

ArubaOS 8.10.0.6 Release Notes



a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2023 Hewlett Packard Enterprise Development LP.

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	3
Revision History	4
Release Overview	5
Important	5
Related Documents	5
Supported Browsers	5
Terminology Change	6
Contacting Support	6
What's New in ArubaOS 8.10.0.6	8
CLI	8
Behavioral Changes	8
Supported Platforms in ArubaOS 8.10.0.6	9
Mobility Conductor Platforms	9
Mobility Controller Platforms	9
AP Platforms	9
End-of-Support	12
Regulatory Updates in ArubaOS 8.10.0.6	13
Resolved Issues in ArubaOS 8.10.0.6	14
Known Issues in ArubaOS 8.10.0.6	24
Limitations	24
Known Issues	25
Upgrade Procedure	30
Important Points to Remember	30
Memory Requirements	31
Low Free Flash Memory	31
Backing up Critical Data	34
Upgrading ArubaOS	35
Verifying the ArubaOS Upgrade	37
Downgrading ArubaOS	37
Before Calling Technical Support	39

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 02	Added limitation on Airtime Fairness Mode .
Revision 01	Initial release.

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.x requires Hash-to-Element (H2E) for 6 Ghz WPA3-
SAE connections. H2E is supported only on Windows 11, Linux wpa_supplicant version 2.10 and later
versions. Hence, users must upgrade their Windows and Linux software for successful 6 Ghz WPA3-
SAE connections.
- 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.

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 Conductor 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:

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	<ul style="list-style-type: none"> ▪ Windows 10 or later ▪ macOS
Firefox 107.0.1 or later	<ul style="list-style-type: none"> ▪ Windows 10 or later ▪ macOS
Apple Safari 15.4 (17613.17.1.13) or later	<ul style="list-style-type: none"> ▪ macOS
Google Chrome 108.0.5359.71 or later	<ul style="list-style-type: none"> ▪ 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	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

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

CLI

show stm perf-history commands

Starting from ArubaOS 8.10.0.6, the **show stm perf-history duration** and **show stm perf-history interval** commands can be used to view the output for the specified time interval.

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 8.10.0.6.

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 3: *Supported Mobility Conductor Platforms*

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

Mobility Controller Platforms

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

Table 4: *Supported Mobility Controller Platforms*

Mobility Controller Family	Mobility Controller Model
7000 Series Mobility Controllers	7005, 7008, 7010, 7024, 7030
7200 Series Mobility Controllers	7205, 7210, 7220, 7240, 7240XM, 7280
9000 Series Mobility Controllers	9004, 9012
9200 Series Mobility Controllers	9240
MC-VA-xxx Virtual Mobility Controllers	MC-VA-10, MC-VA-50, MC-VA-250, MC-VA-1K

AP Platforms

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

Table 5: *Supported AP Platforms*

AP Family	AP Model
200 Series	AP-204, AP-205
203H Series	AP-203H
203R Series	AP-203R, AP-203RP

Table 5: Supported AP Platforms

AP Family	AP Model
205H Series	AP-205H
207 Series	AP-207
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, AP-303HR
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
370EX Series	AP-375EX, AP-377EX, AP-375ATEX
AP-387	AP-387
500 Series	AP-504, AP-505
500H Series	AP-503H, AP-503HR, AP-505H, AP-505HR
510 Series	AP-514, AP-515, AP-518
518 Series	AP-518
530 Series	AP-534, AP-535
550 Series	AP-555
560 Series	AP-565, AP-567
570 Series	AP-574, AP-575, AP-577
580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX

Table 5: *Supported AP Platforms*

AP Family	AP Model
630 Series	AP-635
650 Series	AP-655

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

The following AP models will no longer be supported beginning with the next major release, ArubaOS 8.11.0.0 and higher:

- 200 Series
- 203H Series
- 203R Series
- 205H Series
- 207 Series
- 210 Series
- 220 Series
- 228 Series
- 270 Series
- 320 Series
- 330 Series
- 340 Series
- AP-387

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_86062

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in ArubaOS 8.10.0.6*

New Bug ID	Description	Reported Version
AOS-156661 AOS-224890	The authentication survivability feature did not work as expected when the uplink was down. The fix ensures that the feature works as expected. This issue was observed in managed devices running ArubaOS 8.2.2.2 or later versions.	ArubaOS 8.2.2.2
AOS-214944	The profmgr process crashed on Mobility Conductors running ArubaOS 8.6.0.7 or later versions. This issue occurred while deleting the roles configured for AirGroup. The fix ensures that the Mobility Conductors work as expected.	ArubaOS 8.6.0.7
AOS-221514	The status of the VRRP instance was changed to vrrp is not in INIT state . This issue occurred when a new VLAN was added to the port-channel interface. The fix ensures that the Mobility Conductor works as expected. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.5 or later versions.	ArubaOS 8.10.0.5
AOS-224618 AOS-224619 AOS-224620 AOS-227759	The datapath process crashed on 9004 controllers and the controllers rebooted unexpectedly. The log files listed the reason for the reboot as Reboot Cause: Kernel Panic (Intent:cause: 86:50) . The fix ensures that the controllers work as expected. This issue was observed in 9004 controllers running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-218844 AOS-227400 AOS-231009	Some APs failed to preload image during cluster live upgrade. The fix ensures that the APs preload image during an upgrade. This issue was observed in APs running ArubaOS 8.6.0.9 or later versions in a cluster setup.	ArubaOS 8.6.0.9
AOS-219315	Some 9004 controllers running ArubaOS 8.7.1.10 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as Reboot Cause: Kernel Panic (Intent:cause: 86:50) . The fix ensures that the controllers work as expected. Duplicates: AOS-223786, AOS-223787, AOS-240010, AOS-234981, and AOS-220422	ArubaOS 8.7.1.10
AOS-221011	High channel utilization was observed in AP-515 access points running ArubaOS 8.6.0.0 or later versions. Enhancements to the wireless driver resolved the issue.	ArubaOS 8.7.1.3
AOS-223221 AOS-237950	Some AP-514 and AP-515 access points running ArubaOS 8.6.0.0 or later versions generated the error logs, CPU: 1 PID: 1979 at ../../../../soft-ap/broadcom/esdk6/main/src/wl/../../src/wl/sys/wlc.c:22608 wlc_calc_frame_time+0x12c/0x410 [wl_v6]() . The fix ensures that the APs work as expected.	ArubaOS 8.7.1.4

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-226017	The airmatch_recv process crashed on Mobility Conductors running ArubaOS 8.6.0.9 or later versions. The log files listed the reason for the event as Exceeded max number of packet limit . The fix ensures that the Mobility Conductors work as expected. Duplicates: AOS-231886, AOS-235947, AOS-238770, AOS-239637	ArubaOS 8.6.0.9
AOS-238025	Some AP-615 access points running ArubaOS 8.11.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as AP Reboot reason: BadPtr: 00000004 PC: _kmalloc_track_caller+0x84/0x17c Warm-reset . The fix ensures that the APs work as expected.	ArubaOS8.11.0.0
AOS-228371	Users were unable to delete a RADIUS server even when the server was not in use and an error message, RADIUS Server In use was displayed. The fix ensures that users can delete a RADIUS server that is not in use. This issue was observed in Mobility Conductors running ArubaOS 8.7.1.5 or later versions.	ArubaOS 8.7.1.5
AOS-228581 AOS-228791	Some managed devices running ArubaOS 8.8.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as Reboot Cause: Datapath timeout (SOS Assert) (in ipsec_decrypt) . This issue occurred when the buffer memory was queued in the wrong processor. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.4
AOS-229207 AOS-229888	Users observed a discrepancy between the client count displayed in the WebUI of a Mobility Conductor and the CLI of a managed device. This issue occurred when the WebUI of the Mobility Conductor reported the client count, including the client entries that were retained to accommodate temporary client disconnections. The fix ensures that the WebUI and CLI display the correct number of clients. This issue was observed in Mobility Conductors running ArubaOS 8.5.0.13 or later versions.	ArubaOS 8.5.0.13
AOS-231856	A few APs running ArubaOS 8.6.0.0 or later versions crashed unexpectedly. The log files listed the reason for the event as An internal system error has occurred at file sapd_sysctl.c function sapd_sysctl_write_param line 184 error Error writing /proc/net/wifi0/max_eirp_per_chan : Invalid argument . This issue occurred due to a change of channel on one or both the radios when EIRP check was done for a new channel. The fix ensures that the EIRP request is processed, and no error logs are generated.	ArubaOS 8.7.1.8
AOS-231990	The Dashboard > Infrastructure page of the WebUI displayed incorrect Last Reboot time. The fix ensures that the WebUI displays the correct Last Reboot time. This issue was observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.1.8
AOS-232378	The pim process crashed on managed devices running ArubaOS 8.7.1.8 or later versions. This issue occurred due to invalid memory access. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.8

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-232970	The AP MAC address was not present in the calling station ID of the RADIUS accounting packets and hence, the RADIUS accounting requests were discarded. The fix ensures that the MAC address is present in the calling station ID. This issue was observed in managed devices running ArubaOS 8.7.1.6 or later versions in a cluster setup.	ArubaOS 8.7.1.6
AOS-234103 AOS-240610	Some clients experienced downstream packet disruption. The fix ensures that the APs work as expected. This issue was observed in AP-205 access points running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.17
AOS-234480 AOS-238970	The apflash ap31x-ap32x backup partition command did not upgrade the backup partition of AP-315 access points running ArubaOS 8.7.1.9 or later versions in a cluster setup. The fix ensures that the command upgrades the backup partition of the APs.	ArubaOS 8.7.1.9
AOS-234747 AOS-235575	A high number of TX retransmissions was observed on a few APs. The fix ensures that the APs work as expected. This issue was observed in AP-535 and AP-565 access points running ArubaOS 8.6.0.17 or later versions.	ArubaOS 8.6.0.17
AOS-234782	A few AP-505H access points running ArubaOS 8.10.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as skb double free detected!" at ("file-name/line-number/function-name") net/core/skbuff.c:1849/consume_skb() . The fix ensures that the APs work as expected.	ArubaOS 8.10.0.0
AOS-234783	Some AP-505H access points running ArubaOS 8.10.0.0 or later versions were flooded with wlc_offload PhyRxSts Circular Buffer Control logs and crashed unexpectedly. The log files listed the reason for the event as Kernel panic - not syncing: Ktrace core monitor: cpu0 hung for 45 seconds, hung cpu count: 1 . The fix ensures that the APs work as expected.	ArubaOS 8.10.0.0
AOS-235242 AOS-235777	The auth process crashed and an error message, auth module busy was displayed. This issue occurred when the show run command was issued. The fix ensures that the users are able to issue the show run command. This issue was observed in managed devices running ArubaOS 8.6.0.17 or later versions.	ArubaOS 8.6.0.17
AOS-235672	Some wired clients received IP addresses even before a successful 802.1X authentication. The fix ensures that the clients receive IP addresses only after a successful authentication. This issue was observed in APs running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-235744 AOS-235752	Some managed devices were unable to receive any configuration from the Mobility Conductor. This issue occurred when changes to a few group names were not synchronized on the standby Mobility Conductor before a reboot. The fix ensures that the managed devices receive configurations from the Mobility Conductor. This issue was observed in Mobility Conductors running ArubaOS 8.6.0.17 or later versions.	ArubaOS 8.6.0.17

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-235820 AOS-239962	The wms process crashed on Mobility Conductors running ArubaOS 8.10.0.2 or later versions. This issue occurred when the wms process exceeded the virtual memory limit of 2 GB. The fix ensures that the Mobility Conductors work as expected.	ArubaOS 8.10.0.2
AOS-235834 AOS-240216	Some AP-535 and AP-555 access points running ArubaOS 8.6.0.19 or later versions crashed and rebooted unexpectedly. The log file lists the reason for reboot as: Reboot caused by kernel panic: Fatal exception in interrupt . The fix ensures that the APs work as expected.	ArubaOS 8.6.0.19
AOS-236170 AOS-239298	The Dashboard > Overview > Wireless Clients page of the WebUI did not display any information for Retried Frames . The fix ensures that the WebUI displays the information about retried frames. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-236225 AOS-234379	Some 630 Series and 650 Series access points running ArubaOS 8.9.0.1 or later versions experienced issues with the Draeger medical devices. The fix ensures that the APs work as expected.	ArubaOS 8.9.0.1
AOS-236242	The apmove command did not work as expected when the APs were connected to backup LMS controllers. The fix ensures that the users can issue the apmove command. This issue was observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.1.9
AOS-236427	The license feature bits of a stand-alone controller were changed to enabled after restoring the flash backup. The fix ensures that the status of the license feature bits does not change after restoring the flash backup. This issue was observed in stand-alone controllers / 7010 controllers running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-236445 AOS-238079	Some users were unable to add or allocate licenses using the WebUI. The fix ensures that users are able to add or allocate licenses using the WebUI. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-236728	Some AP-535 access points running ArubaOS 8.9.0.3 crashed and rebooted unexpectedly. The log files listed the reason for the event as Reboot caused by kernel panic: softlockup: hung tasks . The fix ensures that the APs work as expected.	ArubaOS 8.9.0.3
AOS-236813	Mobility Conductors running ArubaOS 8.10.0.2 or later versions generated multiple log messages, switch_daemon.0x204c03b68f82[8050]: <310322> <8050> [switch.10.143.242.6:58000] ofc-switch-manager Unknown message type 12 . The fix ensures that the Mobility Conductors work as expected.	ArubaOS 8.10.0.2

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-236841 AOS-238400	The Configuration > Services > Clusters >Add Controller page of the WebUI did not display the list of VRRP VLANs . The fix ensures that the WebUI displays the list of VRRP VLANs. This issue was observed in managed devices running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-236881	After upgrading Mobility Conductors to ArubaOS 8.6.0.9 or later versions, the profile manager in the secondary Mobility Conductor stopped responding. This issue occurred when IPv6 mode was enabled in the secondary Mobility Conductor because of which it failed to download certificates from the primary Mobility Conductor. The fix ensures that the secondary Mobility Conductor works as expected when IPv6 mode is enabled.	ArubaOS 8.6.0.9
AOS-237113	High latency and jitter were observed on stand-alone controllers running ArubaOS 8.7.1.9 or later versions. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.7.1.9
AOS-237203	Some stand-alone controllers with IAP-VPN tunnels generated multiple error logs. The fix ensures that the controllers do not generate error logs. This issue was observed in stand-alone controllers running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-237386	The packetin_dispatcher process crashed unexpectedly on a Mobility Conductor running ArubaOS 8.10.0.2 or later versions. The fix ensures that the Mobility Conductors work as expected.	ArubaOS 8.10.0.2
AOS-237473 AOS-238104	The core files of the nanny process were not collected by the Mobility Conductor. The fix ensures that the Mobility Conductor collects the core files of the nanny process. This issue was observed in Mobility Conductor running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-237510	Some WPA3-SAE opmode clients were unable to download user roles from ClearPass Policy Manager after a successful MAC authentication. The log file listed the reason for the event as Cannot be assigned downloadable role, role is in error state . The fix ensures that the clients are able to download user roles from ClearPass Policy Manager. This issue was observed in managed devices running ArubaOS 8.6.0.18 or later versions.	ArubaOS 8.6.0.18
AOS-237815	Mobility Conductors running ArubaOS 8.6.0.19 did not have sufficient free flash space. This issue occurred when the AP image files took excessive flash space. The fix ensures that the Mobility Conductors work as expected.	ArubaOS 8.6.0.19
AOS-237851	Some AP-535 access points running ArubaOS 8.10.0.2 or later versions 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 (phyrf_ani.c:718) . The fix ensures that the APs work as expected.	ArubaOS 8.10.0.2

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-237897	The WebCC logs were stored in an invalid message format and as a result, the syslog server reported incorrect data. The fix ensures that the WebCC logs are logged in a valid message format. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.7.1.9
AOS-238080	Some AP-635 access points running ArubaOS 8.10.0.2 or later versions rebooted unexpectedly. The log files listed the reason for the event as reboot caused by kernel panic: Take care of the TARGET ASSERT first "ar_wal_tx_send.c:9117 Assertion p pdu_opts->rc_subfrms_max failed" . The fix ensures that the APs do not reboot unexpectedly.	ArubaOS 8.10.0.2
AOS-238205	Some 9240 controllers running ArubaOS 8.10.0.3 or later versions did not respond to the SNMP GET request to OID WLSXSYSTEMEXT MIB::sysExtFanStatus . The fix ensures that the controllers respond to the SNMP GET request.	ArubaOS 8.10.0.3
AOS-238218 AOS-239882 AOS-241230	The mongo database took up a lot of flash space. This issue was observed in Mobility Conductors running ArubaOS 8.9.0.3 or later versions. The fix ensures that the Mobility Conductors work as expected.	ArubaOS 8.9.0.3
AOS-238387	The authentication survivability feature did not work as expected and hence, clients were unable to connect to the network. This issue occurred when the RADIUS server returned a username that was different from the Certificate Common Name (CN). The fix ensures that the authentication survivability feature works as expected. This issue was observed in managed devices running ArubaOS 8.6.0.17 or later versions.	ArubaOS 8.6.0.17
AOS-238410 AOS-238939 AOS-238564 AOS-238487	The httpd process crashed on Mobility Conductors and managed devices running ArubaOS 8.6.0.0 or later versions. This issue occurred when a specific type of cURL request was sent to the controllers. The fix ensures that the managed devices and Mobility Conductors work as expected.	ArubaOS 8.10.0.3
AOS-238500	Some clients were unable to connect to a few APs. This issue occurred when the tunnel between the AP and the managed device in a cluster was down. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-238519 AOS-240280	The BSS table of the Remote AP was reset unexpectedly. This issue occurred after a reboot of the Mobility Conductor. The fix ensures that the AP BSS table does not reset after a reboot of the Mobility Conductor. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-238578 AOS-238575 AOS-238576	The halt command did not save the audit-trail logs of the stand-alone controllers. As a result, the show audit-trail history command did not display the configuration changes done before a reboot. The fix ensures that the halt command saves the audit-trail logs of the controllers. This issue was observed in stand-alone controllers running ArubaOS 8.10.0.3 or later versions.	ArubaOS 8.10.0.3

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-238589 AOS-239319	The impystart process crashed on Mobility Conductor Virtual Appliances running ArubaOS 8.10.0.2 or later versions. The fix ensures that the Mobility Conductor Virtual Appliances work as expected.	ArubaOS 8.10.0.2
AOS-238681	The RADIUS request access packets contained the IP address of the Mobility Conductor as the NAS IP address instead of the CoA VRRP IP address of the managed device. Hence, clients experienced connectivity issues. The fix ensures that the RADIUS request access packets contain the correct NAS IP address. This issue was observed in managed devices running ArubaOS 8.9.0.1 or later versions in a cluster setup.	ArubaOS 8.9.0.1
AOS-238701 AOS-238934 AOS-239570	The authmgr , httpd , fwvisibility , ctamon , and ucm processes were stuck in NOT_RESPONDING or INITIALIZING state. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.6.0.19 or later versions in a cluster setup.	ArubaOS 8.6.0.19
AOS-238768	WebUI took a long time to display the AP and client information. The fix ensures that the WebUI displays the AP and client information without any delay. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-238836	Clients that used machine and user authentication were unable to connect to SSIDs. This issue was observed when WPA2 encryption was used. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.6.0.18 or later versions.	ArubaOS 8.6.0.18
AOS-238848	Some managed devices running ArubaOS 8.10.0.2 or later versions displayed an error message, Different SNMP hosts should not have same engine-id value , while configuring the SNMPv3 trap host. This issue occurred when the same SNMP engine-id was configured for multiple SNMPv3 trap hosts. The fix ensures that the managed devices work as expected.	ArubaOS 8.10.0.2
AOS-238853	The health report sent to the Azure IoT Hub did not contain all the required information about the AP. The fix ensures that the health report contains the necessary information. This issue was observed in APs running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.2
AOS-238918	The Configuration > IoT > Zigbee Services page of the WebUI did not allow users to delete the Zigbee service profile. The fix ensures that users can delete the Zigbee service profile using the WebUI. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.2 or later versions.	
AOS-238921 AOS-241183	Some 7240XM controllers running ArubaOS 8.10.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2) . This issue occurred when IPv6 DNS response was received. The fix ensures that the controllers work as expected.	ArubaOS 8.10.0.2

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-238954	Clients that used machine and user authentication were unable to connect to SSIDs. This issue was observed when WPA3 encryption was used. The fix ensures seamless connectivity. This issue was observed in AP-515 access points running ArubaOS 8.6.0.18 or later versions.	ArubaOS 8.6.0.18
AOS-238960	Some stand-alone controllers running ArubaOS 8.7.1.8 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2) . The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.7.1.8
AOS-238968	Some APs failed to send the IDS deauthentication frames even when the protect valid station parameter was enabled. This issue occurred when APs were connected in AM mode on 5 GHz channel. The fix ensures that the APs send the deauthentication frames when the valid station parameter is enabled. This issue was observed in AP-515 and AP-505 access points running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-239067	Some AP-535 access points running ArubaOS 8.10.0.0 or later versions 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 . The fix ensures that APs work as expected.	ArubaOS 8.11.0.0
AOS-239165	Some AP-635 access points running ArubaOS 8.10.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as Reboot caused by kernel panic with "sched_algo_qos.c:3794 Assertion (rtxop > 0) failed" . The fix ensures that the APs work as expected.	ArubaOS 8.10.0.2
AOS-239202 AOS-240267	The ble_daemon process consumed high memory and data packets were also dropped. This issue occurred when the BLE operation mode was enabled on the APs. The fix ensures that the APs work as expected. This issue was observed in APs running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-239260	Some AP-505 access points running ArubaOS 8.6.0.18 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as BadPtr:00000294 PC:tun_rcv_esp2_prep+0x10c/0x15c Warm-reset . The fix ensures that the APs work as expected.	ArubaOS 8.6.0.18
AOS-239289	The output of the show datapath cluster details command displayed an incorrect time stamp. This issue occurred when the managed devices were up for more than 49 days. The fix ensures that the command displays the correct timestamp. This issue was observed in managed devices running ArubaOS 8.10.0.2 or later versions in a cluster setup.	ArubaOS 8.10.0.2
AOS-239327	The OSPF process crashed on managed devices running ArubaOS 8.10.0.2 or later versions in a VPNC topology. The fix ensures that the managed devices work as expected.	

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-239329 AOS-240018 AOS-241151	Some APs displayed an error message, sapd_sysctl_An internal system error has occurred at file sapd_sysctl.c function sapd_sysctl_write_param line 180 error Error opening /proc/sys/dev/wifi0/rts_mode : No such file or directory. 0 . The fix ensures that the APs do not display the error message. This issue was observed in 200 Series, 203H Series, 203R Series, 205H Series, 210 Series, 220 Series, 228 Series, 270 Series, and AP-345 access points running ArubaOS 8.10.0.5.	ArubaOS 8.10.0.5
AOS-239341	Some clients were unable to connect to AP-345 access points running ArubaOS 8.6.0.10 or later versions. The fix ensures seamless connectivity.	ArubaOS 8.6.0.10
AOS-239487	The PCAP files of some APs were incorrectly sent to the default folder of the dump server and not to the user-defined folder. This issue was caused due to the defined dump-server settings not being honoured. The fix ensures that the PCAP files are sent following all the user-defined dump-server settings and will use SCP if that is what has been configured. This issue was observed in APs running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-239165	Some AP-635 access points running ArubaOS 8.10.0.2 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as Reboot caused by kernel panic with "sched_algo_qos.c:3794 Assertion (rtxop > 0) failed" . The fix ensures that the APs work as expected.	ArubaOS 8.10.0.2
AOS-239623	The output of the show ap ble-ibeacon-info command displayed an incorrect APB Radio BLE Operational TxPower . The fix ensures that the command displays the correct operational Tx power. This issue was observed in APs running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.4
AOS-239662	Some clients experienced issues with audio transmission during Skype and Microsoft Teams calls. The fix ensures that the clients do not experience issues with audio transmission. This issue was observed in APs running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-240057	The uplink VLAN did not work as expected. This issue occurred when an Instant Access Point was converted to a Remote AP. The fix ensures that the uplink VLAN works as expected. This issue was observed in AP-635 access points running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-240199	Users were unable to establish connection with a managed device using the mdconnect and logon commands. The fix ensures that the commands work as expected. This issue was observed in managed devices running ArubaOS 8.7.1.11 or later versions.	
AOS-240300	AirMatch assigned incorrect power levels to AP-277 access points running ArubaOS 8.10.0.4 or later versions. The fix ensures that AirMatch assigns correct power levels for APs.	ArubaOS 8.10.0.4

Table 6: Resolved Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-240347	Users were unable to collect the tech support logs of the Mobility Conductor. The fix ensures that the tech support logs of the Mobility Conductor are available for the users. This issue was observed in Mobility Conductors running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-240371	The 802.1X authentication failed for a few clients. This issue occurred when AP-635 access points were configured as Remote AP. The fix ensures successful authentication. This issue was observed in AP-635 access points running ArubaOS 8.10.0.4 or later versions.	ArubaOS 8.10.0.4
AOS-240772 AOS-240775	The STM process crashed on managed devices running ArubaOS 8.10.0.2 or later versions. This issue occurred due to memory leak. The fix ensures that the managed devices work as expected.	ArubaOS 8.10.0.2

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

Limitations

Following are the limitations observed in this release.

IP Default-Gateway Management Address

Aruba recommends to not configure the IP default-gateway management address for 7010, 7024, 7205, and 7280 controllers running ArubaOS 8.10.0.0.

650 Series and 630 Series Access Points

The 650 Series and 630 Series access points have the following limitations:

- No spectrum analysis on any radio
- No Zero-Wait DFS
- No Hotspot and Air Slice support on the 6 GHz radio
- No 802.11mc responder and initiator functionality on any radio
- Only 4 VAPs on the 6 GHz radio instead of 16
- Maximum of 512 associated clients on any radio, instead of 1024

6 GHz Channel Information in Regulatory Domain Profile

ArubaOS does not display the 6 GHz channel information in the existing regulatory domain profile of Wi-Fi 6E APs by default.

To include 6 GHz channel information, ensure that you change the country code to a different country code, apply the change, and then revert it to the original country code. Another option is to create a new regulatory domain profile that includes the 6 GHz channel information by default, or copy the existing regulatory domain profile into a new regulatory domain profile to save the configuration.

The following example configures a regulatory domain profile and specifies a valid 6 GHz band.

```
host) [mynode] (config) #ap regulatory-domain-profile reg-635
host) [mynode] (Regulatory Domain profile "reg-635") #country-code US
host) [mynode] (Regulatory Domain profile "reg-635") #valid-6ghz-channel 165
```


Air Slice

Air Slice is partially enabled on 500 Series access points and 510 Series access points. However, WMM boost will be functional even if Air Slice high-priority queuing is disabled.

Airtime Fairness Mode

Airtime Fairness Mode is not supported in 802.11ax access points.

7000 Series and 7200 Series Controllers

The **cpboot** command does not upgrade the ArubaOS software version of 7000 Series and 7200 Series controllers.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in ArubaOS 8.10.0.6*

New Bug ID	Description	Reported Version
AOS-151022 AOS-188417	The output of the show datapath uplink command displays an incorrect session count. This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. Old Bug ID: 185176	ArubaOS 8.1.0.0
AOS-156537	Multicast streaming fails when broadcast and multicast optimization is enabled on the user VLAN. This issue is observed in managed devices running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
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 the 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. 3. Change the VLAN of user role from trunk mode to access mode.	ArubaOS 8.4.0.0
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

Table 7: Known Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-216536 AOS-220630	Some managed devices running ArubaOS 8.5.0.11 or later versions are unable to come up on the Mobility Conductor. This issue occurs when the managed devices receive the branch IP address as the controller IP address in a VPNC deployment.	ArubaOS 8.5.0.11
AOS-219150	Mobility Conductor fails to push the SRC NAT pool configuration to the 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-219423	Honeywell Handheld 60SL0 devices are unable to connect to 802.1X SSIDs. This issue is observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-219791	The aggressive scanning mode under ARM profile settings is enabled by default. This issue is observed in APs running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-221308	The execute-cli command does not work as expected for a few show commands. This issue is observed in Mobility Conductors running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-225263 AOS-232589	L2 database synchronization fails on standby controllers. This issue is observed in stand-alone controllers running ArubaOS 8.8.0.1 or later versions.	ArubaOS 8.8.0.1
AOS-227981 AOS-233098	A few 7010, 7024, 7205, and 7280 controllers running ArubaOS 8.0.0.0 or later versions incorrectly route the incoming external subnet traffic on management port to data ports.	ArubaOS 8.7.1.6
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-229190 AOS-229798 AOS-230295	The Dashboard > Overview > Clients page of the WebUI does not display active and standby controller information. This issue is observed in Mobility Conductors running ArubaOS 8.10.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-229828	Some managed devices face issues while supporting weak ciphers during SSL/TLS negotiations. This issue is observed in managed devices running ArubaOS 8.7.1.6 or later versions.	ArubaOS 8.7.1.6
AOS-230900 AOS-231081 AOS-234940	Some 530 Series and 550 Series access points running ArubaOS 8.6.0.0 or later versions crash and reboot unexpectedly. The log files list the reason for reboot as Reboot caused by kernel panic: Take care of the TARGET ASSERT first.	ArubaOS 8.7.1.7
AOS-231206 AOS-239396 AOS-240563	The wpa3_sae process crashes or is stuck in the PROCESS_NOT_RESPONDING_CRITICAL state. This issue occurs due to timer corruption. This issue was observed in managed devices running ArubaOS 8.6.0.17 or later versions.	ArubaOS 8.6.0.17

Table 7: Known Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-231283	The log files of a 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
AOS-231473	The Dashboard > Overview > Wired Clients page of the WebUI does not display the details of the APs to which clients are connected. This issue occurs in a IPv6 deployment. This issue is observed in Mobility Conductors running ArubaOS 8.8.0.2 or later versions.	ArubaOS 8.8.0.2
AOS-232443	Server derivation rules are not assigned correctly and an error message, Missing server in attribute list is displayed. This issue occurs when there is a delay in response from the RADIUS server. This issue is observed in stand-alone controllers running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-232493	The entries of denylisted clients are not synchronized between the managed devices. This issue is observed in managed devices running ArubaOS 8.6.0.15 or later versions in a cluster setup.	ArubaOS 8.6.0.15
AOS-232620	A discrepancy is observed between the total number of APs and the total number of AP BLE devices reported. This issue is observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.8.0.2
AOS-232897	The wlan ht-ssid-profile command overrides the radio frequencies from 80 MHz to 40 MHz, although the show ap bss-table command displays the radio frequencies as 80 MHz. This issue is observed in AP-515 and AP-535 access points running ArubaOS 8.7.1.9 and ArubaOS 8.10.0.0 versions.	ArubaOS 8.7.1.9
AOS-232997	Some managed devices running ArubaOS 8.7.1.9 or later versions are stuck after an upgrade and the aaa process crashes.	ArubaOS 8.7.1.9
AOS-233582	The licensing server fails to update the IP address of the secondary Mobility Conductor. This issue occurs when the secondary Mobility Conductor becomes the primary Mobility Conductor. This issue is observed in managed devices running ArubaOS 8.6.0.11 or later versions.	ArubaOS 8.6.0.11
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-234103	Some clients experience downstream packet disruption. This issue is observed in APs running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.17
AOS-234315	A few APs sent PAPI messages to external IP addresses, and the logs displayed a random IP address for the PAPI_Send failed error message. This issue is observed in APs running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15

Table 7: Known Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
AOS-234761 AOS-240612 AOS-240809	The Dashboard > Overview > Wireless Clients page of the WebUI does not display the IP address of the Active Controller and Standby Controller . However, the CLI displays the IP address of the active and standby controllers. This issue is observed in Mobility Conductors running ArubaOS 8.7.1.10 or later versions.	ArubaOS 8.7.1.10
AOS-235479	The commands, copy ftp and copy tftp do not work as expected for the management interface. This issue is observed in managed devices running ArubaOS 8.6.0.17 or later versions. Workaround: Ensure that the file server is reachable via OOB if OOB is configured for platforms that support the OOB Management port.	ArubaOS 8.6.0.17
AOS-236200	Some AP-374 access points configured as mesh APs crash unexpectedly. The log files list the reason for the crash as kernel panic: Fatal exception . This issue is observed in AP-374 access points running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-236721	The Configuration > Roles & Policies > Roles page of the WebUI does not display ACLs configured for the role. However, the CLI displays the list of ACLs. This issue is observed in Mobility Conductors running ArubaOS 8.6.0.16 or later versions.	ArubaOS 8.6.0.16
AOS-236852	The error log, ofa: <310202> <6481> <ERRS> 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 9240 controllers running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-237348	Some AP-535 access points running ArubaOS 8.9.0.3 or later versions crash and reboot unexpectedly. The log files list the reason for the reboot as Reboot caused by kernel panic: Take care of the TARGET ASSERT at whal_rcvc.c:1656 Assertion .	ArubaOS 8.9.0.3
AOS-237479	Some APs running ArubaOS 8.7.1.7 or later versions are unable to form standby tunnels with the cluster nodes. This issue occurs due to a race condition.	ArubaOS 8.7.1.7
AOS-238727	Users are unable to reset the IPsec MTU value using the no crypto ipsec mtu command. This issue is observed in Mobility Conductors running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-239498	Some AP-515 access points running ArubaOS 8.6.0.19 or later versions crash and reboot unexpectedly. The log files list the reason for the event as AP Reboot reason: BadPtr:0000000f PC:wlc_get_txh_info+0x118/0x210 [wl_v6] Warm-reset .	ArubaOS 8.6.0.19

Table 7: Known Issues in ArubaOS 8.10.0.6

New Bug ID	Description	Reported Version
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 was 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-239872	WebUI does not allow users to live upgrade a cluster. However, the CLI allows users to upgrade a cluster. This issue occurs when the name of the cluster contain spaces. This issue is observed in managed devices running ArubaOS 8.5.0.0 or later versions.	ArubaOS 8.10.0.4
AOS-240185	Clients are unable to obtain user roles from ClearPass Policy Manager and fall into the initial role. This issue occurs due to radius accounting. This issue is observed in managed devices running ArubaOS 8.7.1.10 or later versions.	ArubaOS 8.7.1.10
AOS-240211	Some AP-535 access points running ArubaOS 8.6.0.18 or later versions do not transmit beacons on 5 GHz channels even after radar detection when static channel is set.	ArubaOS 8.6.0.18
AOS-240279	Mobility Conductors running ArubaOS 8.10.0.4 or later versions push additional IGMP and OSPF configurations to the managed devices. This issue occurs when a VLAN configuration is edited.	ArubaOS 8.10.0.4
AOS-240312	The arci-cli-helper process crashes on 7240XM controllers running ArubaOS 8.7.1.10 or later versions.	ArubaOS 8.7.1.10
AOS-240425	The HTTPS connection is interrupted and the ICMP communication is blocked for some VIA clients. This issue occurs when, <ul style="list-style-type: none"> ■the default size of 1452 bytes is used for MTU ■the DF bit is set for IP packets This issue is observed in controllers running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-240646	The output of the show ap ble_ibeacon_info command does not display the name of the AP. This issue is observed in Mobility Conductors running ArubaOS 8.10.0.2 or later versions.	ArubaOS 8.10.0.2
AOS-240920	The fpapps process crashes on Mobility Conductors running ArubaOS 8.9.0.3 or later versions.	ArubaOS 8.9.0.3

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 34](#) to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
 - **Flash backups:** Use the procedures described in [Backing up Critical Data on page 34](#) to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
 - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 34](#) to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.



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 8](#) for all supported controller models:

Table 8: 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 8](#), 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 8](#)
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: [upgradelImageNew.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 8](#).
- 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.



CAUTION

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see [Memory Requirements on page 31](#).



NOTE

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message is displayed ccurrs 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 34](#) for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the 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 34](#) 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 34](#).
2. Verify that the control plane security is disabled.

3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade 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.