AOS-247807	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-8.10.0.7 or later versions.	AOS-8.10.0.7
AOS-248466	The **Controller discovery preference** field disappears when changing it from **ADP** to **Static** under the **Dashboard > Configuration > Access Point > Provision** page. This issue is observed in controllers running AOS-8.10.0.8 or later versions.	AOS-8.10.0.8
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 controllers running AOS-8.10.0.0 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-8.10.0.0
AOS-248909	A few clients fail to connect to gateways running AOS-8.10.0.0 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-8.10.0.0

Table 4: *Known Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-252206 AOS-255808 AOS-258729 AOS-245600	Some controllers crash unexpectedly due to a memory leak in the **DDS** process. This issue is observed in controllers running AOS-8.6.0.17 or later versions.	AOS-8.10.0.8
AOS-252538	The **IKE XAuth** process fails on Remote APs, causing them to reboot and appear as **Down** on controllers. 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-8.6.0.17 or later versions.	AOS-8.6.0.17
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-8.10.0.11 or later versions.	AOS-8.10.0.11
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-8.10.0.7 or later versions.	AOS-8.10.0.7
AOS-256229	Default roles on some controllers, such as the authenticated role, are lost after enabling the PEF feature. This occurs because the role configurations are not retained when the feature is enabled. This issue is observed in controllersrunning AOS-8.10.0.9 or later versions. **Workaround**: After performing a **write erase** operation, enable the PEF feature and reload the controller to ensure that the default roles are initialized properly.	AOS-8.10.0.9
AOS-256450 AOS-255529	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-8.10.0.8 or later versions in a Mobility Conductor-Managed Device topology.	AOS-8.10.0.8
AOS-256471	Some Mobility Conductors running AOS-8.10.0.12 or later versions experience slow loading times when trying to configure any profiles through the WebUI.	AOS-8.10.0.12
AOS-256636	When PAPI security is enabled, Dot1x-process PAPI checksum verification fails for messages received from APs. However, when control plane security is disabled for APs, APs and mobile devices can communicate as plain text. This issue is observed in APs running AOS-8.6.0.15 or later versions. **Workaround**: Enable control plane security and do not use enhanced security.	AOS-8.6.0.15
AOS-256745	In the **Configuration > System > Profiles** page of the WebUI, the landscape scroll bar cannot be dragged. This issue is observed in controllers running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
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 AP-535 access points running AOS-8.10.0.10 or later versions.	AOS-8.10.0.12

Table 4: *Known Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-258685	When creating a new VLAN, the VLAN ID is not set to **Hash** by default, under **Configuration > Interfaces > VLANs > Options > Assignment Type**. However, in the output of the **show vlan mapping** command, the **Assignment Type** shows **Hash** as expected. In the WebUI, when the **Assignment Type** is actually selected and the changes are saved, the **Assignment Type** is shown correctly in the controller and Mobility Conductor. This issue is observed in controllers running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-259078	By design, a capacity license cannot be added through the WebUI whenever an external license server is configured. However, the **Configuration > License > Capacity License** tab is visible. This issue is observed in managed devices running AOS-8.10.0.0 or later versions. **Note:** Capacity licenses should be added through the CLI of managed devices.	AOS-8.10.0.0
AOS-259552 AOS-261151	When a VPN is configured for the DHCP proxy on controllers, the IP address gets printed in reverse order. This issue is observed in gateways running AOS-8.10.0.13 or later versions.	AOS-8.10.0.13
AOS-259984 AOS-260461 AOS-261609	Users are unable to successfully roam between access points when the controller fails to initiate the 4-way handshake for the new association. This issue occurs on enhanced-open ESSIDs with MAC authentication enabled when the authentication server overrides the controller's initial VLAN assignment. This issue is observed in controllers running AOS-8.10.0.14 or later versions.	AOS-8.10.0.14
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-8.10.0.14 or later versions.	AOS-8.10.0.14
AOS-260519	Stale entries are not cleared in the WebUI when the **clear gap-db** command is executed for the AP. This issue occurs due to the SC-MON process not being able to clear down AP entries successfully. This issue is observed in APs running AOS-8.10.0.6 or later versions.	AOS-8.10.0.6
AOS-260880	In 9240 gateways, when configuring a VPN IP over DHCP proxy option, users are unable to connect to the VPN. This issue is observed in gateways running AOS-8.10.0.1 or later versions.	AOS-8.10.0.14
AOS-261195	In some controllers running AOS-8.10.0.15, the values for **MATCH METHOD**, **MATCH TYPE** and **MATCH AP/RULE** are incorrect for valid APs. This information is seen in the **Dashboard > Security > Detected Radios** page of the WebUI and also in the output of the **show wms ap list** command.	AOS-8.10.0.15
AOS-261483	The **airmatch ap freeze** command is unable to freeze channel 165 on the controller. This issue is observed in AP-535 access points running AOS-8.10.0.15 or later versions.	AOS-8.10.0.15

Table 4: *Known Issues in AOS-8.10.0.16*

Bug ID	Description	Reported Version
AOS-261852 AOS-261583	In a managed devices cluster with wired AirGroup server enabled, packets transmitted on the uplink of one controller are revived with the MAC address of the other controller. This issue is observed in the Mobility Conductors or controllers running AOS-8.10.0.9 or later versions.	AOS-8.10.0.9
AOS-259662 AOS-259664 AOS-262009	Some AP-635 access points running AOS-8.10.0.14 or later versions, experience assertion errors and reboot unexpectedly. The log files list the reason as **wlan_wmi.c:653 Assertion 0 failedparam0 :zero, param1 :zero, param2 :zero**.	AOS-8.10.0.14

Chapter 7
Limitations in AOS-8.10.x

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

Title	Description
Port-Channel Limitation in 7280 Controllers	The 7280 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-8 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 650 Series and 630 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 500 Series APs	Air Slice is partially enabled on 500 Series access points and 510 Series access points. However, WMM boost will be functional even if Air Slice high-priority queuing is disabled.

Title	Description
cpboot command in 7000 Series and 7200 Series Controllers	The **cpboot** command does not upgrade the AOS-8 software version of 7000 Series and 7200 Series controllers.

Chapter 8
Upgrade Procedure

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

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

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-8 runs on your managed device?
  - Are all managed devices running the same version of AOS-8?
  - What services are used on your managed device (employee wireless, guest access, Remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load AOS-8 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-8, 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 *Aruba Mobility Conductor Licensing Guide*.
- With the introduction of the Long Supported Release (LSR) and Short Supported Release (SSR) terminology in AOS-8.10.0.0, 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-8.10.0.0 MultiVersion support.

- Only for the AOS-8.10.0.0 LSR release, AOS-8.6.0.0 is treated as an LSR despite being beyond N-3. As such a Mobility Conductor running AOS-8.10.0.0 supports managed devices running AOS-8.10.0.0, AOS-8.9.0.0, AOS-8.8.0.0, AOS-8.7.0.0 and AOS-8.6.0.0.

RAM and FLASH Storage Requirements

All Aruba 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:

- Ensure sufficient RAM and flash space is available in the Controller/MD/BGW before proceeding with the upgrade.
- Execute the **show memory** command to identify the available free memory.
- 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 RAM, free some used memory. Copy any log files, crash data, or flash backups from your gateways to a desired location. Delete the following files from the Controller/MD/BGW to free FLASH storage:
  - **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 34 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 34 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 34 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device
- The show commands are available under **Analyze > Tool > Commands** section of Aruba Central.

If available RAM is not suffiicient to meet the requirements stated in the appropriate release notes, it may be necessary to reboot the device and then immediately upgrade, or disable some functionality. The user should consult HPE/Aruba technical support for guidance.

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-8 image has increased in size and this may cause issues while upgrading to newer AOS-8 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 controller. Then delete the **flashbackup.tar.gz** and **configbackup.tar.gz** files from the flash memory of the controller.
- 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 controller 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 controller 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-8 upgrade as listed in Table 5
4. **If you are unable to free up sufficient flash memory, contact Technical Support. Do not reboot the controller.**
5. If sufficient flash memory is available, proceed with the standard AOS-8 upgrade. See Upgrading AOS-8.
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-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        : AOS-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 controller. If any of the errors listed in step 4 were observed, the following errors might occur while booting AOS-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 controller 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-8 upgrade procedure. See Upgrading AOS-8.
- 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-8 upgrade procedure in the same partition. See Upgrading AOS-8.

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-8

Upgrade AOS-8 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 RAM and FLASH Storage Requirements on page 31.

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-8 from a TFTP server, FTP server, or local file.

1. Download the AOS-8 image from the customer support site.
2. Upload the AOS-8 image to a PC or workstation on your network.
3. Validate the SHA hash for the AOS-8 image:
   a. Download the **Aruba.sha256** file from the download directory.

b. Load the AOS-8 image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.

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

The AOS-8 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-8 image.

4. Log in to the AOS-8 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.

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-8 from a TFTP server, FTP server, or local file.

1. Download the AOS-8 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-8 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-8 Upgrade

Verify the AOS-8 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-8 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 34 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-8 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 34 for information on creating a backup.

Downgrading AOS-8

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-8 version, perform the following steps:

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 34.
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-8 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-8 version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the AOS-8 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-8 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-8 version.
- If any new certificates were added in the upgraded AOS-8 version, reinstall these certificates in the downgraded AOS-8 version.

Downgrade AOS-8 version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the AOS-8 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-8 version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade AOS-8 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-8 version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the AOS-8 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-8 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-8 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.