ArubaOS 8.7.1.10 Release Notes

a Hewlett Packard
Enterprise company

Copyright Information

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

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

Contents

Chapter 1
Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release:

Table 1: *Revision History*

Revision	Change Description
Revision 03	Added limitation on **Airtime Fairness Mode**.
Revision 02	**AOS-228104** was added as a resolved issue.
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:

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	▪ Windows 10 or later ▪ macOS
Firefox 107.0.1 or later	▪ Windows 10 or later ▪ macOS
Apple Safari 15.4 (17613.17.1.13) or later	▪ macOS
Google Chrome 108.0.5359.71 or later	▪ Windows 10 or later ▪ macOS

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

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

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	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.

New Features and Enhancements in ArubaOS 8.7.1.10

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

CLI

show ap debug ble-table

The **ibeacon** parameter has been added to the **show ap debug ble-table ap-name <name>** command to view the ibeacon statistics of an AP.

```
(host) [mynode] #show ap debug  ble-table ap-name AP505h_solum ibeacon
BLE Device Table [iBeacon]
--------------------------
MAC                Major  Minor  UUID  Meas. Pow.  RSSI  Last Update
---                -----  -----  ----  ----------  ----  -----------
28:de:65:44:8a:68  --     --     --                                  --
-79   I:122s
ac:23:3f:a9:d0:7f  0      0      E2C56DB5-DFFB-48D2-B060-D0F5A71096E0  -59
-24   I:0s
3c:a3:08:93:53:04  0      0      4152554E-F99B-4A3B-86D0-947070693A78  --
-82   I:269s
20:4c:03:b2:79:1c  0      0      4152554E-F99B-4A3B-86D0-947070693A78  -56
-91   I:2s
20:4c:03:44:23:58  --     --     --                                  --
-90   I:29s
5c:f8:21:e6:d5:58  0      0      4152554E-F99B-4A3B-86D0-947070693A78  -56
-39   I:0s
54:6c:0e:15:7b:5f  0      0      4152554E-F99B-4A3B-86D0-947070693A78  -60
-37   I:0s
54:6c:0e:15:6b:c6  0      0      4152554E-F99B-4A3B-86D0-947070693A78  -60
-36   I:0s
Note: Battery level for LS-BT1USB devices is indicated as USB.
Note: Uptime is shown as Days hour:minute:second.
Note: Last Update is time in seconds since last heard update.
Note: Meas. Pow. is the averaged RSSI (in dBm) when the iBeacon is calibrated.
Note: Tx_Power is shown in dBm in the APBs section for radios that support radio
profile type 1. For all other APB radios, Tx_Power is a discrete level from 0-15.
Status Flags:L:AP's local beacon; I:iBeacon; A:Beacon management capable
:H:High power beacon; T:Asset Tag Beacon; U:Upgrade of firmware pending
:u:Beacon management update received
Last Update Flags:I: Device observed by internal radio
:E: Device observed by external radio
Generic Filter:S:serviceUUIDFilter; C:companyIdentifierFilter
:M:macOuiFilter; L:localNameFilter
```

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 8.7.1.10.

Chapter 4
Supported Platforms in ArubaOS 8.7.1.10

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 8.7.1.10*

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 8.7.1.10*

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, 9012
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 in ArubaOS 8.7.1.10*

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

Table 5: *Supported AP Platforms in ArubaOS 8.7.1.10*

AP Family	AP Model
203R Series	AP-203R, AP-203RP
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-387	AP-387
500 Series	AP-504, AP-505
500H Series	AP-503H, AP-505H
510 Series	AP-514, AP-515, 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

Chapter 5
Regulatory Updates in ArubaOS 8.7.1.10

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_84631

Chapter 6
Resolved Issues in ArubaOS 8.7.1.10

The following issues are resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-144672 AOS-233036	A few managed devices were stuck, clients were unable to pass traffic, and new clients were unable to connect to the managed devices. This issue occurred when more than 255 users were connected to the Remote AP in bridge mode when RADIUS accounting was enabled. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.6.0.11
AOS-190621 AOS-198482	The WebUI did not filter the names of the APs that had the special characters, + and %. The fix ensures that the WebUI filters the names of the APs that have the special characters, + and %. This issue was observed in managed devices and Mobility Masters running ArubaOS 8.2.0.0 or later versions.	ArubaOS 8.4.0.2
AOS-196042	The output of the **show ucc dns-ip-learning** command displayed **Unknown** for **Service Provider**. The fix ensures that the command displays the correct **Service Provider**. This issue is observed in managed devices running ArubaOS 8.6.0.9 or later versions. Duplicates: AOS-217995, AOS-221263, AOS-233788	ArubaOS 8.6.0.9
AOS-201428	The **show log all** command did not display the output in a chronological order. The fix ensures that the command displays the output in a chronological order. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. Duplicates: AOS-232254, AOS-204928, AOS-216968, AOS-217626	ArubaOS 8.3.0.0
AOS-204785	Some Remote APs took a long time to come up after an upgrade. The fix ensures that the Remote APs connect and come up seamlessly. This issue was observed in Remote APs running ArubaOS 8.5.0.6 or later versions in a cluster setup.	ArubaOS 8.5.0.6
AOS-205192	The channels configured using in the **Configuration > System > Profiles > All Profiles > AP > Regulatory Domain** profile page of the WebUI did not take effect. The fix ensures that the channel configured using WebUI takes effect and works as expected. This issue was observed in Mobility Masters running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-205650 AOS-231536	DHCP traffic from relay agent was not forwarded through the next-hop list configured in Layer 3 GRE tunnel. The fix ensures that the DHCP traffic is forwarded correctly. This issue was observed in managed devices running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-206577 AOS-232877	The **no MTU** command returned a validation error. This was is observed when a Layer-2 IPv6 GRE tunnel was formed between the managed devices. The fix ensures that the command does not return a validation error. This issue was observed in managed devices running ArubaOS 8.7.0.0 or later versions.	ArubaOS8.7.0.0
AOS-207356 AOS-221325	Wired clients connected to AP-505 access points in split-tunnel mode experienced poor connection speed. Enhancements to the wireless driver resolved the issue. This issue was observed in AP-505 remote mode access points running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-207692	Some managed devices running ArubaOS 8.6.0.4 or later versions logged multiple authentication error messages. The fix ensures that the managed devices do not log multiple authentication error messages.	ArubaOS 8.6.0.4
AOS-208853	Some AP-555 access points in bridge mode did not transmit multicast traffic at the configured multicast rate and continued to transmit multicast traffic at the lowest default tx-rate. The fix ensures that the APs transmit multicast traffic at the configured multicast rate. This issue was observed in AP-555 access points running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-208957 AOS-229568 AOS-232888	Some APs were stuck in ID flag. The fix ensures that the APs are not stuck in ID flag. This issue was observed in APs running ArubaOS 8.6.0.10 or later versions.	ArubaOS 8.6.0.10
AOS-209972 AOS-232532	An error message, **Trap Name is incorrect. Use the command show snmp trap-list to get the valid trap names** was displayed when an incorrect or unsupported trap command was executed. The fix ensures that appropriate error messages are displayed. This issue was observed in Mobility Masters running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-210490 AOS-231222	Some managed devices running ArubaOS 8.5.0.8 or later versions displayed the error message, **Error: Tunnel is part of a tunnel-group**. This issue occurred while deleting an L2 GRE tunnel which was not a part of any tunnel group. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.8
AOS-212029 AOS-218163	Certain data from websites were not being downloaded on a few APs. This issue occurred when the MTU length was more than 314 bytes. The fix ensures that users able to download data from websites. This issue was observed in APs running ArubaOS 8.6.0.2 or later versions.	ArubaOS 8.6.0.2
AOS-212255	Some APs were stuck in **Reboot in progress** state during cluster live upgrade. Hence, the live upgrade process was interrupted and the remaining APs were also stuck in **Not In Progress** state. This issue occurred when an AP, after a reboot, came up on a different managed device which was not part of the cluster that was being upgraded. The fix ensures that the cluster upgrade is not stuck and APs upgrade as expected.	ArubaOS 8.5.0.10

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-212523 AOS-232369	The **pcapdumpd** process consumed high CPU memory and hence, users were unable to issue the **show ap monitor ap-list** command, The fix ensures that the APs work as expected. This issue was observed in APs running ArubaOS 8.7.1.5 or later versions.	ArubaOS 8.7.1.5
AOS-214575 AOS-228506	A few APs running ArubaOS 8.3.0.13 or later versions took a long time to come up on the Mobility Controller Virtual Appliance. This issue occurred when, ▪ factory reset APs were re-provisioned from Mobility Master Hardware Appliances. ▪ the IP address of the Mobility Controller Virtual Appliance was configured as the LMS IP address in the AP system profile. The fix ensures that the APs do not take a long time to come up on the Mobility Controller Virtual Appliance.	ArubaOS 8.3.0.13
AOS-215727	Stale AP entries that were cleared using the **clear gap-db** command prior to the upgrade reappeared on the Mobility Master after an upgrade. The fix ensures that the stale AP entries are cleared when the **clear gap-db** command is executed. This issue was observed in Mobility Masters running ArubaOS 8.5.0.11 or later versions. Duplicates: AOS-216896, AOS-217593, AOS-234459	ArubaOS 8.5.0.11
AOS-219769	The RAP GRE MTU value was not updated consistently in a cluster. The fix ensures that the RAP GRE MTU value is updated correctly. This issue was observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.8.0.0
AOS-219803	The XML query done on a non-existing user, resulted in an invalid response. The fix ensures that the XML query returns a valid response. This issue was observed in managed devices running ArubaOS 8.7.1.2 or later versions.	ArubaOS 8.7.1.2
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-221643	Stand-alone controllers running ArubaOS 8.4.0.0 or later versions failed to send the client login and logout details of captive portal authentication to the Palo Alto Firewall. The fix ensures that the controllers send the client details to the Palo Alto Firewall.	ArubaOS 8.7.1.3
AOS-222290 AOS-229250	Memory leak was observed in the **cli** process. This issue occurred when multiple CLI commands were executed without logging out from the session for a long period of time. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.5.0.13
AOS-222379 AOS-235427 AOS-232702	A few users experienced poor connectivity speed and users were unable to browse the internet intermittently. The fix ensures seamless connectivity and optimal network speed. This issue was observed in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-222983	Users were unable to issue the **no kernel coredump** command on managed devices running ArubaOS 8.6.0.9 or later versions. The fix ensures that the users are able to issue the **no kernel coredump** command.	ArubaOS 8.6.0.9
AOS-223274	Packet drop was observed on LACP configured AP-535 access points running ArubaOS 8.7.1.4 or later versions. This issue occurred when the outer IP header TOS value was different than the original inner IP header in ICMP error frame since the controller sent the ICMP destination unreachable frames back to the sender. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.4
AOS-223362 AOS-227300	Some AP-555 access points running ArubaOS 8.6.0.9 or later versions crashed unexpectedly. The log files listed the reason for the event as **Kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.9
AOS-224081 AOS-224083 AOS-225940	The **Dashboard > Overview > WLANs** page of the WebUI displayed incorrect **Usage** value. The fix ensures that the WebUI displays the correct **Usage** value. This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions in a cluster setup.	ArubaOS 8.5.0.10
AOS-224408	Some AP-325 access points running ArubaOS 8.6.0.0 or later versions were unable to send network capabilities in LLDP-MED information. Hence, clients were unable to receive the IP address. The fix ensures that the APs work as expected. This issue was observed in AP-325 access points running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.8.0.0
AOS-224523 AOS-224762	The **logging source-interface** command did not work as expected. The fix ensures that the command works as expected. This issue was observed in stand-alone controllers running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-224661	The IP classification configured using the **ip access-list geolocation** command incorrectly allowed traffic from countries that were blacklisted. The fix ensures that the IP classification feature works as expected. This issue was observed in 9000 Series controllers running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-225257 AOS-228159	A few clients experienced connectivity issues. This issue occurred when MBO was enabled on MPSK-AES SSIDs. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.1.4
AOS-225268	Some Remote APs were assigned to incorrect nodes. The fix ensures that the Remote APs are assigned to correct nodes. This issue was observed in managed devices running ArubaOS 8.6.0.0 or later versions in a cluster setup.	ArubaOS 8.7.1.3
AOS-225660	The **UCM** process crashed on Mobility Masters running ArubaOS 8.7.0.0 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.7.1.4

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-226333	Some AP-515 access points running ArubaOS 8.6.0.9 crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: SomeCrash Warm-reset**. The fix ensures that the APs work as expected. Duplicates: AOS-217939, AOS-218720, AOS-220295, AOS-221157, AOS-223959, AOS-226907, AOS-227773, AOS-228370, AOS-228372, AOS-228373, AOS-228374, AOS-228634, AOS-228733, AOS-228993, AOS-229001, AOS-229002, AOS-229003, AOS-229004, AOS-229006, AOS-229007, AOS-229008, AOS-229012, AOS-229013, AOS-229014, AOS-229100, AOS-234063, and AOS-228844	ArubaOS 8.6.0.9
AOS-226503	Dynamic bandwidth contract table was exhausted. This issue occurred due to ▪ Memory leak in BWC table. ▪ BWC table entries were not being cleared for clients that do not have IP address after L2 authentication. The fix ensures that the bandwidth contract configuration works as expected. This issue was observed in Mobility Masters running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-226579	Some APs running ArubaOS 8.6.0.13 or later versions generated multiple error messages, **ofa_gsm_event_user_process: port not found:1**. The fix ensures that APs work as expected.	ArubaOS 8.6.0.13
AOS-226851 AOS-227319 AOS-228483	The IPsec map in the route table of the managed device had an incorrect IP address of the Mobility Master. This issue occurred when the managed device had been up for more than 180 hours. The fix ensures that the correct IP address of the Mobility Master is available in the IPsec map. This issue was observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.7.1.5
AOS-226880	The LLDP process returned an incorrect value for **lldpLocSysName**. This issue occurred due to memory corruption. The fix ensures that the LLDP process returns correct values. This issue was observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-227079	When AirMatch changed channels and enabled DFS channels, connectivity issues were observed. The fix ensures that no connectivity issues are observed. This issue was observed in APs running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-227448 AOS-227447	The core file was not available after a crash. This issue occurred when the **switch_daemon** process crashed. The fix ensures that the core files are available when the Mobility Master crashes unexpectedly. This issue was observed in Mobility Masters running ArubaOS 8.6.0.13 or later versions.	ArubaOS 8.6.0.13
AOS-227454	Users were unable to connect to IKEv1 authenticated VIA. This issue occurred when **isakmd** process was stuck in busy state. The fix ensures that users are able to connect to IKEv1 authenticated VIA. This issue is observed was 7240XM controllers running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-227557	Some managed devices running ArubaOS 8.7.1.5 or later versions in a cluster setup incorrectly used the IP address of the Mobility Master as the NAS IP address. This issue occurred after a cluster live upgrade. The fix ensures that the managed devices use the correct NAS IP address.	ArubaOS 8.7.1.5
AOS-227719	The **Dashboard > Infrastructure** page of the WebUI displayed an incorrect **Uptime** of the Mobility Master. This issue occurred when the Mobility Master had been UP for more than a year. The fix ensures that the WebUI displays the correct **Uptime**. This issue was observed in Mobility Masters running ArubaOS 8.5.0.13 or later versions.	ArubaOS 8.5.0.13
AOS-228051	Some managed devices running ArubaOS 8.6.0.14 or later versions generated the log message, **wms[3677]: <316234> <5720> |wms| Cannot find Probe. At:handle_bss_channel_ delete line:117 Probe f0:5c:19:a2:4c:e0**. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.14
AOS-228056	Users were unable to delete the configured time range neither through the **no time-range** command nor through the **Configuration > Roles and Policies > <role> > Time Range** field of the WebUI. The fix ensures that the users are able to delete the configured time range. This issue was observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-228104	A few AP-535 access points running ArubaOS 8.6.0.16 or later versions crashed unexpectedly. The log files listed the reason for the event as **Firmware Assert - PC : 0x4b1ce6dc, whal_ reset.c:943 Assertion (wait < wait_timeout) failedparam0**. This issue occurred when, ▪ there was continuous bi-directional traffic flow in a mixed-client network. ▪ channels were busy The fix ensures that the APs work as expected.	ArubaOS 8.6.0.16
AOS-228397	The client match unsupported list was removed after a reboot of the Mobility Master. The fix ensures that the client match unsupported list is available after a reboot of the Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.6.0.10 or later versions.	ArubaOS 8.6.0.10
AOS-228429	A few clients were unable to obtain the correct role from the ClearPass Policy Manager. The fix ensures that the clients are able to obtain the correct role from the ClearPass Policy Manager. This issue was observed in Mobility Masters running ArubaOS 8.5.0.13 or later versions.	ArubaOS 8.5.0.13
AOS-228462	The **show airmatch debug schedule switch-info** command did not display any output. This issue occurred when there were more than 120 controllers connected in the network. The fix ensures that the **show airmatch debug schedule switch-info** command works as expected. This issue was observed in Mobility Masters running ArubaOS 8.6.0.10 or later versions.	ArubaOS 8.6.0.10

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-228475	Users were unable to drag and re-order server rules. The fix ensures that users are able to drag and re-order server rules. This issue was observed in Mobility Masters running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.1.5
AOS-228570 AOS-227756 AOS-229834	The **Dashboard > Overview** page of the WebUI displayed incorrect AP and client count. The fix ensures that the WebUI displays the correct number of AP and client count. This issue was observed in Mobility Masters running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-228714	APs located in different geographical locations were incorrectly present in the same AirMatch partition. This issue occurred when interferers with same MAC address was present at different geographical locations. The fix ensures that the APs in different geographical locations are not present in the same AirMatch partition. This issue was observed in APs running ArubaOS 8.6.0.14 or later versions.	ArubaOS 8.6.0.14
AOS-228785	Captive portal authentication in bridge mode did not work as expected for APs in mesh mode. The fix ensures that the captive portal authentication works as expected. This issue was observed in managed devices running ArubaOS 8.7.1.5 or later versions.	ArubaOS 8.7.1.5
AOS-228992 AOS-228997	The **auth** process crashed on managed devices running ArubaOS 8.0.0.0 or later versions. This issue occurred when the TACACS server was unresponsive. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.5
AOS-229059	The kernel logs of a controller contained the debug and kernel logs of the APs. The fix ensures that the kernel logs of a controller do not contain the logs of the APs. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.7.1.5
AOS-229097	The **auth** process crashed on managed devices running ArubaOS 8.0.0.0 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.5
AOS-229114	Some 7240XM controllers running ArubaOS 8.6.0.10 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2).** The fix ensures that the 7240XM controllers work as expected.	ArubaOS 8.6.0.10
AOS-229145	Some clients randomly fell back to the logon role. This issue occurred in bridge mode SSIDs. The fix ensures that the clients are assigned to the configured roles. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-229319 AOS-226891	Some clients in decrypt-tunnel mode were deauthenticated and sapcp ageout was also observed in management frames. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-229368	Users were unable to clone the configuration of an existing folder to a new folder. This issue occurred when the VLAN name or an ID is mapped to a user role. The fix ensures that the users are able to clone the configuration of an existing folder to a new folder. This issue was observed in Mobility Masters running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-229559	A wrong policy was enforced when a combination of DPI application-based rules and WebCC-based policies were used. This issue occurred when firewall classified traffic only based on HTTP and HTTPS protocol. The fix ensures that firewall considers other protocols like SSL, HTTP2, QUIC, and SPDY. This issue was observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-229622 AOS-232085	Some AP-535 access points running ArubaOS 8.6.0.15 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the reboot as **kernel panic: Rebooting the AP. NSS FW crashed**. The fix ensures that APs work as expected.	ArubaOS 8.6.0.15
AOS-229883	An SNMP walk returned incorrect values for the **wlsxWlanRadioTable** OID. The fix ensures that the SNMP walk returns correct values. This issue was observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-229897	Users were unable to download logs from the **Diagnostics > Technical Support** page of the WebUI. The fix ensures that the users are able to download logs using the WebUI. This issue was observed in Mobility Masters running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-229947 AOS-232100	The **stm** process crashed on managed devices running ArubaOS 8.6.0.16 or later versions in a cluster setup. This issue occurred when the operating mode of the AP was changed from AP mode to AM mode. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.16
AOS-229948	The **Configuration > Access Points** page of the WebUI did not display the list of available APs. Also, the number of available APs differed between the WebUI and CLI. The fix ensures that the WebUI displays the correct number of APs. This issue was observed in Mobility Masters running ArubaOS 8.6.0.9 or later versions. Duplicates: AOS-226909, AOS-230436, AOS-231548, AOS-232192	ArubaOS 8.6.0.9
AOS-229952	The output of the **show ap essid** command displayed an incorrect value for **VLAN**. The fix ensures that the command displays the correct value for **VLAN**. This issue was observed in managed devices running ArubaOS 8.5.0.13 or later versions. Duplicates**:** AOS-229695, AOS-229900, AOS-229953, AOS-228644, AOS-232410, and AOS-235524	ArubaOS 8.5.0.13

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-230061	Traffic got denied and ACLs were not applied correctly. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.6.0.15
AOS-230169	The firewall cp deny rule failed to deny traffic for cluster CoA VRRP addresses. The fix ensures that the firewall cp deny rule denies traffic as expected. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions in a cluster setup.	ArubaOS 8.8.0.1
AOS-230242	The **Configuration > WLANs** page of the WebUI did not display the list of available WLANs. The fix ensures that the WLANs page of the WebUI displays the list of available WLANs. This issue was observed in Mobility Masters running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-230417	The **Configuration > Access Points > Campus APs** page of the WebUI did not sort the entries based on the **Type** of the APs. The fix ensures that the WebUI sorts entries based in the **Type** of the APs. This issue was observed in Mobility Masters running ArubaOS 8.6.0.14 or later versions.	ArubaOS 8.6.0.14
AOS-230538	A few AP-555 access points running ArubaOS 8.7.1.4 or later versions failed to generate coredump. This issue occurred when the name of the AP had the special character "/". The fix ensures that the APs generate the coredump file.	ArubaOS 8.7.1.4
AOS-230598	The **auth** process crashed on managed devices running ArubaOS 8.0.0.0 or later versions. The log file listed the reason for the reboot as **Segmentation Fault: bridge_ip_user_free**. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.7
AOS-230690	The feature bits of Mobility Controller Virtual Appliance incorrectly changed to enabled after restoring flash backup. The fix ensures that the Mobility Controller Virtual Appliances work as expected. This issue was observed in Mobility Controller Virtual Appliances running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-230732	A few clients did not receive any reply from the DNS server. Also, packets that were dropped were encapsulated in GRE and the outer IP header had a checksum value of 0xFFFF. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.6.0.10 or later versions.	ArubaOS 8.6.0.10
AOS-230798 AOS-231576	The output of the **show global-user-table list** command displayed duplicate user entries for bridge-mode SSIDs. The fix ensures that the command does not display the duplicate entries. This issue was observed in Mobility Masters running ArubaOS 8.7.1.8.	ArubaOS 8.7.1.8

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-230807	Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **Kernel panic - not syncing: softlockup: hung tasks**. The fix ensures that APs work as expected. This issue was observed on APs running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.7.1.8
AOS-230822	The error message, **Error decrementing DS refcountfor cert** was displayed when users uploaded a new server certificate. This issue occurred when users tried to change the current switch certificate to an expired certificate. The fix ensures that the referencing for handling switch certificates works correctly. This issue was observed in Mobility Masters running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-230836	Clients with ASUS USB-AC68 USB wireless adapter were unable to pass traffic. This issue occurred when beamforming was enabled. The fix ensures that clients with ASUS USB-AC68 USB wireless adapter are able to pass traffic. This issue was observed in AP-345 access points running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-230842	The internal server authentication was marked as out of service. This issue occurred after a reboot of the managed device when the Mobility Master was down. The fix ensures that the managed devices work as expected. This issue was observed in managed devices, except 7000 Series and 7200 Series controllers, running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-230900 AOS-231081 AOS-234940	Some 530 Series and 550 Series access points running ArubaOS 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for reboot as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs function as expected.	ArubaOS 8.7.1.7
AOS-230957 AOS-234528 AOS-235240	Mobility Master Hardware Appliance running ArubaOS 8.9.0.1 or later versions was unable to monitor and provision managed devices and /tmp folder was fully utilized. The fix ensures that the Mobility Master Hardware Appliance works as expected.	ArubaOS 8.9.0.1
AOS-231218 AOS-232924 AOS-235193	High CPU utilization was observed in the **pptpd** process of stand-alone controllers running ArubaOS 8.5.0.0-FIPS or later versions. This issue occurred because the FIPS version did not support the **pptpd** process. The fix ensures support for the **pptpd** process.	ArubaOS 8.5.0.0-FIPS
AOS-231225	Stations were unable to associate to the APs. The fix ensures that stations could connect to APs. This issue was observed in APs running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-231326	Some managed devices running ArubaOS 8.7.1.7 or later versions crashed and rebooted unexpectedly. The log files listed the reason for this event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**. This issue occurred due to socket buffer corruption. The fix ensures that the managed devices work as expected. Duplicates: AOS-231256, AOS-233583, AOS-233673, AOS-231372	ArubaOS 8.7.1.7

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-231348	A few APs running ArubaOS 8.0.0.0 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **SomeCrash Warm-reset and AP-505 rebooted Panic:assert Warm-reset at the same time.** The fix ensures that the APs work as expected.	ArubaOS 8.7.1.4
AOS-231434	Some 7210 controllers running ArubaOS 8.6.0.15 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Soft Watchdog reset (Intent:cause:register de:86:70:2)**. The fix ensures that the 7210 controllers work as expected.	ArubaOS 8.6.0.15
AOS-231437 AOS-233640	Some APs were incorrectly power restricted and the radios got disabled. The fix ensures that the APs work as expected. This issue was observed in AP-505 and AP-515 access points running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.9.0.2
AOS-231535	A controller crashed and rebooted unexpectedly. The log files listed the reason for the event as **out-of-memory access**. This issue was observed in an environment with high 802.1x transaction rate and auth-server timeouts. The fix ensures that the controller works as expected. This issue was observed in 7220 controllers running ArubaOS 8.6.0.15.	ArubaOS 8.6.0.15
AOS-231654	A few clients got disconnected from the network. The log file listed the reason for the event as **Reason code: Previous authentication no longer valid (0x0002)**. The fix ensures seamless connectivity. This issue was observed in 200 Series access points running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-231770	Some clients were unable to pass traffic due to high memory utilization. The fix ensures that the clients can pass traffic. This issue was observed in APs running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.9.0.2
AOS-231849	Mesh Portal APs did not change channels even after AirMatch changed the channels. This issue was observed in APs that had only mesh VAPs configured. The fix ensures that the APs work as expected. This issue was observed in APs running ArubaOS 8.6.0.16 or later versions.	ArubaOS 8.6.0.16
AOS-231859	AirWave displayed an incorrect number of clients connected to the Mobility Master. This issue occurred when AMON stats messages were not sent for Remote AP wired users. The fix ensures that the AirWave displays the correct number of clients connected to the Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.1.6
AOS-231990	The **Dashboard > Infrastructure** page displayed an 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

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-232014	During the EST enrollment process, a dummy private key was generated and stored as a plain text. The fix ensures that the dummy key file is removed from the flash. This issue was observed in APs running ArubaOS 8.7.1.6 or later versions.	ArubaOS 8.7.1.6
AOS-232079	ACLs were not applied correctly. This issue occurred when DPI was enabled. The fix ensures that the ACLs are applied correctly on managed devices. This issue was observed in managed devices running ArubaOS 8.6.0.16 or later versions.	ArubaOS 8.6.0.10
AOS-232096	S-AAC controllers leaked data traffic of wireless clients that were connected in split-tunnel forwarding mode. The fix ensures that the controllers do not leak traffic. This issue was observed in managed devices running ArubaOS 8.7.1.6 or later versions.	ArubaOS 8.7.1.6
AOS-232120	Timestamp value was not updated correctly in the radius accounting packets. The fix ensures that the timestamp value is updated correctly. This issue was observed in 7280 controllers running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.10.0.0
AOS-232130	iOS native VPN with EAP authentication did not work on managed devices running ArubaOS 8.0.0.0 or later versions. The fix ensures that the iOS native VPN with EAP authentication works as expected.	ArubaOS 8.9.0.1
AOS-232171	The list of clients that were not L2 connected were still displayed in the user table even when CoA disconnect was triggered. The fix ensures that the user table is updated correctly. This issue was observed in managed devices running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-232277	Some managed devices running ArubaOS 8.7.1.5 or later versions displayed incorrect timestamp for the NTP server. However, the Mobility Master displayed the correct timestamp. The fix ensures that the managed devices display correct timestamp for NTP servers.	ArubaOS 8.7.1.5
AOS-232311	The user table did not list the entries of L3 connected clients and hence, clients were unable to pass traffic. Also, the netdestination configuration was not synchronized between authmgr and sapm processes. This issue was observed when ValidUser ACL was configured for bridge mode clients. The fix ensures that the users are able to pass traffic. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.10 or later versions.	ArubaOS 8.6.0.10
AOS-232430	The spanning tree and interface related configuration details were not displayed in the output of the **show running-config** command. The fix ensures that the command displays the spanning tree and interface related configuration details. This issue was observed in Mobility Masters running ArubaOS 8.6.0.10 or later versions.	ArubaOS 8.6.0.10

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-232443	Server derivation rules were not assigned correctly and an error message, **Missing server in attribute list** was displayed. This issue occurred when there was a delay in response from the RADIUS server. The fix ensures that the server derivation rules are assigned correctly. This issue was observed in stand-alone controllers running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-232475	Neither the **no time-range** command nor the **Configuration > Roles and Policies > <role> > Time Range** field of the WebUI allows users to delete the configured time range. The fix ensures that the WebUI works as expected. This issue is observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-232493	The entries of blacklisted clients were not synchronized between the managed devices. The fix ensures that the entries are synchronized between the managed devices. This issue was observed in managed devices running ArubaOS 8.6.0.15 or later versions in a cluster setup.	ArubaOS 8.6.0.15
AOS-232552	A few APs running ArubaOS 8.6.0.0 or later versions displayed multiple error log messages. This issue occurred due to a race condition. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.8
AOS-232643	Clients that did not support AMPDU aggregation faced periodic downstream traffic disruption. Enhancements to the wireless driver resolved the issue. This issue was observed in APs running ArubaOS8.6.0.0 or later versions.	ArubaOS 8.7.1.0
AOS-232800	Some managed devices that are part of an L3 mobility domain rebooted unexpectedly. The log files listed the reason for the reboot as **Reboot Cause: Nanny rebooted machine - mobileip process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.7.1.5 or later versions.	ArubaOS 8.7.1.5
AOS-232874	The WebUI did not work on standby Mobility Masters running ArubaOS 8.7.1.8 or later versions. The fix ensures that the WebUI works on standby Mobility Masters.	ArubaOS 8.7.1.7
AOS-232991	Users were unable to issue the **lc-cluster exclude-vlan** command and an error message, **ERROR: Invalid character** was displayed. The fix ensures that users are able to issue the **lc-cluster exclude-vlan** command . This issue was observed in Mobility Masters running ArubaOS 8.7.1.7 or later versions.	ArubaOS 8.7.1.7
AOS-233005	Memory leak was observed in the **stm** process of Mobility Master. The fix ensures that the Mobility Master works as expected. This issue was observed in Mobility Masters running ArubaOS 8.7.1.7 or later versions.	ArubaOS 8.7.1.7

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-233043	Some managed devices were unable to come up on the Mobility Master. This issue occurred when the managed devices incorrectly routed traffic via the default GRT route. The fix ensures that the managed devices connect to Mobility Master seamlessly. This issue is observed in managed devices running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-233115 AOS-233213	A few clients dropped Wifi-calling IPsec traffic that came through GRE tunnels. This issue occurred when tunnel keepalive was enabled. The fix ensures that the clients do not drop any traffic. This issue was observed in managed devices running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-233188 AOS-233811 AOS-234844	Some managed devices were unable to come up using ZTP. This issue occurred when the Master IP configuration was not available. The fix ensures that the managed devices are able to come up using ZTP. This issue was observed in managed devices running ArubaOS 8.7.1.7 or later versions.	ArubaOS 8.7.1.7
AOS-233199	When clients moved between UAC and S-UAC, the details of the active and dormant stations were not displayed in the output of the **show ap association** and **show ap association dormant** commands. The fix ensures that the managed devices display the details of the active and dormant stations. This issue was observed in managed devices running ArubaOS 8.7.1.9 or later versions in a cluster setup.	ArubaOS 8.7.1.9
AOS-233217	Some AP-535 access points did not transmit beacons in 5 GHz radio mode and clients were unable to view the SSIDs. The fix ensures that the APs transmit beacons and work as expected. This issue was observed in AP-535 access points running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.10
AOS-233290	The **sapd** process crashed on AP-205 access points running ArubaOS 8.7.1.6 or later versions. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.6
AOS-233399	Poor network performance was observed, and captive portal page did not load as expected for non-HE devices. This issue occurred when open system was configured. The fix ensures that the APs work as expected. This issue was observed in 510 Series access points running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-233411 AOS-234524 AOS-235363	Some APs running ArubaOS 8.6.0.17 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.17
AOS-233438	Some AP-515 access points running ArubaOS 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **PC is at phy_utils_write_phyreg_nopi+0x70/0x130 [wl_v6]**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.0

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-233518	Some AP-635 access points running ArubaOS 8.0.0.0 or later versions crashed unexpectedly. The log files listed the reason for event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first (:Excep :0 Exception detected Thread name : WLAN_SCHED0)**. The fix ensures that the APs work as expected.	ArubaOS 8.9.0.3
AOS-233572	Some AP-335 access points running ArubaOS 8.7.1.9 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.9
AOS-233766	IPsec flapping was observed between primary and secondary Mobility Masters in a certificate-based Layer 3 redundancy deployment. The fix ensures no IPsec flapping. This issue is observed in Mobility Masters running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-233854 AOS-234907	Some managed devices running ArubaOS 8.7.1.8 or later versions generated excessive kernel logs. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.8
AOS-233869	The **im_helper** process was stuck in **busy** state when users tried to export the iBeacon configurations from the Mobility Master. The fix ensures that the **im_helper** process is not stuck. This issue was observed in Mobility Masters running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-234082	Some AP-535 access points running ArubaOS 8.7.1.9 or later versions crashed unexpectedly. The log files listed the reason of the event as **kernel panic: Take care of the TARGET ASSERT first (ar_wal_tx_seq.c:3041 Assertion)**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.9
AOS-234329	Some AP-515 access points running ArubaOS 8.7.1.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **PC is at asap_set_wmm+0x5d4**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.6
AOS-234477	Instead of scanning at the scheduled intervals, radios were wrongly scanned for every 10 seconds. The fix ensures that the radios are scanned at the configured time intervals. This issue was observed in APs running ArubaOS 8.4.0.0 or later versions	ArubaOS 8.4.0.0
AOS-234603 AOS-235235	The **ble_relay** process crashed on 7205 controllers running ArubaOS 8.7.1.9 or later versions. The log files listed the reason for the event as **Module BLE Relay controller is Busy. Please try later**. The fix ensures that the controllers work as expected.	ArubaOS 8.7.1.9
AOS-235257	The **AP sapd** process crashed on managed devices running ArubaOS 8.7.1.7 or later versions. This issue occurred when a hotspotter attack was detected. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.7

Table 6: *Resolved Issues in ArubaOS 8.7.1.10*

New Bug ID	Description	Reported Version
AOS-2312488	Remote APs were unable to come up on the managed devices and an error message, **Cluster inner ip is zero for RAP, mac 20:4c:03:5b:97:4e. Check lc-rap-pool configuration on the MM** was displayed. This issue occurred when the IP address of the lc-rap-pool ended with 127. The fix ensures that the Remote APs are able to come up on managed devices. This issue was observed in Remote APs running ArubaOS 8.7.1.6 or later versions.	ArubaOS 8.7.1.6

Chapter 7
Known Issues in ArubaOS 8.7.1.10

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

Limitation

Following are the limitations observed in this release:

Airtime Fairness Mode

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

No Support for Unique Local Address over IPv6 Network

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

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.

Known Issues

Following are the known issues observed in this release:

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-125897	151952	When a managed device reboots, APs and clients boot without IP addresses and other fields. This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. Duplicates: AOS-187598, AOS-189036, AOS-192082 , AOS-192723 , AOS-192731, AOS-192734, AOS-195746, AOS-198423, and AOS-204676	ArubaOS 8.0.1.0
AOS-151022 AOS-188417	185176	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.	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

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
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 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-193231 AOS-200101 AOS-207456	—	The **Dashboard > Infrastructure > Access Devices** page of the WebUI displays an error message, **Error retrieving information**. This issue is observed in Mobility Masters running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-200515 AOS-219987	—	The **DDS** process crashes on managed devices running ArubaOS 8.3.0.10 or later versions.	ArubaOS 8.3.0.10
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-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-203614 AOS-209261	—	The Mobility Master dashboard does not display the number of APs and clients that are 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-203682 AOS-195432	—	The **Dashboard > WLANs** page of the WebUI does not display the list of all the clients and APs. This issue is observed in Mobility Masters running ArubaOS 8.5.0.2 or later versions. **Duplicates:** AOS-195432, AOS-195433, AOS-218290, and AOS-220829	ArubaOS 8.6.0.15

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206541	—	The **Maintenance > Software Management** page does not display the list of all managed devices that are 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
AOS-206929	—	The **show global-user-table** command does not provide an IPv6-based filtering option. This issue is observed in Mobility Masters running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-206930	—	Some Mobility Masters running ArubaOS 8.7.0.0 or later versions allow to configure the same IPv6 address twice. This issue occurs when the user enters the same IPv6 address in a different format.	ArubaOS 8.7.0.0
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-207303	—	Users are unable to add a managed device to an existing cluster of managed devices configured with rap-public-ip address. This issue is observed in managed devices running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
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-209273	—	The **Dashboard > Infrastructure** page of the WebUI does not display the data in graphical charts for mesh APs. This issue is observed in Mobility Masters running ArubaOS 8.7.0.0 or later versions	ArubaOS 8.7.0.0

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
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 Masters running ArubaOS 8.3.0.13 or later versions.	ArubaOS 8.3.0.13
AOS-209977	—	An SNMP query with an incorrect string fails to record the offending IP address in the trap or log information. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
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-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-212772 AOS-221882	—	Some IPv6 clients are unable to access websites that have only IPv4 addresses. This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-214944	—	The **profmgr** process crashes on Mobility Masters running ArubaOS 8.6.0.7 or later versions. This issue occurs while deleting roles configured for AirGroup.	ArubaOS 8.6.0.7
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 35 seconds is configured as the UCC session idle timeout.	ArubaOS 8.6.0.6
AOS-217194	—	The WebUI displays an error message, **access-group is not configured** while configuring BCMC optimization. This issue is observed in managed devices running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-217890	—	Some managed devices running ArubaOS 8.5.0.10 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (SOS Assert)**.	ArubaOS 8.5.0.10
AOS-218037 AOS-232229	—	The **Source interface** drop-down list in the **Configuration > Controller** page of the WebUI does not list the source interface options. This issue occurs while configuring the Master IP address. This issue is observed in Mobility Masters running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.8.0.0

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218426	—	The status LED displays incorrect status. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-219307 AOS-223234	—	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-219379 AOS-221300	—	Some managed devices are unable to connect to Mobility Masters. The log files list the reason for the event as **<WARN> |fpapps| handleMasterIpMsg: Ignoring duplicate Uplink update from CFGM: ip x.x.x.x sec_master_ip 0.0.0.0 role 3;**. This issue is observed in managed devices running ArubaOS 8.7.1.1 or later versions in a cluster setup.	ArubaOS 8.7.1.1
AOS-219765 AOS-231995 AOS-232259	—	Some AP-555 access points running ArubaOS 8.7.1.7 crash and reboot unexpectedly. The log files list the reason for the event as **AP-555 crashed: Take care of the TARGET ASSERT first - ar_wal_tx_seq.c:3041 Assertion seq_ctrl**.	ArubaOS 8.7.1.7
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-219936	—	The stand-alone controllers display the error message, **Module Profile Manager is busy. Please try later** while configuring netdestination. This issue is observed in stand-alone controllers running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
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-221982	—	Some VIA users experience connectivity issues. This issue is observed on IKEV2 EAP-GTC terminated VIA clients that use external ClearPass Policy Management (CPPM) authentication. This issue is observed in managed devices running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-222445 AOS-229980	—	Some managed devices running ArubaOS 8.7.1.8 or later versions log the error message, **<DE-cx7008-2 10.0.103.52> publisher[3302]: PAPI_Send: sendto DHCP Server failed: No such file or directory Message Code 0 Sequence Num is 1760.**	ArubaOS 8.7.1.8
AOS-222493	—	The **AP group** drop-down list in the **Configuration > Access Points > Campus APs** page of the WebUI takes a long time to load the list of available AP groups. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.7.1.3

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222786	—	The logs downloaded using the WebUI are incomplete and have missing files. This issue is observed in Mobility Masters running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.71.3
AOS-223337	—	The clients added to the client match unsupported list are still considered for client match steers. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-224463	—	The RADIUS Radsec server does not work with TPM certificates on Mobility Masters running ArubaOS 8.6.0.0-FIPS or later versions.	ArubaOS 8.6.0.0-FIPS
AOS-225070	—	The AirGroup server table incorrectly displays duplicate host names. This issue is observed in managed devices running ArubaOS 8.6.0.11 or later versions.	ArubaOS 8.6.0.11
AOS-225135 AOS-229451	—	Clients connected to APs are unable to send or receive data packets from APs. This issue occurs when the ACL changes are not updated on APs. This issue is observed in APs running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-225871	—	The **Reboot** option in the **Maintenance > Access Points** page does not reboot the APs. This issue is observed in Mobility Masters running ArubaOS 8.7.1.2 or later versions.	ArubaOS 8.7.1.2
AOS-226426	—	The Mobility Master Hardware Appliances running ArubaOS 8.5.0.10 or later versions display the message, **DHCP WAIT** and the menu options are disabled. This issue occurs after a reboot.	ArubaOS 8.5.0.10
AOS-226455	—	The **show datapath netdest-id** command does not display any output. This issue is observed in managed devices running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-226773	—	The MAC ACLs do not work as expected when OpenFlow is enabled. This issue is observed in managed devices running ArubaOS 8.6.0.11 or later versions in a cluster setup.	ArubaOS 8.6.0.11
AOS-227016 AOS-229420	—	Some users experience a delay while downloading the VIA VPN profile. This issue is observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-227076 AOS-226143	—	AppRF fails to classify traffic for a few applications. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.12 or later versions.	ArubaOS 8.5.0.12

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-227258	—	The **Dashboard > Overview** page of the WebUI displays the status of 2.4 GHz radio even when 2.4 GHz radio was disabled in the rf dot11g-radio-profile. This issue is observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-227324	—	The **ofc_cli_agent** process crashes on Mobility Masters running ArubaOS 8.6.0.13 or later versions. This issue occurs when the **show openflow-controller ports** command is executed.	ArubaOS 8.6.0.13
AOS-227458	—	Some managed devices running ArubaOS 8.6.0.10 or later versions log multiple **DHCP-RELAY** and **Cannot find Probe** syslog messages.	ArubaOS 8.6.0.10
AOS-227542	—	Some Mobility Masters running ArubaOS 8.7.1.4 or later versions display the error message, **topology [6772]: <310310> <6772> <ERRS> |topology| |ofc-topology| max port limit(current:8750, max:8750) reached, rejecting new.**	ArubaOS 8.7.1.4
AOS-227659	—	Some managed devices running ArubaOS 8.7.1.4 or later versions are unable to download the roles from the ClearPass Policy Manager. This issue occurs when the roles exceed the buffer size of 16kb.	ArubaOS 8.7.1.4
AOS-227916	—	Mobility Masters running ArubaOS 8.7.1.4 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Nanny rebooted machine - low on free memory due to OFC flow_manager leak**.	ArubaOS 8.7.1.4
AOS-227966	—	A few 7010, 7024, 7205, and 7280 controllers running ArubaOS 8.0.0.0 or later versions respond with its own MAC address to ARP requests sent for the management interface.	ArubaOS 8.7.1.6
AOS-227976	—	ICMP incorrectly forwards traffic through the management port instead of the data port. This issue occurs when the **ip default-gateway mgmt <gateway-ip>** address is configured. This issue is observed in 7205, 7010, 7024, and 7280 controllers running ArubaOS 8.7.1.7 or later versions. **Workaround:** It is recommended not to configure the IP default-gateway management address for 7010, 7024, 7205, and 7280 controllers running ArubaOS 8.7.1.7 or later versions.	ArubaOS 8.7.1.7
AOS-227981	—	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

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-228356	—	The **detect-wireless-hosted-network** and **protect-wireless-hosted-network** parameters of the **ids unauthorized-device-profile** command does not work as expected in stand-alone controllers running ArubaOS 8.6.0.13 or later versions.	ArubaOS 8.6.0.13
AOS-228502	—	A managed device in a cluster was unable to pass through manual SNMP Walk performed on Linux / AirWave server. This issue is observed in managed devices running ArubaOS 8.7.1.6 or later versions.	ArubaOS 8.7.1.6
AOS-229024	—	Some AP-505 access points running ArubaOS 8.7.1.5 or later versions crashes and reboots 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-229207	—	Users observe a discrepancy between the client count displayed in the WebUI of aMobility Master and the CLI of a managed device. This issue occurs because the WebUI of the Mobility Master reports the client count including the client entries that are retained to accommodate temporary client disconnections. This issue is observed in Mobility Masters running ArubaOS 8.5.0.13 or later versions.	ArubaOS 8.5.0.13
AOS-229263	—	Some AP-325 access points running ArubaOS 8.7.1.6 or later versions crashed unexpectedly. The log files list the reason for the event as **PC is at aruba_am_tx_pkt_handler_data_ol+0xe60/0x1b44 and aruba_am_tx_pkt_handler_data_ol+0xe48/0x1b44**.	ArubaOS 8.7.1.6
AOS-229474 AOS-229582 AOS-229990	—	The **show ap database flags** command does not filter the output based on the specified flags. This issue is observed in Mobility Masters running ArubaOS 8.6.0.15 or later versions.	ArubaOS 8.6.0.15
AOS-229690	—	The output of the **show ucc** command does not display a few column titles. This issue is observed in Mobility Masters running ArubaOS 8.7.0.0. or later versions.	ArubaOS 8.7.0.0
AOS-230375	—	Mobility Master fails to push the mapping configuration of the web server certificate to the managed devices. This issue is observed in Mobility Masters running ArubaOS 8.0.1.0 or later versions.	ArubaOS 8.0.1.0
AOS-230434	—	A few AP-305 access points running ArubaOS 8.7.1.7 or later versions crash unexpectedly. The log files list the reason for the event as **PC is at osif_vap_open+0x24/0x50**.	ArubaOS 8.7.1.7
AOS-230475 AOS-231207	—	API enforcement issues are observed when DPI and WebCC rules coexist. This issue is observed in managed devices running ArubaOS 8.6.0.13 or later versions.	ArubaOS 8.6.0.13

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-230508	—	A few APs crash and reboot unexpectedly. The log files list the reason for the event as **kernel page fault at virtual address 00000000, epc == 8017d554, ra == c005e32c**. This issue is observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-231233	—	Users are unable to upgrade APs using the FTP server. Also, the TFTP server is selected automatically to upgrade the APs. This issue is observed in managed devices running ArubaOS 8.7.1.5 or later versions.	ArubaOS 8.7.1.5
AOS-231649	—	Users with read-only access are able to enable configurations and view passwords configured for WLANs. This issue is observed in Mobility Masters running ArubaOS 8.7.1.6 or later versions.	ArubaOS 8.7.1.6
AOS-232377	—	PAN firewall integration does not work as expected on 7240XM controllers running ArubaOS 8.7.1.5 or later versions.	ArubaOS 8.7.1.5
AOS-232378	—	The **pim** process crashes on managed devices running ArubaOS 8.7.1.8 or later versions.	ArubaOS 8.7.1.8
AOS-232462	—	Some managed devices running ArubaOS 8.6.0.10 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Reboot Cause: Reboot Cause: Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:60)**. This issue occurs due to memory corruption.	ArubaOS 8.6.0.10
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-233926	—	Some AP-535 access points running ArubaOS 8.7.1.9 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **kernel panic: Take care of the TARGET ASSERT first (ERR_ MACTX_CBF_SS_PER_USER:0 Ucode Asserted).**	ArubaOS 8.7.1.9
AOS-234202	—	Some AP-535 access points running ArubaOS 8.7.1.9 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **kernel panic: Take care of the TARGET ASSERT first (wal_soc_ dev_hw.c:667 Assertion)**.	ArubaOS 8.7.1.9
AOS-234819 AOS-235085	—	Some Remote APs running ArubaOS 8.6.0.9 or later versions do not broadcast BSSIDs and are stuck in AM mode. **Workaround:** Reload the managed device or re-configure the DRT file using the **ap regulatory activate <drt_file_name>** command,	ArubaOS 8.6.0.9

Table 7: *Known Issues in ArubaOS 8.7.1.10*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-235063	—	An error message, I**nvalid data: Static FW CP ACL cannot be deleted** is displayed when users try to delete the custom ACL. This issue is observed in managed devices running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-235847	—	The **ble_daemon_s** process crashes on 9004 controllers running ArubaOS 8.7.1.10.	ArubaOS 8.7.1.10

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, 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 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 39 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 39 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 39 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.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 39.

NOTE

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

In the WebUI

The following steps describe how to upgrade 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.

NOTE

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.

NOTE

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

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

In the CLI

The following steps describe how to upgrade 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 39 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 39 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 39.
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.