ArubaOS 8.6.0.10 Release Notes

a Hewlett Packard
Enterprise company

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code 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, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Chapter 1
Revision History

The following table provides the revision history of this document.

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

For a list of terms, refer Glossary.

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 Master Licensing 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:

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

Terminology Change

As part of advancing 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	https://asp.arubanetworks.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
New Features and Enhancements in ArubaOS 8.6.0.10

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

Chapter 4
Supported Platforms in ArubaOS 8.6.0.10

This chapter describes the platforms supported in this release.

Mobility Master Platforms

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

Table 3: *Supported Mobility Master Platforms in ArubaOS 8.6.0.10*

Mobility Master Family	Mobility Master Model
Hardware Mobility Master	MM-HW-1K, MM-HW-5K, MM-HW-10K
Virtual Mobility Master	MM-VA-50, MM-VA-500, MM-VA-1K, MM-VA-5K, MM-VA-10K

Mobility Controller Platforms

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

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.6.0.10*

Mobility Controller Family	Mobility Controller Model
7000 Series Hardware Mobility Controllers	7005, 7008, 7010, 7024, 7030
7200 Series Hardware Mobility Controllers	7205, 7210, 7220, 7240, 7240XM, 7280
9000 Series Hardware Mobility Controllers	9004
MC-VA-xxx Virtual Mobility Controllers	MC-VA-50, MC-VA-250, MC-VA-1K

AP Platforms

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

Table 5: *Supported AP Platforms in ArubaOS 8.6.0.10*

AP Family	AP Model
100 Series	AP-104, AP-105
103 Series	AP-103

Table 5: *Supported AP Platforms in ArubaOS 8.6.0.10*

AP Family	AP Model
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135
170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1
200 Series	AP-204, AP-205
203H Series	AP-203H
205H Series	AP-205H
207 Series	AP-207
203R Series	AP-203R, AP-203RP
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303 Series	AP-303, AP-303P
303H Series	AP-303H
310 Series	AP-314, AP-315
318 Series	AP-318
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377
AP-387	AP-387
500 Series	AP-504, AP-505
510 Series	AP-514, AP-515
530 Series	AP-534, AP-535
550 Series	AP-555

Table 5: *Supported AP Platforms in ArubaOS 8.6.0.10*

AP Family	AP Model
RAP 3 Series	RAP-3WN, RAP-3WNP
RAP 100 Series	RAP-108, RAP-109
RAP 155 Series	RAP-155, RAP-155P

Chapter 5
Regulatory Updates in ArubaOS 8.6.0.10

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 https://asp.arubanetworks.com/.

The following DRT file version is part of this release:

- DRT-1.0_80561

Chapter 6
Resolved Issues in ArubaOS 8.6.0.10

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-183519	—	Some APs were incorrectly marked as down in datazone controllers. The fix ensures that the controllers display the correct status of APs. This issue was observed in stand-alone controllers running ArubaOS 8.3.0.4 or later versions.	ArubaOS 8.3.0.4
AOS-197323 AOS-212920	—	The **Dashboard > Infrastructure** page of the WebUI did not display the static channel details assigned to an AP. The fix ensures that the WebUI displays the static channel details assigned to an AP. This issue was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-199403 AOS-218203	—	Some managed devices running ArubaOS 8.6.0.7 or later versions were down after a failover. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.7
AOS-201718 AOS-217092	—	Users were unable to view the WLAN and client details using WebUI and an error message, **Error retrieving information please try again later** was displayed. The fix ensures that the WebUI displays the WLAN and client details. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-201831	—	The **S-UAC** process in a cluster member sent the **fdb-update-on-assoc** message sporadically. This issue is resolved by sending the **fdb-update-on-assoc** message only when **fdb-update-on-assoc** is enabled and the station is not dormant. This issue was observed in managed devices running ArubaOS 8.5.0.5 in a cluster topology.	ArubaOS 8.5.0.5
AOS-202210 AOS-218532	—	The **show iap table** and **show iap table long** commands did not display the list of Instant APs. The fix ensures that the commands display the list of Instant APs. This issue was observed in controllers running ArubaOS 8.6.0.6 or later versions in a VPNC deployment.	ArubaOS 8.6.0.6
AOS-202247 AOS-218834	—	Some APs running ArubaOS 8.5.0.10 crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Reason: Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.10

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-202308 AOS-216193 AOS-219439	—	A few clients took a long time to roam between APs. The fix ensures that clients do not take a long time to roam between APs. This issue was observed in stand-alone controllers running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-203077 AOS-203232	—	Configurations committed using the **firewall cp** command were not synchronized on the standby Mobility Master. This issue occurred when static firewall entries were deleted. The fix ensures that the configurations are synchronized on the standby Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.6.0.3 or later versions.	ArubaOS 8.6.0.3
AOS-203115 AOS-217219	—	The IAP-VPN tunnel went down and the error message, **Failed to create internal-iap IP user entry and user entry due to too many user entries 128** was displayed. This issue occurred when the user table had 128 entries. The fix ensures that the stand-alone controllers work as expected. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-203517 AOS-204709 AOS-213765 AOS-221056	—	The **datapath** process crashed on managed devices running ArubaOS 8.3.0.7 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.3.0.7
AOS-204187	—	The command **vpn-peer peer-mac** did not support Suite-B cryptography for custom certificates. The fix ensures that the command supports Suite-B cryptography for custom certificates. This issue was observed in Mobility Masters running ArubaOS 8.2.2.8 or later versions.	ArubaOS 8.2.2.8
AOS-204241	—	Some managed devices logged spurious DHCP DBUG messages. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-206216 AOS-213940 AOS-214072 AOS-220300	—	Some APs running ArubaOS 8.6.0.6 crashed unexpectedly. The log file listed the reason for the event as, **reboot caused by Firmware Assert - ar_wal_tx_de.c:68**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.6
AOS-206293 AOS-220915	—	Some AP-535 access points running ArubaOS 8.6.0.6 or later versions crashed unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.6
AOS-206389 AOS-216860	—	The **SAPD** process crashed on managed devices running ArubaOS 8.6.0.5 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.5

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206537	—	The **H** flag indicating standby tunnel was not displayed in the output of the **show datapath tunnel-table** command and this resulted in a network loop. The fix ensures that the **H** flag is displayed in the output of the **show datapath tunnel-table** command. This issue was observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206907	—	Some AP-303H access points running ArubaOS 8.5.0.5 or later versions crashed and rebooted unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: assert.** The fix ensures that the APs work as expected.	ArubaOS 8.5.0.5
AOS-207691	—	CLI displayed an incorrect IP address for a TACACS server. The fix ensures that the CLI displays the correct IP addresses for TACACS servers. This issue was observed in managed devices running ArubaOS 8.3.0.8 or later versions.	ArubaOS 8.3.0.8
AOS-207775 AOS-215946	—	The **auth** process crashed on managed devices running ArubaOS 8.5.0.9 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.9
AOS-207841 AOS-217633	—	Some managed devices running ArubaOS 8.7.0.1 or later versions experienced configuration failures. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.0.1
AOS-208420	—	Users were unable to log in to the CLI of a controller. This issue occurred when the password had special characters, < and/or >. The fix ensures that users are able to log in to CLI of a controller. This issue was observed in controllers running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.5
AOS-208740 AOS-213754	—	The **profmgr** process crashed on a few Mobility Masters running ArubaOS 8.5.0.11 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.5.0.11
AOS-208846	—	Clients connected to bridge mode SSIDs were unable to receive IP addresses and pass traffic. The fix ensures that clients are able to receive IP addresses. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209136	—	A few clients were disconnected due to the **Tx fail reached maximum** error. This issue occurred due to an incorrect state of variables in the AP while peer STA is in power save state, which lead to the packets being sent out when the peer STA was also in power save state. Since the peer STA was in power save state, it did not acknowledge the packets and the AP exhausted the maximum retries and disconnected the clients. The fix ensures that the state of variables in APs power save state machine is updated correctly. This issue was observed in AP-315 access points running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-209165		The **Configuration > AP Groups** page did not sort the list of AP groups based on when they were created, and hence the newly created AP groups were displayed at the bottom of the table. The fix ensures that the WebUI sorts the list of AP groups. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-209879 AOS-220470	—	The **trusted vlan add** command removed all the existing trusted VLANs. The fix ensures that the **trusted vlan add** command does not remove all the existing trusted VLANs. This issue was observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-209936 AOS-215097	—	Mobility Masters running ArubaOS 8.6.0.6 or later versions displayed some BSSIDs as rouge BSSIDs even after manually white-listing the BSSIDs. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.6.0.6
AOS-210638	—	The **ARM** process crashed on managed devices running ArubaOS 8.6.0.5 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.5
AOS-210922	—	The **auth** process crashed on stand-alone controllers running ArubaOS 8.5.0.10 or later versions and APs rebooted unexpectedly. The log file listed the reason for the reboot as **Unable to set up IPSec tunnel, Error:RC_ERROR_IKEV2_TIMEOUT**. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.5.0.10
AOS-210963	—	Some AP-203R access points running ArubaOS 8.7.0.0 or later versions did not send wireless tarpit / deauth frames even if IDS wireless containment was configured. The fix ensures that the APs work as expected.	ArubaOS 8.7.0.0
AOS-211578 AOS-219595	—	The bucketmap was not updated for a specific BSSID of an AP. The fix ensures that the bucketmap is updated. This issue was observed in APs running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-211622 AOS-211728 AOS-220433 AOS-222658	—	Some stand-alone controllers running ArubaOS 8.3.0.14 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:0:2c)**. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.3.0.14
AOS-211730 AOS-220327	—	Users were unable to map server certificate as switch certificate on a secondary Mobility Master running ArubaOS 8.5.0.10 or later versions. The fix ensures that users are able to map server certificate as switch certificate on a secondary Mobility Master.	ArubaOS 8.5.0.10
AOS-211861 AOS-219057	—	The whitelist database was downloaded successfully from the Activate server only after a restart of the **CPSec** process. The fix ensures that the whitelist database was downloaded successfully without a restart of the **CPSec** process. This issue was observed in Mobility Masters running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-211878 AOS-214377	—	Some APs failed to come up as Remote APs. This issue occurred when the MTU size was not adjusted automatically. The fix ensures that APs come up as Remote APs. This issue was observed in APs running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212198	—	Some RAP-3WN Remote APs running ArubaOS 8.5.0.8 or later versions rebooted unexpectedly. This issue occurred when the time between the controller and the Remote AP was not in synchronization. The fix ensures that the Remote APs work as expected.	ArubaOS 8.5.0.8
AOS-212310 AOS-219441	—	The **WebCC** and **NTPd** processes were in busy state in stand-alone controllers running ArubaOS 8.5.0.12 or later versions. This issue occurred when a DNS server or an NTP Server was unreachable. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.5.0.12
AOS-212904	—	Users were unable to access the L3 redundant controller using the CLI and the error message, **Permission path (/) is Invalid for user (ads.jvicentini)** was displayed. The fix ensures that the users are able to access the L3 redundant controller using CLI. This issue was observed in standby Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212935	—	Temporary ACL was applied to user roles even if the disaster-recovery mode was disabled. This issue occurred when configuration changes in disaster-recovery mode were not submitted using the **write memory** command. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.3.0.6 or later versions.	ArubaOS 8.3.0.6
AOS-212936	—	Some users experienced network outage. The fix ensures that the users do not experience network outage. This issue was observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-213011 AOS-219946	—	Packet loss was observed for a few clients during a cluster failover. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.10
AOS-213041 AOS-215501	—	A managed device did not classify WebCC and DPI traffic. The fix ensures that the managed device classifies WebCC and DPI traffic. This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-213115	—	Some managed devices running ArubaOS 8.5.0.10 crashed and rebooted unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first.** The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.10
AOS-213305 AOS-213310	—	Some APs crashed and rebooted unexpectedly. The log file lists the reason for the event as **PC is at wlc_nar_dotxstatus+0x88/0x7d8: AOS-200674 instrumentation kicks in (wlc_nar_validate_cubby).** The fix ensures that the APs work as expected. This issue was observed in AP-515 access points running ArubaOS 8.7.0.0 or later versions	ArubaOS 8.7.0.0
AOS-213307	—	L2 GRE ICMP keepalive response was sent outside the tunnel and hence, it was dropped by the firewall. This issue was observed in managed devices running ArubaOS 8.5.0.1 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.6
AOS-213337	—	A few AP-325 access points running ArubaOS 8.5.0.10 or later versions crashed unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.10

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213492	—	Some APs running ArubaOS 8.6.0.6 logged the error message, **assoc response: try later** when MBO was enabled. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.6
AOS-214243 AOS-215775	—	Some managed devices running ArubaOS 8.6.0.7 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**. This issue occurred due to a race condition. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.7
AOS-214391 AOS-217130 AOS-217832	—	The **STM** process crashed on managed devices running ArubaOS 8.6.0.5 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.8
AOS-214434	—	Some APs were unable to come up on a managed device. This issue occurred when UDP 8209 traffic was sent without establishing IPsec tunnels. The fix ensures that the APs are able to come up on a managed device. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-214510 AOS-219139	—	A few clients were disconnected from the network. The log files listed the reason for the event as **Wlan driver excessive tx fail quick kickout**. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-214829	—	Some AP-115 access points running ArubaOS 8.3.0.0 did not come up on a controller. This issue occurred when 802.1X authentication was enabled. The fix ensures that APs are able to come up on a controller.	ArubaOS 8.3.0.0
AOS-214963	—	Some APs running ArubaOS 8.5.0.11 or later versions detected false radar. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.11
AOS-214977 AOS-220420	—	Memory leak was observed in **arci-cli-helper** process. This issue occurred while running an API script. The fix ensures that the APs work as expected. This issue was observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-215012 AOS-215567	—	The AP debug counters, **Total Bootstraps** and **Reboots** were not reset after upgrading the managed devices to ArubaOS 8.5.0.11 or later versions. The fix ensures that the AP debug counters get reset. This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-215021	—	The **Channel Width Capability** configured on AirWave was not available in the **Dashboard > Overview > Wireless Clients** page of the WebUI. The fix ensures that the WebUI displays the **Channel Width Capability**. This issue is observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-215048 AOS-218412	—	A few clients were unable to connect to 802.1X SSIDs. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-215073	—	Some AP-515 access points running ArubaOS 8.5.0.8 or later versions went down and kept rebooting. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.8
AOS-215495	—	Some AP-535 access points running ArubaOS 8.5.0.5 or later versions displayed the error message, **ARM Channel 40 Physical_Error_Rate 0 MAC_Error_Rate 84 Frame_Retry_Rate 0 arm_error_rate_threshold 70 arm_error_rate_wait_time 90**. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.5
AOS-215498	—	Some AP-535 access points running ArubaOS 8.5.0.11 or later versions detected false radar. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.11
AOS-215857 AOS-216162	—	Some AP-514 and AP-515 access points running ArubaOS 8.4.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for reboot as, **AP Reboot reason: Warm-reset**. This issue occurred due to a beacon inactivity loop condition in the 5 GHz radio. The fix ensures that the 5 GHz radio does not encounter beacon inactivity and the AP works as expected.	ArubaOS 8.7.1.1
AOS-216512	—	The DHCP client / station related AMON message sent the mask, server IP address, and client IP address in a reverse order to the AirWave server. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-216752 AOS-217439 AOS-217893	—	The **impystart** process crashed on a Mobility Master Virtual Appliance. The fix ensures that the Mobility Master Virtual Appliance works as expected. This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.5.0.4 or later versions.	ArubaOS 8.5.0.4
AOS-216764	—	Users were not redirected to the captive portal page. The fix ensures that the captive portal works as expected. This issue was observed in managed devices running ArubaOS 8.7.1.0 or later versions in a cluster setup.	ArubaOS 8.7.1.0

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216766	—	Some APs generated sapd coredump. The fix ensures that the APs work as expected. This issue was observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-216972	—	Some managed devices running ArubaOS 8.6.0.7 or later versions forwarded data frames that are larger than the configured IPsec tunnel MTU value. The fix ensures that the managed devices do not forward data frames that are larger than the configured IPsec tunnel MTU value.	ArubaOS 8.6.0.7
AOS-217106	—	The **no valid** parameter of the **ap regulatory-domain-profile** command did not work while creating a new regulatory profile. The fix ensures that the **no valid** parameter of the **ap regulatory-domain-profile** command works as expected. This issue was observed in controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.6.0.7
AOS-217382	—	VRRP flapping was observed in a few Mobility Masters. This issue occurred when the VRRP master could not send periodic advertisements. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-217539 AOS-219010 AOS-219952 AOS-220918 AOS-221298	—	The **auth** process crashed on managed devices running ArubaOS 8.6.0.6 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.6
AOS-217678 AOS-218131	—	Some APs did not honor the user alias route src-nat ACL and tunneled the traffic to managed devices. The issue occurred when a netdestination alias was configured in the ACL. The fix ensures that the APs work as expected. This issue is observed in APs running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-217694 AOS-218525 AOS-220916	—	Some APs running ArubaOS 8.7.1.1 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.1
AOS-217703	—	Some managed devices took a long time to boot up after an upgrade. The fix ensures that the managed devices do not take a long time to boot up. This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-217807	—	Some Remote APs took a long time to come up on a managed device. This issue occurred due to a delay in whitelist-db synchronization between the Mobility Master and managed devices and when external authentication was enabled for Remote APs. The fix ensures that the Remote APs do not take a long time to come up on a managed device. This issue was observed in managed devices running ArubaOS 8.6.0.5 or later versions in a cluster setup.	ArubaOS 8.6.0.5
AOS-218012	—	The **Maintenance** tab of the WebUI displayed a list of clusters that were not configured for that particular node. The fix ensures that the WebUI displays the correct information. This issue was observed in Mobility Masters running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-218070	—	The **auth** process crashed on managed devices running ArubaOS 8.6.0.0 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.0
AOS-218117 AOS-219179	—	The **show ntp servers** and **show ntp status** commands displayed the error message, **Address family for hostname not supported**. However, the WebUI displayed the NTP servers. The fix ensures that the commands do not display the error message. This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-218167	—	Users were unable to delete static OSPF aggregate routes. The fix ensures that the users are able to delete static OSPF aggregate routes. This issue was observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-218208	—	Some clients were unable to connect to APs. The log file listed the reason for the event as, **AP is resource constrained**. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-218277 AOS-214428	—	The **auth** process crashed on managed devices running ArubaOS 8.5.0.11 or later versions. Hence, the Remote APs rebooted and VIA users faced connectivity issues. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.11
AOS-218404 AOS-212330	—	Some APs were unable to ping a few clients. The fix ensures that the APs are able to ping the clients. This issue was observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218488 AOS-219694	—	The management VLAN address of the Mobility Master was pointing to the Remote AP tunnel. The fix ensures that the management VLAN address is not available in the Remote AP tunnel. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-218518 AOS-218880 AOS-222186 AOS-222204	—	Some managed devices running ArubaOS 8.7.1.0 or later versions crashed unexpectedly. The log files listed the reason for the event as **Reboot reason Datapath timeout (SOS Assert).** The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.0
AOS-218622	—	Some APs running ArubaOS 8.6.0.6 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC:aruba_wlc_ratesel_ getcurrate+0x24/0xd0 [wl_v6] Warm-reset**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.1
AOS-218646	—	Ascom i63 phones connected to AP-515 access points running ArubaOS 8.6.0.7 or later versions experienced degraded audio quality. The fix ensures that the clients do not experience degraded audio quality.	ArubaOS 8.6.0.7
AOS-218822	—	High flash memory utilization was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.5.0.10
AOS-219008	—	Some UI endpoints like API page and spectrum page displayed information even before authentication. This issue was observed when the API request came over port 443. The fix ensures that the managed devices work as expected.	ArubaOS 8.8.0.0
AOS-219034	—	Clients connected to HT-enabled SSIDs connected as non-HT clients. The fix ensures that the APs work as expected. This issue is observed in APs running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-219098 AOS-219914	—	Some devices were unable to connect to the network. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219178	—	Clients connected to the anchor controller were unable to receive IP addresses. The fix ensures that the clients are able to receive IP addresses. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-219214	—	The validuser acl list was reordered in stand-alone controllers running ArubaOS 8.6.0.8 or later versions. The fix ensures that the validuser acl list is not reordered.	ArubaOS 8.6.0.8

Table 6: *Resolved Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219328	—	SNMP configurations failed and the error message, **Error: User (itam_net) should be created before adding to the trap host** was displayed. This issue occurred when the SNMP server v3 trap host which had the engine-id same as the engine-id of the controller was removed and added again. The fix ensures that the SNMP configurations do not fail. This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-219384	—	Some APs running ArubaOS 8.7.1.1 or later versions crashed unexpectedly. The log files listed the reason for the event as **PC is at wlc_nar_dotxstatus+0x450**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.1
AOS-219423	—	Honeywell Handheld 60SL0 devices were unable to connect to 802.1X SSIDs. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-219627 AOS-218851	—	Clients were unable to connect to 2.4 GHz SSID of some APs. This issue occurred when the MAC address of the Radio 1 was incorrect. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219978 AOS-220568	—	iPhone 12 Pro users experienced poor upstream network performance. This issue occurred when APs operated in tunnel mode. The fix ensures optimal network performance. This issue was observed in APs running ArubaOS 8.6.0.9 or later versions in tunnel mode.	ArubaOS 8.7.1.2
AOS-220398	—	A few clients in bridge mode were unable to connect to WPA2-PSK SSIDs. The fix ensures that the clients in bridge mode are able to connect to WPA2-PSK SSIDs. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-221478 AOS-221569 AOS-221572	—	The **auth** process crashed on managed devices running ArubaOS 8.5.0.9 or later versions. This issue occurred when the **show auth-tracebuf mac** command was executed. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.9

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

Limitation

Following are the limitations observed in this release:

Port-Channel Limitation in 7280 Controllers

On 7280 controllers with all the member ports of each port-channel configured from the same NAE (Network Acceleration Engine), if one of the member ports experiences link flap either due to a network event or a user driven action, the rest of the port-channels also observe the link flap for less than a second.

No Support for Unique Local Address over IPv6 Network

The IPv6 addresses for interface tunnels do not accept unique local addresses.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** command displays incorrect session count. This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions.	ArubaOS 8.1.0.0
AOS-151355	185602	A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.	ArubaOS 8.0.1.0
AOS-153742 AOS-194948	188871	A stand-alone controller crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in 7010 controllers running ArubaOS 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.5.0.1

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-155404 AOS-207878	191106	An AP is unable to establish IKE/IPsec tunnel with the managed device. This issue occurs when the AP is enrolled with EST certificates. This issue is observed in AP-515 access points running ArubaOS 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.6.0.4
AOS-156068	192100	The **DDS** process in a managed device running ArubaOS 8.2.1.1 or later versions crashes unexpectedly.	ArubaOS 8.2.1.1
AOS-157472 AOS-209050	—	The MAC address of the AP is not present in the called-station-ID of RADIUS accounting messages. This issue is observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-182847	—	A few users are unable to copy the **WPA Passphrase** field and **High-throughput** profile to a new SSID profile in the **Configuration > System > Profiles > Wireless LAN > SSID > <SSID_Profile>** option of the WebUI. This issue occurs when a new SSID profile is created from an existing SSID profile using WebUI. This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.4.0.0
AOS-184947 AOS-192737	—	The jitter and health score data are missing from the **Dashboard > Infrastructure > Uplink > Health** page in the WebUI. This issue is observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions.	ArubaOS 8.4.0.4
AOS-185538 AOS-195334	—	High number of EAP-TLS timeouts are observed in a managed device. This issue occurs when multiple IP addresses are assigned to each client. This issue is observed in managed devices running ArubaOS 8.3.0.8 or later versions.	ArubaOS 8.3.0.8
AOS-188972 AOS-194746 AOS-208631 AOS-213627	—	Mobility Master displays the blacklisted clients although the clients were removed from the managed device. This issue is observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions in a cluster setup.	ArubaOS 8.4.0.4
AOS-190071 AOS-190372	—	A few users are unable to access websites when WebCC is enabled on the user role. This issue occurs in a Per-User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in 7005 controllers running ArubaOS 8.4.0.0. **Workaround:** Perform the following steps to resolve the issue: 1. Remove web category from the ACL rules and apply **any any any permit** policy. 2. Disable WebCC on the user role.	ArubaOS 8.4.0.0

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
		3. Change the VLAN of user role from trunk mode to access mode.	
AOS-192725	—	The **Dashboard > Overview** page of the WebUI displays incorrect number of users intermittently. This issue is observed in Mobility Masters running ArubaOS 8.3.0.8 or later versions. **Duplicates:** AOS-188255, AOS-190476, AOS-190946, AOS-193586, AOS-194784, AOS-196004, AOS-200375, and AOS-210787	ArubaOS 8.3.0.8
AOS-193184	—	All L2 connected managed devices move to L3 connected state after an upgrade. This issue is observed in managed devices running ArubaOS 8.5.0.2 or later versions.	ArubaOS 8.5.0.2
AOS-193560	—	The number of APs that are DOWN are incorrectly displayed in the **Dashboard > Overview** page of the WebUI. However, the CLI displays the correct status of APs. This issue is observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions. **Duplicates**: AOS-198565, AOS-200262, AOS-204794, AOS-212249, AOS-208110, AOS-209989, and AOS-212249	ArubaOS 8.4.0.4
AOS-193775 AOS-194581 AOS-197372	—	A mismatch of AP count and client count is observed between the Mobility Master and the managed device. This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.5.0.2
AOS-193883 AOS-197756	—	A few APs are unable to use DHCP IPv6 addresses and option 52 for master discovery. This issue occurs when APs did not clear the previous LMS entries after an upgrade. This issue is observed in access points running ArubaOS 8.3.0.8 or later versions. **Workaround:** Delete the IPv4 addresses from ap system profile using the command, **ap system-profile** and from high availability profiles using the command, **ha.**	ArubaOS 8.3.0.8
AOS-194381	—	Some managed devices lose the route-cache entries and drop the VRRP IP addresses sporadically. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-194911	—	Incorrect flag output is displayed for APs configured with 802.1X authentication when the **show ap database** command is executed. This issue is observed in APs running ArubaOS 8.5.0.2 or later versions.	ArubaOS 8.5.0.2
AOS-194964	—	A few users are unable to clone configuration from an existing group to a new group in a Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.4.0.1 or later versions.	ArubaOS 8.5.0.2

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
		Workaround: Execute the **rf dot11a-radio-profile <profile name>** command to change the operating mode of the AP from am-mode to ap-mode.	
AOS-195089	—	The DNS traffic is incorrectly getting classified as **Thunder** and is getting blocked. This issue occurs when the DNS traffic is blocked and peer-peer ACL is denied for users. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-195100 AOS-198302 AOS-204455 AOS-206735	—	The health status of a managed device is incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master's WebUI. This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-195177	—	Some managed devices frequently generate internal system error logs. This issue occurs when the **sapd** process reads a non-existent interface. This issue is observed in 7220 controllers running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-195434	—	An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is observed in APs running ArubaOS 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.5.0.2
AOS-196457	—	High radio noise floor is observed on APs. This issue is observed in AP-515 access points running ArubaOS 8.5.0.2 or later versions.	ArubaOS 8.5.0.2
AOS-196864	—	Although a new VLAN ID is successfully connected, the managed device displays that the VLAN ID fails with a different ID. This issue is observed when new VLANs are added and the total number of VLANs are 100/101, 200/201, 300/301 and so on. This issue is observed in managed devices running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-196878 AOS-197216	—	The **Datapath** process crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.** This issue is observed in managed devices running ArubaOS 8.5.0.2 or later versions.	ArubaOS 8.5.0.2
AOS-197023	—	Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions. **Workaround:** The following are recommended: ■ In the CLI, execute the **ap regulatory-domain-profile** command to create an AP regulatory-domain- profile without any channel configuration, save the changes, and later add or delete channels	ArubaOS 8.5.0.4

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
		as desired. ■ In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes, and later add or delete channels as desired in the **Configuration > AP Groups** page.	
AOS-197497	—	AirMatch selects the same channel for two neighboring APs even after radar detection. This issue is observed in managed devices running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-197812	—	A mismatch of user roles is observed in the WebUI and CLI of the Mobility Master and managed device. This issue occurs when UDR is configured to assign user roles to clients. This issue is observed in Mobility Masters and managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-198024	—	Users are unable to access any page after the fifth page using the **Maintenance > Access Point** page in the WebUI. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-198281	—	The details of the **Up** time in **Managed network > Dashboard > Access Points > Access Points** table does not get updated correctly. This issue is observed in Mobility Masters running ArubaOS 8.2.2.6 or later versions.	ArubaOS 8.2.2.6
AOS-198483	—	WebUI does not have an option to map the **rf dot11-60GHz-radio-profile** to an AP group. This issue is observed in Mobility Masters running ArubaOS 8.5.0.4 or later versions.	ArubaOS 8.5.0.4
AOS-198849 AOS-198850	—	Users are unable to configure 2.4 GHz radio profile in the **Configuration > System > Profiles > 2.4 GHz radio profile** page and the WebUI displays an error message, **Feature is not enabled in the license.** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-198991	—	Users are unable to add a VLAN to an existing trunk port using the **Configuration > Interfaces > VLANs** page of the WebUI. This issue is observed in Mobility Masters running ArubaOS 8.6.0.1 or later versions.	ArubaOS 8.6.0.2
AOS-199492	—	Some APs do not get displayed in the **show airgroup aps** command output and the auto-associate policy stops working as expected. This issue occurs when the AirGroup domain is in distributed mode and is not validated in a cluster deployment. This issue is observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200733	—	Some APs running ArubaOS 8.5.0.3 or later versions crash and reboot unexpectedly. The log file list the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8.**	ArubaOS 8.5.0.3
AOS-200765	—	Some managed devices running ArubaOS 8.3.0.7 or later versions in a cluster setup log the error message, **<199804> <4844> |authmgr| |cluster| gsm_auth.c, auth_gsm_publish_ip_user_local_section:1011: auth_gsm_publish_ip_user_local_section: ip_user_local_flags.**	ArubaOS 8.3.0.7
AOS-201042	—	A large number of packet drops are observed in a few APs running ArubaOS 8.3.0.6 or later versions. This issue occurs when the AP SAP MTU datapath tunnel is set to 1514.	ArubaOS 8.3.0.6
AOS-201376	—	The measured power, **Meas. Pow** column in the **show ap debug ble-table** command does not get updated when the TX power of an AP is changed. This issue is observed in APs running ArubaOS 8.5.0.6 or later versions.	ArubaOS 8.5.0.6
AOS-201439 AOS-201448	—	Some AP-303H access points running ArubaOS 8.5.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**.	ArubaOS 8.5.0.5
AOS-202129 AOS-204127	—	The **Configuration > AP groups** page does not have the **Split radio** toggle button to enable the tri-radio feature. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-202426 AOS-203652	—	Some 510 Series access points running ArubaOS 8.6.0.4 crash and reboot unexpectedly. The log files lists the reason for the event as **PC is at: wlc_phy_enable_hwaci_28nm+0x938 - undefined instruction: 0 [#1]**.	ArubaOS 8.6.0.4
AOS-202552 AOS-203990	—	The **Dashboard > Traffic Analysis > AppRF** page of the WebUI displays **Unknown** for WLANs, Roles, and Devices. This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-203201	—	A managed device is unable to download configurations from the Mobility Master using VPNC. This issue is observed in managed devices running ArubaOS 8.2.2.6 or later versions.	ArubaOS 8.2.2.6
AOS-203336	—	The **Dashboard > Infrastructure > Access Points** page of the WebUI and the **show log** command display different values for the last AP reboot time. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203438	—	The configuration for EIRP made using the WebUI is not visible in stand-alone controllers running ArubaOS 8.6.0.3 or later versions.	ArubaOS 8.6.0.3
AOS-203614 AOS-209261	—	The Mobility Master dashboard does not display the number of APs and clients present in the network. This issue is observed in Mobility Masters running ArubaOS 8.6.0.2 or later versions.	ArubaOS 8.6.0.2
AOS-203910 AOS-209692	—	The stand-alone controllers running ArubaOS 8.6.0.3 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**.	ArubaOS 8.6.0.3
AOS-204414	—	The VLAN range configured using the **ntp-standalone vlan-range** command is not correctly sent to the managed devices. This issue occurs when the user repeatedly modifies the VLAN range. This issue occurs in Mobility Masters running ArubaOS 8.0.1.0 or later versions. **Workaround:** Delete the VLAN range configured on the Mobility Master and re-configure the **ntp-standalone vlan-range.**	ArubaOS 8.3.0.8
AOS-205319 AOS-206993 AOS-216577 AOS-218524	—	Some APs running ArubaOS 8.6.0.5 or later versions crash and reboot unexpectedly. The log file listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**.	ArubaOS 8.6.0.5
AOS-206178	—	System logs do not display the reason why an AP has shut down. This issue is observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206541	—	The **Maintenance > Software Management** page does not display the list of all managed devices that are a part of a cluster. This issue is observed in Mobility Masters running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-206752	—	The console log of 7205 controllers running ArubaOS 8.5.0.9 or later versions displays the **ofald| |sdn| ERRS ofconn_rx:476 <10.50.1.26:6633> socket read failed, err:Resource temporarily unavailable(11)** message.	ArubaOS 8.5.0.9
AOS-206795	—	A user is unable to rename a node from the Mobility Master node hierarchy. This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions. **Workaround:** Restart **profmgr** process to rename the node.	ArubaOS 8.3.0.7

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206890	—	The **body** field in the **Configuration > Services > Guest Provisioning** page of the WebUI does not allow users to add multiple paragraphs for email messages. This issue is observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206902 AOS-208241	—	AirGroup users are unable to connect to Sonos speakers. This issue is observed in managed devices running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-207006 AOS-215138	—	APs go down and UDP 8209 traffic is sent without UDP 4500 traffic. This issue is observed in managed devices running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-207245	—	Some managed devices running ArubaOS 8.5.0.8 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 53:86:0:802c).**	ArubaOS 8.5.0.8
AOS-207366	—	The **show advanced options** menu is not available in the **Configuration > Access Points > Campus APs** page of the WebUI. This issue occurs when more than one AP is selected. This issue is observed in Mobility Masters running ArubaOS 8.3.0.13.	ArubaOS 8.3.0.13
AOS-207692	—	Some managed devices running ArubaOS 8.6.0.4 or later versions log multiple authentication error messages.	ArubaOS 8.6.0.4
AOS-209276	—	The **show datapath crypto counters** command displays the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. This issue is observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-209912	—	A few managed devices fail to filter and drop spoofed ARP responses from the clients. The user entry for the other IP address was present on the managed devices but not in the route cache table. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-209977	—	SNMP query with an incorrect string fails to record the offending IP address. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-210198	—	The **Dashboard > Security > Detected Radio** page of the WebUI display incorrect number of **Clients**. This issue is observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210482	—	Some managed devices running ArubaOS 8.3.0.6 or later versions display the error message, **Invalid set request** while configuring ESSID for a Beacon Report Request profile.	ArubaOS 8.3.0.6
AOS-210490	—	Some managed devices running ArubaOS 8.5.0.8 or later versions display the error message, **Error: Tunnel is part of a tunnel-group** while deleting a L2 GRE tunnel which is not a part of any tunnel group.	ArubaOS 8.5.0.8
AOS-210992	—	The Mobility Master displays an error message, **Flow Group delete: id not found** after an upgrade. This issue occurs when logging levels are not configured correctly. This issue is observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-211658	—	A few clients are unable to connect to AP-535 access points running ArubaOS 8.6.0.5 or later versions in a cluster setup. This issue occurs when WMM and HT configurations are enabled.	ArubaOS 8.6.0.5
AOS-211720	—	The **STM** process crashes on managed devices and hence, APs failover to another cluster. This issue is observed in managed devices running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5
AOS-211863	—	Some APs do not come up on managed devices. This issue occurs when ▪ the forwarding mode is changed to bridge mode. ▪ the name of the ACL is 64 bytes. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212038	—	The **show memory <process-name>** command does not display information related to the **dpagent** process. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212255	—	Some APs are stuck in **Not in Progress** state during cluster live upgrade. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-213507	—	Some managed devices running ArubaOS 8.5.0.10 or later versions crash unexpectedly. The log files list the reason for the event as, **Reboot Cause: Soft Watchdog reset**. Duplicates: AOS-210240, AOS-214964, AOS-215393, AOS-215421, AOS-215628, AOS-215765, AOS-215827, AOS-216087, AOS-216315, AOS-216420, AOS-216888, AOS-217041, AOS-218007, AOS-218021, AOS-218907, AOS-219588, AOS-219597, AOS-220471, AOS-220981, AOS-221390, AOS-221642, and AOS-222036	ArubaOS 8.5.0.10

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-215461 AOS-220709	—	Database synchronization fails between standby and stand-alone controllers running ArubaOS 8.6.0.9 or later versions. The log files list the reason for the event as **Standby switch did not acknowledge the WMS database restore request**.	ArubaOS 8.6.0.9
AOS-215852	—	Mobility Masters running ArubaOS 8.6.0.6 or later versions log the error message, **ofa: 07765|ofproto|INFO|Aruba-SDN: 1 flow_mods 28 s ago (1 modifications).** This issue occurs when openflow is enabled and when 35 seconds is configured as UCC session idle timeout.	ArubaOS 8.6.0.6
AOS-216874 AOS-219841	—	The virtual MAC address of VLAN gets deleted from the bridge table and results in a network outage. This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-217184 AOS-218026 AOS-220562 AOS-220985	—	Some 7240XM controllers running ArubaOS 8.7.1.1 or later versions crash and reboot unexpectedly. The log files list the reason for the events as, **Kernel Panic (Intent:cause:register 12:86:b0:4)**. This issue occurs due to socket buffer corruption.	ArubaOS 8.7.1.1
AOS-218328 AOS-220026	—	VRRP flapping is observed on managed devices running ArubaOS 8.6.0.4 or later versions and hence, clients face connectivity issues.	ArubaOS 8.6.0.4
AOS-218621	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **AP Reboot reason: BadAddr:6c0094119461 PC:wlc_ampdu_recv_ addba_resp+0x240/0x838 [wl_v6] Warm-reset**.	ArubaOS 8.7.1.1
AOS-218642	—	Some iPads and other clients are unable to access the internet. This issue occurs when client entries are not removed by the managed devices even when CoA disconnect is triggered for the clients. This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-219307	—	Some managed devices running ArubaOS 8.5.0.12 or later versions crash unexpectedly. The log files list the reason for the event as, **Reboot cause: Kernel Panic (Intent:cause:register 12:86:f0:2)**.	ArubaOS 8.5.0.12
AOS-219383	—	The **Configuration > License > License Usage** tab does not display the license details. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.12 or later versions.	ArubaOS 8.5.0.12
AOS-219385	—	Some APs take a long time to come up on the backup data center after primary data center failover. This issue is observed in APs running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10

Table 7: *Known Issues in ArubaOS 8.6.0.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220053	—	Some Remote APs went down on managed devices running ArubaOS 8.6.0.5 or later versions. This issue occurs after a failover.	ArubaOS 8.6.0.5
AOS-220108	—	The **OFA** process crashes on Mobility Master Virtual Appliances running ArubaOS 8.6.0.6 or later versions. This issue occurs when the **show openflow debug ports** command is executed.	ArubaOS 8.6.0.6
AOS-220251	—	Some users experience connectivity issue. This issue occurs when APs do not respond to the authentication frames in MultiZone networks that have non-cluster zones and dot11r enabled Virtual APs. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.4 or later versions.	ArubaOS 8.5.0.4
AOS-220515	—	Some managed devices running ArubaOS 8.0.0.0 or later versions display the error message, **|fpapps| filling up the default gateway configuration.**	ArubaOS 8.5.0.12
AOS-220552	—	The **Configuration > Services > Clusters** page of the WebUI does not display the status of live upgrade. This issue occurs when the cluster profile name has blank spaces. This issue is observed in Mobility Masters running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-220903	—	The **s** flag indicating LACP striping is not displayed in the output of the **show ap database long** command even if LLDP is enabled on two uplinks. This issue is observed in APs running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-221018 AOS-220919	—	Some users are unable to connect to SSIDs. This issue occurs in 802.11r and MultiZone enabled configurations. This issue is observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-221144	—	ARP packets are not forwarded to the uplink switch when bcmc-optimization is enabled on the controllers. This issue is observed in Mobility Masters and managed devices running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-221743 AOS-212229	—	Some APs running ArubaOS 8.5.0.10 or later versions reboot unexpectedly. The log files list the reason for the events as, **skb_release_data+0xa0/0xc8/neigh_flush_dev+0x60**.	ArubaOS 8.5.0.10
AOS-222540	—	Some APs drop EAPOL packets from the bridge mode wired port. This issue is observed in APs running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9

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 Master, managed device, master controller, or stand-alone controller.

Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of 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 Master Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Master, or two versions lower. For example multiversion is supported if a Mobility Master is running ArubaOS 8.5.0.0 and the managed devices are running ArubaOS 8.5.0.0, ArubaOS 8.4.0.0, or ArubaOS 8.3.0.0.

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 150 MB of 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 the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 36 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 36 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 36 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the flash memory to an external server or mass storage device. You should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Log files
- Flash backup

Backing up and Restoring Flash Memory

You can backup and restore the flash memory using the WebUI or CLI.

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 36.

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 Master or managed device will not load a corrupted ArubaOS image.

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

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

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

In the CLI

The following steps describe how to upgrade 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 Master.
3. Execute the **ping** command to verify the network connection between the Mobility Master and the SCP server, FTP server, or TFTP server.

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

or

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

or

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

4. Execute the **show image version** command to check if the 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 Master.

```
(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 Master 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 36 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the 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 36 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 36.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the partition that contains the pre-upgrade ArubaOS version.

   When you specify a boot partition or copy an image file to a system partition, Mobility Master 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 Master 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 Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.

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

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

c. Click **Copy**.

2. Determine the partition on which your pre-upgrade 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 Master or managed device reboots after the countdown period.

4. When the boot process is complete, verify that the Mobility Master or managed device is using the correct 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 Master or managed device:

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

or

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

2. Set the Mobility Master or managed device to boot with your pre-upgrade configuration file.

(host) # boot config-file `<backup configuration filename>`

3. Execute the **show image version** command to view the partition on which your pre-upgrade 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 Master or managed device.

```
(host) # reload
```

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