ArubaOS 8.10.0.11 Release Notes

aruba
a Hewlett Packard Enterprise company

Copyright Information

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 ArubaOS release notes includes the following topics:

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

Important

- As mandated by the Wi-Fi Alliance, ArubaOS 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 ArubaOS 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 ArubaOS 8.9.0.0 still use **aruba-master** during DNS discovery. The usage of **aruba-conductor** is to align with the Inclusive Language Initiative.
- Upgrading from ArubaOS 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. ArubaOS 8.10.0.11 must be manually upgraded for these controllers.

Related Documents

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

- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS 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 ArubaOS 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	arubanetworks.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 ArubaOS 8.10.0.11

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

Separation of Cluster and Datapath Commands from 'tar log tech-support'

Cluster and datapath commands have been separated from **tar log tech-support**. For cluster logs, users should use: **tar logs tech-support cluster**.

Behavioral Changes

This release does not introduce any changes in ArubaOS behaviors, resources, or support that would require you to modify the existing system configurations after updating to 8.10.0.11.

Chapter 4
Supported Platforms

Supported Platforms in ArubaOS 8.x

This section displays the supported platforms in ArubaOS 8.x. The **minimum version supported** column displays the minimum ArubaOS 8.x version that can be run on a platform. The **latest version supported** column displays the newest ArubaOS 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 Conductors		ArubaOS 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		ArubaOS 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			ArubaOS 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	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			ArubaOS 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			ArubaOS 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_89428

Chapter 6
Resolved Issues in ArubaOS 8.10.0.11

This chapter describes the resolved issues in this release.

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-156537	Multicast streaming failed when broadcast and multicast optimization was enabled on the user VLAN. The fix ensures multicast streaming works as expected. This issue was observed in managed devices running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-215875	The **show ap arm state** command displayed deprecated information such as Edge, Relevant Neighbors, Valid Neighbors, Neighbor Density, and Client Density. The fix ensures the command displays updated information. This issue was observed in Mobility Controllers running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219791	The ARM profile settings mistakenly enabled aggressive scanning mode by default, which was not intended for daily production use. The fix ensures aggressive scanning is not enabled by default. This issue was observed in access points running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-222450 AOS-252037	The output of the **show aaa user-delete-result** command listed **0.0.0.0** IP addresses for IPv6 managed devices. The issue occurred because these devices did not get delete command requests. The fix ensures this delete command is sent to IPv6 controllers and gets populated with their corresponding IPv6 addresses. This issue was observed in Mobility Conductors running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-222450 AOS-252037	When the **aaa user delete** command is run on an Mobility Conductor, the **show aaa user-delete-result** command can be used to obtain a list of results of Managed Devices. However, the command was not sent to IPv6 Managed Devices and their IPs were listed with an IP address of **0.0.0.0** in output of the **show aaa user-delete-result** command. The fix ensures this delete command is sent to IPv6 controllers and populated with their corresponding IPv6 address. This issue was observed in Mobility Conductors running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-228357	Some standalone controllers encountered a PSM watchdog issue with signature **psmdebug 0x01ff000d phydebug 0x21 macctl 0x4160403 maccmd 0x4**. The fix ensures the APs work as expected. This issue was observed in AP-515 access points running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-232897	The **wlan ht-ssid-profile** CLI command overrode the radio frequencies from 80 MHz to 40 MHz, although the **show ap bss-table** CLI command displayed the radio frequencies as 80 MHz. The fix ensures that the **wlan ht-ssid-profile** CLI command does not override the radio frequencies. This issue was observed in AP-515 and AP-535 access points running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-237012	Random VIA usernames were incorrectly displayed in the user table and controller dashboard. The fix ensures that usernames are never truncated. This issue was observed on managed devices running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-239382	Some 7240XM Mobility Conductors running ArubaOS 8.7.1.9 or later versions configured in a cluster setup crashed and rebooted unexpectedly. The log files list the reason for the event as **Datapath timeout (SOS Assert)**. The fix ensures the Mobility Conductors work as expected.	ArubaOS 8.7.1.9
AOS-239653	After disconnecting from a wireless AP using 802.1x secured SSID, some clients were not logged out of the Palo Alto firewall. If the same client tried to connect again with a different username, it caused the controller to not logout the previous username and did not ask for a login for the new username. This caused the firewall not to update host information nor associate with correct firewall policy. The fix ensures the controllers work as expected. This issue was observed in controllers running ArubaOS 8.9.0.3 or later versions.	ArubaOS 8.9.0.3
AOS-239850 AOS-249756	Some Mobility Conductors crashed unexpectedly due to a memory leak in the **vmsvc** process. The log files listed the reason as **[vmsvc] HostinfoOSData: Error: no distro file found**. The fix ensures the Mobility Conductors work as expected. This issue was observed in Mobility Conductors running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-241236 AOS-251864 AOS-252982 AOS-242339 AOS-249777	Some AP-535 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_seq.c:646 Assertion !CHK_TID_FLG(ptid, WAL_TX_TID_SEND_BAR)**. The fix ensures the APs work as expected. The issue was observed in access points running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-241560	Accessing controllers through the WebUI led to excessive logs regarding the **show uplink cellular details** command, including errors stating **Command not applicable for this platform (pos: 0)**, which can be safely ignored. The fix ensures that such logs no longer display. This issue was observed in standalone 7220 Mobility Conductors running ArubaOS 8.10.0.5 or later versions.	ArubaOS 8.10.0.5

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-242107	Some AP-535 access points incorrectly detected 5 GHz interferences after upgrading to ArubaOS 8.10.0.4. The fix ensures that the access points function as expected. This issue was observed in access points running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-242115 AOS-253066	Some access points displayed the error message **ol_ath_send_peer_assoc 663: Unexpected negotiated ni_phymode 30(18) for iv_cur_mode 30(16)** after they were activated. The issue caused connectivity problems. The fix ensures the access points function as expected. This issue was observed in access points running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-242404	The reason and timestamp of APs in a **DOWN** status was not displayed in the Mobility Conductor dashboard under **Infrastructure > Access Devices**. The information displayed was **AP is down since - because of the following reason: None**, or similar. The fix ensures the correct data is displayed in the WebUI. This issue was observed in ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-242962 AOS-244935 AOS-245697 AOS-246559 AOS-248871 AOS-248913	Some APs randomly went offline and did not come up on the controller. The logs displayed the error **MMC init failed**. The issue was related to the eMMC flash memory of the AP entering an abnormal state. The fix improves the internal timing of the flash memory to ensure that the AP does not crash. This issue was observed on AP-635 and AP-655 access points running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-244659	Some clients experienced unexpected issues while roaming when using the OpenFlow protocol. The fix ensures OpenFlow works as expected and causes no issues. This issue was observed in Mobility Controllers running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-244772	For some 9004 gateways running ArubaOS 8.10.0.0 or later versions, the **show datapath user standby** command failed to display some standby user entries. This issue occurred due to data format incompatibility. The fix ensures that the **show datapath user standby** command displays the correct entries.	ArubaOS 8.10.0.0
AOS-244869	In some access points, the 4-way handshake process failed when WPA2 key-2 frames were re-transmitted by wireless clients. The fix ensures the 4-way handshake process works as expected. This issue was observed in access points running ArubaOS 8.6.0.17 or later versions.	ArubaOS 8.6.0.17
AOS-245329	The **resolvwrap** process continuously crashed whenever a VLAN that was set to **dhcp-client** failed to get an IP. The fix ensures the **resolvwrap** process does not crash in this scenario. This issue was observed in gateways running ArubaOS 8.6.0.20 or later versions.	ArubaOS 8.6.0.20

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-245914 AOS-251217 AOS-252911 AOS-246729 AOS-246925	Some AP-535, AP-635, and AP-655 access points crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first first running 8.10.0.7**. The fix ensures the access points work as expected. This issue was observed in access points running ArubaOS 8.10.0.7.	ArubaOS 8.10.0.7
AOS-246164 AOS-249753	The **profmgr** process crashed unexpectedly when configuration changes were applied to an **aaa server-group**. The fix ensures the process does not crash in this context. This issue was observed in managed devices running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-246679 AOS-251757	Some Remote APs failed to come online due to receiving duplicate inner IP addresses. This problem occurred randomly across various Remote APs. A discrepancy was discovered between the allowlist entries on the Mobility Controller and those on the managed devices for the affected Remote APs. The fix ensures the RAPs work as expected. This issue was observed on Remote APs running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-246732	9000 Series controllers were hanging during boot up if the RJ45 console cable was connected to the controller but not to the console server or computer (in case of USB console access). The fix ensures the controllers boot up correctly. This issue was observed in controllers running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-246931 AOS-248213 AOS-251763 AOS-248234 AOS-249778	Some AP-635 access points unexpectedly rebooted. The logs list the reboot reason as **Reboot caused by kernel panic with "hca_HwComponentBbQca6018_reset.cpp:169 Assertion 0 failed"**. The fix ensures the access points perform as expected. This issue was observed in APs running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-247147 AOS-251395	Some Mobility Conductors running ArubaOS 8.10.0.7 or later versions experienced classification issues with the WLAN Management System database. The fix ensures Mobility Conductors work as expected.	ArubaOS 8.10.0.7
AOS-247153	Some access points crashed and rebooted with reason **wal_rc_ul.c:218 Assertion num_rix failed**. The issue was related to the AP driver image, which has been updated to prevent these crashes from happening. This issue was observed in AP-635 access points running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-247796 AOS-248297 AOS-245421	Some AP-535 access points crashed and rebooted due to memory corruption. The memory corruption issue was fixed by aligning the address based on availability in the pool. This issue was observed in access points running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-247952 AOS-251996	The output of the **show ap bss-table ap-name** and **ap monitor ap-list ap-name** commands showed incorrect Tx BSSID flag information. Some VAPs showed an incorrect **(*+)** flag next to their BSSID in the CLI output. The fix ensures the table output of the commands is accurate. This issue was observed in AP-635 access points running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-248120	In 9240 controllers running ArubaOS 8.10.0.7 or later versions, clients failed to authenticate through EAP when many clients connected to AP-315 access points. The issue occurred because multicast frames were sent with WMM headers. The fix ensures that multicast packets are always sent without WMM headers to support non-WMM clients.	ArubaOS 8.10.0.7
AOS-248151	Some AP-535 access points crashed and rebooted unexpectedly. The log file listed the reason for reboot as **Ap crashed at sched_algo_txbf.c:1909 Assertion 0 failedparam0 :zero, param1 :zero, param2 :zero**. The fix ensures the access points perform as expected. This issue was observed in AP-535 access points running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-248267 AOS-251592	The RADIUS/RadSec server could not connect to the FQDN host after rebooting the controller, resulting in IP loopbacks. The issue occurred due to replication problems during validation. The fix ensures the controller works as expected. This issue was observed in standalone controllers running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8
AOS-248282	7010 controllers displayed PVST+ issues where the removal of VLANs led to the incorrect transmission of PVST+ BPDUs with both PVID and 802.1Q VLAN ID set to **0**. A check was added to avoid transmission of BPDUs with PVID equal to **0**. This issue was observed on controllers running ArubaOS 8.6.0.10 or later versions.	ArubaOS 8.6.0.10
AOS-248405 AOS-249646	The **login_fcgi** process crashed unexpectedly in some controllers. This issue was related to the memory required for executing the process being insufficient. The fix increases the memory allocation for the process to ensure no crashes happen. This issue was observed in 7240XM controllers running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-248415	In some controllers, the **fpapps** process displayed the error message **fpapps_amon_uplink_update_compression_stats: Cannot retrieve compression info**. This log meant that the controller failed to retrieve compression data. The fix ensures the controller can fetch such data successfully. This issue was observed in 9240 controllers running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8
AOS-248607	APs supporting 802.11ac randomly broadcasted in 20 MHz, despite the minimum channel bandwidth set to 40 MHz. The issue occurred because the APs changed channel after receiving a broadcasted CSA frame. This issue was observed in APs running ArubaOS 8.10.0.0 or later versions. The fix ensures that the APs perform as expected.	ArubaOS 8.10.0.0
AOS-248875	In the **Configuration > Roles and Policies** page of the WebUI, some Mobility Conductors displayed the **No Changes Done** error when deleting **Aliases**. The fix ensures the aliases can be deleted as expected. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-248958	Some AP-315 access points were detecting fake radars. The radar log files listed the radars with **typeid 37** and **typeid 34**. The fix ensures fake radars are filtered and minimal entries are populated in the radar log files. This issue was observed in APs running ArubaOS 8.7.1.7 or later versions.	ArubaOS 8.7.1.7
AOS-248961	Layer 3 interface displayed as **Down** on managed devices. As a result, guest users were unable to authenticate. The fix ensures guest users are able to pass the authentication process and managed devices work as expected. This issue was observed on managed devices running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-249028 AOS-251475	After upgrading from ArubaOS 8.6.0.20 to ArubaOS 8.10.0.7 or later versions, the **HTTPD** process crashed with reason **Segmentation fault**. The issue occurred due to an incorrect parameter sent to a log function. The fix ensures the controllers perform as expected.	ArubaOS 8.10.0.7
AOS-249066 AOS-250718	The **auth** process crashed and reloaded, causing connectivity issues when more than 37 dormant IP addresses were associated with a single MAC address. The fix ensures the **auth** process works as expected. This issue is observed in controllers running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-249109	A ping latency while pinging the default gateway was observed on 9012 and 9004 gateways running ArubaOS 8.10.0.0 or later versions. This issue occurred because the response for every 15th ping packet was delayed as the system was busy gathering port statistics. The fix ensures that the ping latency for the gateways is reduced to 23 ms and 7 ms respectively.	ArubaOS 8.10.0.0
AOS-249127	9004 gateways crashed and rebooted unexpectedly. This issue occurred because of a **NULL** pointer user entry access. The fix ensures an addition of a **NULL** check before accessing the user entry. This issue was observed in gateways running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-249133 AOS-249273	Some 9240 controllers running ArubaOS 8.10.0.4 or later versions rebooted with **Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause: 86:34)**. This issue was caused by gradual memory leak within the **fpapps** process. The fix ensures the controllers perform as expected.	ArubaOS 8.10.0.4
AOS-249181	Some AP-535 access points rebooted unexpectedly. The log files listed the reason as **kernel panic: Take care of the TARGET ASSERT first**. The issue occurred because the interprocess communication buffers were not initialized when the spectral scan was started. The fix ensures APs work as expected. This issue was observed in APs running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-249197	Some AirGroup servers were not discovered by clients. Devices such as Mersive Solstice Pods did not appear in Apple clients' screen mirroring device list. This issue was related to AirGroup's refresh logic when using discovery packets and was seen when there were nine or more MDNS service profiles configured in the AirGroup profile. The fix ensures that servers are discovered by clients as expected. This issue was observed in managed devices running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-249260	Some Mobility Controller Virtual Appliance deployments crashed when running ArubaOS 8.10.0.7 or later versions. This issue was observed whenever the CLI password was passed as **NULL**. The fix ensures such deployments work as expected.	ArubaOS 8.10.0.7
AOS-249262 AOS-249847	Some AP-535 access points rebooted unexpectedly. The logs listed the reason as **kernel panic: Take care of the TARGET ASSERT first - wlan_wmi.c:653**. The fix ensures the APs perform as expected. This issue was observed in APs running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-249529	When a cluster member becomes reachable and the status of the peer changes to **DISCONNECTED**, there is a log entry indicating **peer disconnected**, like so: **<ERRS> |cluster_mgr| Peer x.x.x.x heartbeat missed, Disconnected**. This log was not available in controllers running ArubaOS 8.10.0.7 or later versions. This issue occurred due to modifications in the cluster heartbeat mechanism. The fix ensures the log is available.	ArubaOS 8.10.0.7
AOS-249749	Neighbor AP information was incomplete in the output of the **show ap arm state** command. The fix ensures the information is correctly displayed. This issue was observed in APs running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8
AOS-249815	Tunnel performance with MTU 1500 was poor. This issue was caused due to the AP's internal Traffic Allocation Framework (TAF). The fix includes an update to the AP driver, which resolves the tunnel performance problem. This issue was observed in controllers running ArubaOS 8.11.2.0 or later versions.	ArubaOS 8.11.2.0
AOS-249835	The external Captive Portal failed to load after running the **ap convert** command to migrate ArubaOS 8.x Remote APs to ArubaOS 10.x. The fix ensures that the APs function as expected when the **ap convert** command is run. This issue was observed in Central-managed Remote APs running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.10.0.9
AOS-249961	Handy terminals were unable to associate to some 300 Series access points running ArubaOS 8.10.0.7 or later versions. The issue was related to a conflict with the DoS prevention feature of ArubaOS, which, when enabled, prevented the AP driver from getting crucial data for device association. The fix ensures that terminals are correctly associated with access points.	ArubaOS 8.10.0.7

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-249976	The **show ap debug radio-stats**, **show ap debug bss-stats** commands and MIB (**wlanAPRxDataBytes64**) were showing Rx data byte values lower than the actual received values at 5 GHz. The fix ensures the values are accurate. This issue was observed in controllers running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-250031 AOS-251210	After upgrading to ArubaOS 8.10.0.9, some managed devices could not retrieve user-table information via API calls when using the **show user-table** command. The fix ensures API calls work as expected. This issue was observed in managed devices running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-250070	Some APs were unable to upgrade from ArubaOS 8.x to ArubaOS 10.x. The issue was related to APs getting stuck at the pre-validation stage. The fix ensures that APs can be upgraded successfully. This issue was observed in AP-615 access points running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-250144	AP-635 access points could not establish IPSec tunnels whenever EST certificates were used. Instead, the devices renewed their certificate repeatedly, causing the deletion of the tunnel by the controller. The issue was due to the APs being unable to read EST-related temporary data from their flash memory. The fix ensures APs can access that data and establish a tunnel connection through EST certificates successfully. This issue was observed in AP-635 access points running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-250346	Some AP-345 access points rebooted unexpectedly. The logs listed the reason as **AP Reboot reason: BadPtr:00000000 PC:0x0 Warm-reset**. The fix ensures the APs work as expected. This issue was observed in AP-345 access points running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-250349 AOS-241587	After upgrading to ArubaOS 8.11.2.1, some AirGroup printers were no longer discoverable, preventing users from connecting. The issue occurred because few of the AirGroup server records were being dropped while responding to user queries. The fix ensures all the available servers can be discovered by users. This issue was observed in controllers running ArubaOS 8.11.2.1 or later versions.	ArubaOS 8.11.2.1
AOS-250350	The **Resolve Wrap** process repeatedly crashed and restarted on some 9004-LTE gateways running ArubaOS 8.10.0.0 or later versions. This issue occurred when the **dnsmasq** configuration file contained unsupported characters and multiple domain names. The fix ensures that the **Resolve Wrap** process works as expected.	ArubaOS 8.10.0.0
AOS-250453	Some AP-535 access points running ArubaOS 8.10.0.8 or later versions aged out clients sooner than expected, in spite of the timer being set to allow for longer inactivity. The issue was related to the AP driver, which has been updated to prevent **station ageout timer** problems. The fix ensures APs work as expected.	ArubaOS 8.10.0.8

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-250608	Users experienced S2S VPN connection issues after changing the IP address on one of the VPNC ends. The issue occurred when the VLAN IP address was modified, which changed the source network IP address. The fix ensures controllers work as expected. This issue was observed in 7030 controllers running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-250722	Customers experienced poor quality voice calls on Ascom VoIP phones connected to AP-655 access points. The issue occurred due to a U-APSD power save issue. The fix ensures VoIP calls can be performed as expected. This issue was observed in APs running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-250875 AOS-251543	The **RULES COUNT** column under the **Configuration > Roles & Policies > role > Policies** section of the WebUI displayed a **0** for all roles. The fix ensures the WebUI displays an accurate rule count. This issue was observed in controllers running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-250924	Users experienced video lag issues on M2 and M3 MacBooks connected to AP-325 access points. The issue occurred when the AP returned an incorrect AMSDU flag in ADDBA response frames for non-open, non-PMF, and non-jumbo tunnel modes, which eventually hit the controller and dropped the frames. The fix ensures M2 and M3 MacBooks work as expected when connected to APs. This issue was observed in APs running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8
AOS-251011	Some AP-535 access points crashed and rebooted unexpectedly. This issue occurred because TXBF was enabled for 11a association. The issue was fixed by disabling TXBF for 11a mode association. This issue was observed on access points running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-251055	Some APs were unable to use SCP for dump server collection on IPv6. The fix ensures the AP works as expected. This issue was observed in APs running ArubaOS 8.10.0.6 or later versions.	ArubaOS 8.10.0.6
AOS-251090	The image upgrade history was not displayed for upgrades done through the WebUI when using the **show boot upgrade-history** command. The fix ensures the command output is displayed as expected. This issue was observed in controllers running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8
AOS-251130	The OID **sysExtFanStatus** on the 9240 controllers previously reported the status of the external fans as 2 (inactive) inaccurately. The fix improves the monitoring of fan status by utilizing ALARM signals and will now update the **sysExtFanStatus** value to 1 (active) when there is no ALARM, and to 2 when there is a MAJOR ALARM (indicative of 0 RPM or fan failure) for the fan. This issue was observed in controllers running ArubaOS 8.10.0.6 or later versions.	ArubaOS 8.10.0.6

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-251173	Some APs did not send the correct DHCP decline package type whenever there was an IP address conflict. The fix ensures the message type is sent in alignment with RFC-2131, which resolves the issue. This issue was observed in AP-315 access points running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-251213 AOS-251545 AOS-251648 AOS-251894 AOS-252417 AOS-252427	Some APs rebooted unexpectedly at random intervals. The log files listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures the APs work as expected. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.10.0.8
AOS-251612	The PIM module unexpectedly crashed, which caused a memory leak on 7240XM gateways. The fix ensures the PIM module works as expected. This issue was observed on 7240XM gateways running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-251905	Some Mobility Conductors did not display the OS type of managed devices in the WebUI dashboard. The fix ensures the OS type is displayed in the WebUI. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.6 or later versions.	ArubaOS 8.10.0.6
AOS-251934	Controllers under island node hierarchy, having a partial match in the node path and island index, were displayed in the **show airgroup switches** command output despite the AirGroup function being disabled. The fix ensures the command output is displayed as expected. This issue was observed in controllers running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-252017	Some AP-535 access points were sending the error message **wlan: [0:F:OBJMGR] wlan_objmgr_iterate_log_del_obj_handler: #peer in L-state, MAC** to the syslog servers. Although this condition did not cause immediate connectivity issues, it required the user to reboot the AP to stop the error messages. The fix ensures the APs perform as expected. This issue was observed in APs running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-252038	Some access points with HW-offload function unexpectedly deleted ARP table entries, which caused packets to be dropped. The fix ensures the AP works as expected. This issue was observed in AP-635, AP-655, AP-555, AP-535 access points running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-252186 AOS-251237	In the **Configuration > System > CPsec** page of the WebUI, the option **Only accept APs from specified ranges** did not display the table to add the ranges. The fix ensures the table is displayed as expected. This issue was observed in managed devices running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-252349	The Rx and Tx timestamps were inaccurate when running the **show ap debug client-table** command. The fix ensures the command displays the correct output. This issue was observed in APs running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0

Table 3: *Resolved Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-252424 AOS-253282 AOS-253299	The AP image conversion failed in controllers. The output of the **show ap convert-status** command shows **Pre Validate Failed** as the failure reason. This issue occurred when Central used an IPv6 address. The fix ensures controllers work as expected. This issue was observed in controllers running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9

Chapter 7
Known Issues in ArubaOS 8.10.0.11

This chapter describes the known issues observed in this release.

Known Issues

Following are the known issues observed in this release.

Table 4: *Known Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-205650 AOS-231536	DHCP traffic from relay agent is not forwarded through the next-hop list configured in Layer 3 GRE tunnel. This issue is observed in managed devices running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-209580	The output of the **show ap database** command does not display the **o** or **i** flags, which indicate whether an AP is an outdoor AP or an indoor AP. This issue occurs when the AP installation type is not set to default. This issue is observed in Mobility Conductors running ArubaOS 8.3.0.13 or later versions.	ArubaOS 8.3.0.13
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 ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219150	Mobility Conductor fails to push the SRC NAT pool configuration to managed devices. This issue occurs when the ESI redirect ACL is configured using the WebUI. This issue is observed in Mobility Conductors running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-221308	The **execute-cli** command does not work as expected for a few **show** commands. This issue is observed in Mobility Conductors running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-229024	Some AP-505 access points running ArubaOS 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]**.	ArubaOS 8.7.1.5
AOS-229770	Controllers may not display information on 802.1X connection statuses if 802.1X connection fails. This issue is observed in controllers running ArubaOS 8.7.1.8 or later versions.	ArubaOS 8.7.1.8
AOS-231283	The log files of few Wi-Fi 6E APs (630 Series and 650 Series access points) running ArubaOS 8.10.0.0 or later versions incorrectly display the **6G radio 2 disabled due to mfg configuration** message during reboot of the APs, even though the 6 GHz radio is not disabled when the APs boot up.	ArubaOS 8.10.0.0

Table 4: *Known Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-232092	Some AP-305 and AP-505 access points are not discoverable by Zigbee devices. The southbound traffic is giving the error in as **AP not found**. This issue is observed on devices running ArubaOS8.8.0.1 or later versions.	ArubaOS 8.8.0.1
AOS-232208 AOS-241285	The **Maintenance > Software Management > Upload AOS image for controller** page of the WebUI does not allow for image upgrades in OEM builds, yet the WebUI displays it as an option. This issue is observed in Mobility Controllers running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-232233	Some 9004-LTE controllers cache the LAN side MAC address during boot up. Thus, the gateway does not get an IP address from the modem. This issue is observed in controllers running ArubaOS 8.7.0.0 later versions.	ArubaOS 8.7.1.4
AOS-232875 AOS-239469	The **mon_serv** process crashes in certain high-load scenarios, particularly with a large number of APs and users with high roaming rates. The issue occurs in Mobility Controllers running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-233809	Users are unable to add GRE tunnels to a tunnel group and an incorrect error message **Error: Tunnel is already part of a different tunnel-group** is displayed. This issue is observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-233988 AOS-242222 AOS-252252	Wired clients are unable to ping each other on the same VLAN when the ACL is set to **user any any permit** policy. This issue occurs because SIP is used as the user for both forward and reverse session creation during session ACL lookup. This issue is observed in managed devices running ArubaOS 8.6.0.20 or later versions.	ArubaOS 8.6.0.20
AOS-236171	Some AP-635 access points running ArubaOS 8.10.0.5 or later versions crash due to a PoE power supply change from AF to AT.	ArubaOS 8.10.0.5
AOS-236200	Some AP-374 access points configured as mesh crash with reason: **kernel panic: Fatal exception**. This issue is observed in controllers running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-236852	The error **ofa: |ofa| ofa_gsm_ event_user_process: port not found:19, tnm50c4ddb3b194 end point is not configured or is down** is displayed when a client connects to an IAP-VPN tunnel. This issue is observed in Mobility Conductors running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-237174	Some 9240 controllers record informational logs, even though the system log level is configured as **warning**. This issue is observed in controllers running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-238407 AOS-236630 AOS-240428 AOS-241047	AppRF application or application category ACL is not blocking YouTube on devices connected to APs running ArubaOS 8.6.0.16 or later versions.	ArubaOS 8.6.0.16

Table 4: *Known Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-238846	The error message **Exceeds the max supported vlans 128** displays when creating Layer 2 VLANs at folder level. This issue is observed in Mobility Conductors running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-239521	Users are unable to add a tunnel to a tunnel group and an error message **Error: All tunnels must have same vlan membership** is displayed. 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 ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-239724 AOS-239529	Some APs unexpectedly increase the response time when using DHCP configuration. This issue is observed in APs running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-239814 AOS-239815	In some controllers running ArubaOS 8.6.0.11 or later versions, IPv4 and IPv6 accounting messages are using the same session ID with Passpoint. This causes multiple accounting messages to be sent repeatedly.	ArubaOS 8.6.0.11
AOS-241212 AOS-241537	Some 7220 controllers running ArubaOS 8.10.0.4 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Nanny rebooted machine - low on free memory**.	ArubaOS 8.10.0.4
AOS-242532	Some AP-535 access points are not available on 7210 controllers post power outage. This issue occurs when a USB converter and console cable are used, which interrupts the boot up process and results in the AP not showing up on the controller. The issue is observed in controllers running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-243266	APs upgraded through TFTP get stuck in **Upgrading** status due to an incorrect automatic change of UDP ports. This issue is observed in Mobility Controllers running ArubaOS 8.6.0.20 or later versions.	ArubaOS 8.6.0.20
AOS-243536	Some Mobility Controllers running ArubaOS 8.0.0.0 or later versions display incorrect values in **Discovery State** and **Transport State** for AirGroup services, after running the **show airgroup switches** command. This issue occurs due to a race condition. Therefore, users connected to the affected APs are unable to use AirGroup services.	ArubaOS 8.10.0.6
AOS-244193	Some AP-655 access points are frequently bootstrapping. The issue occurs due to a interoperability issue of the APs firmware with certain third-party-switches. The issue is observed in access points running ArubaOS 8.10.0.6 or later versions.	ArubaOS 8.10.0.6
AOS-244210	Users are unable to configure a negative value for the transmit power setting in the **Overview > Profiles > IoT Profile > BLE Transmit Power** page of the WebUI. This issue is observed in Mobility Controllers running ArubaOS 8.10.0.6 or later versions.	ArubaOS 8.10.0.6

Table 4: *Known Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-244965	An unnecessary debugging log appears as **Received ICMP (DEST_UNREACH, PROT_UNREACH) from X.X.X.X for heartbeat tunnel**. This issue is observed in controllers running ArubaOS 8.10.0.5 or later versions.	ArubaOS 8.10.0.5
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 Master role, but this error is not reported properly. This issue is observed in controllers running ArubaOS 8.10.0.5 or later versions.	ArubaOS 8.10.0.5
AOS-245414	SNMP queries to controllers return valid traffic data for GigE interfaces but might show all zeroes for GRE tunnel interfaces. This issue is observed on Mobility Controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.6.0.17
AOS-245777	In the controller **Dashboard > Overview > Clients** page of the WebUI, applying the **Grouped by signal quality** filter does not correctly organize the client data or display the graph based on signal quality. This issue is observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-246103 AOS-247433 AOS-240688 AOS-250837	Some AP-635 and AP-535 access points reboot randomly with **reboot reason - kernel panic: Take care of the TARGET ASSERT at ar_wal_tx_send.c:11778 first**. This occurs due to issues with M3 controllers recovery, to which the APs are connected. This issue is observed in APs running ArubaOS 8.10.0.5 or later versions.	ArubaOS 8.10.0.5
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 ArubaOS 8.10.0.0 or later versions.	ArubaOS 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 ArubaOS 8.6.0.21 or later versions. **Workaround:** Reload the managed device or restart the **profmgr** process to fix the issue.	ArubaOS 8.6.0.21
AOS-247721	Mobility Conductor in a standby setup fails over and crashes unexpectedly. The log files list the reason as **Datapath Exception**. This issue is observed in Mobility Conductor running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-247793	Some AP-535 access points crash and reboot unexpectedly. The log file lists the reason for reboot as **AP crashed at ar_wal_vdev.c:3320 Assertion vdev_handle->type == WAL_VDEV_TYPE_STA**. This issue is observed in access points running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0

Table 4: *Known Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-248466	The controller discovery preference field disappears when changing it from ADP to Static, under **Dashboard > Configuration > Access Point > Provision** page of the WebUI. This issue is observed in controllers running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8
AOS-248899	The syslog server of some wireless controllers is flooded with error messages related to OpenFlow. Logs such as **ofa: <238503> <5843> |ofa| |sdn| ERRS ofml_openflow_mac_bridge_add_ap:322 AP client(mac-address) not found** are repeatedly displayed on controllers with varying MAC addresses. These errors are related to roaming when connected to a Remote AP, and can be safely ignored. This issue is observed in controllers running ArubaOS 8.10.0.7 or later versions.	ArubaOS 8.10.0.7
AOS-248905	Clients are assigned the wrong role when reconnecting to WPA3 Enterprise (GCM) SSIDs, in both CNSA and non-CNSA mode. The issue is related to PMK caching as part of dot1x authentication. This issue is observed in controllers running ArubaOS 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.	ArubaOS 8.10.0.0
AOS-249361 AOS-247054 AOS-252702 AOS-253220 AOS-247632	A few boot arguments are missing for 9000 Series and 9004-LTE gateways. This issue occurs after the gateways were upgraded to ArubaOS 8.10.0.7. This issue is observed in gateways running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.7
AOS-249568	Rules added from the **Configuration > Roles & Policies > Roles > role > Rules of this Role only** section of the WebUI are not displayed after being added. This issue is observed in controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.10.0.7
AOS-250148	AirGroup's **Transport State** gets stuck on **initializing** status. The issue is related to the current handling of OpenFlow flows in AOS SDN controllers. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.0.0.0
AOS-250612	Some discrepancies in license usage reporting are noted between global and lower-level pools in setups with Mobility Conductors, managed devices, and Campus APs. This issue is observed in managed devices running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.9
AOS-250773	AirWave is seeing delayed or missing SNMP responses from some controllers, causing SNMP timeouts. As a result, AirWave incorrectly marks a controller as down, prompting the controller to send an error message stating **WARN> |snmp| Processing of GET(next) request failed**. This issue is observed in 7210 controllers running ArubaOS 8.10.0.6 or later versions.	ArubaOS 8.10.0.6

Table 4: *Known Issues in ArubaOS 8.10.0.11*

New Bug ID	Description	Reported Version
AOS-250876	The J8177D, a 1G SFP RJ45 T 100m Cat5e, transceiver manufactured in Taiwan does not work on 7200 controllers, whereas the J8177D manufactured in the United States works fine. This issue is observed in controllers running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9
AOS-250883	When a logging server type was deleted, it causes the removal of all other logging types from the **show running-config** and **show logging server** commands' output. This issue is observed in controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.10.0.5
AOS-251605 AOS-241347	Wired AirGroup servers might disappear from the AirGroup server table when GE/PC ports are deactivated. This issue was observed on Mobility Controllers running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.9
AOS-251742 AOS-252082	Users experience increased latency in applications with short, bursty traffic patterns when connected to APs. This issue is observed in AP-515 and AP-505 access points running ArubaOS 8.10.0.8 or later versions.	ArubaOS 8.10.0.8
AOS-252656	Some controllers do not report client count through SNMP OID in 6 GHz connections. This issue is observed in controllers running ArubaOS 8.9.0.0 or later versions.	ArubaOS 8.10.0.8
AOS-252798	The **OFA** process crashes on controllers running ArubaOS 8.10.0.10 or later versions after a RAP deployment. The issue occurs due to a segmentation fault while deleting a client object from the OFML library.	ArubaOS 8.10.0.10
AOS-252888	In some controllers, a **list index out of range exception** error is seen when a **netdestination** alias is configured. This issue is observed in controllers running ArubaOS 8.10.0.9 or later versions.	ArubaOS 8.10.0.9

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 ArubaOS runs on your managed device?
  - Are all managed devices running the same version of ArubaOS?
  - 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 ArubaOS 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 ArubaOS, 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 ArubaOS 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-ArubaOS 8.10.0.0 MultiVersion support.

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

Memory 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:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 35 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 35 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 35 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Low Free Flash Memory

Sometimes, after extended use, the flash memory might get used up for logs and other files. The ArubaOS image has increased in size and this may cause issues while upgrading to newer ArubaOS 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 ArubaOS 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 ArubaOS upgrade. See Upgrading ArubaOS.
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 controller. If any of the errors listed in step 4 were observed, the following errors might occur while booting ArubaOS 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 ArubaOS upgrade procedure. See Upgrading ArubaOS.
- 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 ArubaOS upgrade procedure in the same partition. See Upgrading ArubaOS.

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 ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 32.

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 ArubaOS from a TFTP server, FTP server, or local file.

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

4. Log in to the ArubaOS 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 ArubaOS from a TFTP server, FTP server, or local file.

1. Download the ArubaOS 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 ArubaOS 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 ArubaOS Upgrade

Verify the ArubaOS 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 ArubaOS 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 35 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 ArubaOS 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 35 for information on creating a backup.

Downgrading ArubaOS

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 ArubaOS version, perform the following steps:

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 35.

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 ArubaOS version.

When you specify a boot partition or copy an image file to a system partition, Mobility Conductor or managed device checks if the ArubaOS version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the ArubaOS 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 ArubaOS 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 ArubaOS version.
- If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

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

In the CLI

The following steps describe how to downgrade the ArubaOS 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 ArubaOS 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 ArubaOS 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.