ArubaOS 8.7.1.4 Release Notes

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

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

Contents

Chapter 1
Revision History

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

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 2
Release Overview

This ArubaOS release notes includes the following topics:

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

For a list of terms, refer Glossary.

Related Documents

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

- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- Aruba *Mobility Master Licensing Guide*
- *Aruba Virtual Appliance Installation Guide*
- *Aruba AP Software Quick Start Guide*

Supported Browsers

The following browsers are officially supported for use with the ArubaOS WebUI:

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

Terminology Change

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

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

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.arubanetworks.com/
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Chapter 3
New Features and Enhancements in ArubaOS 8.7.1.4

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

Chapter 4
Supported Platforms in ArubaOS 8.7.1.4

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 8.7.1.4*

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 8.7.1.4*

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 8.7.1.4*

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

Table 5: *Supported AP Platforms in ArubaOS 8.7.1.4*

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 8.7.1.4

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_80433

Chapter 6
Resolved Issues in ArubaOS 8.7.1.4

The following issues are resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-183519	—	Some APs were incorrectly marked as down in datazone controllers. The fix ensures that the controllers display the correct status of APs. This issue was observed in stand-alone controllers running ArubaOS 8.3.0.4 or later versions.	ArubaOS 8.3.0.4
AOS-197210	—	WebUI took a long time to display data. The fix ensures that the WebU displays data without any delay. This issue was observed in stand-alone controllers running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-200762	—	Users were unable to disable Prohibit IP spoofing firewall feature. The fix ensures that users are able to disable the Prohibit IP spoofing feature. This issue when the ARP request frame got flooded as a broadcast ARP instead of unicast ARP. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-202308 AOS-216193 AOS-219439	—	A few clients took a long time to roam between APs. The fix ensures that clients do not take a long time to roam between APs. This issue was observed in stand-alone controllers running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-203077 AOS-203232	—	Configurations committed using the **firewall cp** command were not synchronized on the standby Mobility Master. This issue occurred when static firewall entries were deleted. The fix ensures that the configurations committed using the **firewall cp** command are synchronized on the standby Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.6.0.3 or later versions.	ArubaOS 8.6.0.3
AOS-203115 AOS-217219	—	The IAP-VPN tunnel was down and the error message, **Failed to create internal-iap IP user entry and user entry due to too many user entries 128** was displayed. This issue occurred when the user table had 128 entries. The fix ensures that the stand-alone controllers work as expected. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203168	—	Some managed devices running ArubaOS 8.6.0.3 or later versions frequently disconnected from the cluster. Also, the cluster heartbeats were randomly missed on managed devices which led to packet loss. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.3
AOS-204241	—	Some managed devices logged spurious DHCP DBUG messages. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-205319	—	Some APs running ArubaOS 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected. **Duplicates:** AOS-206993, AOS-216577, AOS-218524, AOS-220039, and AOS-220917	ArubaOS 8.6.0.5
AOS-206216 AOS-213940 AOS-214072 AOS-220300	—	Some APs running ArubaOS 8.6.0.6 crashed unexpectedly. The log file listed the reason for the event as, **reboot caused by Firmware Assert - ar_wal_tx_de.c:68**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.6
AOS-206389 AOS-216860	—	The **SAPD** process crashed on managed devices running ArubaOS 8.6.0.5 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.5
AOS-206537	—	The **H** flag indicating standby tunnel was not displayed in the output of the **show datapath tunnel-table** command and this resulted in a network loop. The fix ensures that the **H** flag is displayed in the output of the **show datapath tunnel-table** command. This issue was observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206907	—	Some AP-303H access points running ArubaOS 8.5.0.5 or later versions crashed and rebooted unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: assert.** The fix ensures that the APs work as expected.	ArubaOS 8.5.0.5
AOS-207775 AOS-215946	—	The **auth** process crashed on managed devices running ArubaOS 8.5.0.9 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.9
AOS-207841	—	Some managed devices running ArubaOS 8.7.0.1 or later versions experienced configuration failures. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.0.1

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207915	—	Some 500 Series access points running ArubaOS 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP Reboot reason: BadAddr:ecf47526bb436b6e PC:wlc_mutx_ bw_ policy_update+0x156c/0x2938 [wl_v6] Warm-reset.** The fix ensures that the APs work as expected. **Duplicates:** AOS-208119, AOS-209128, AOS-210182, AOS-210217, AOS-211247, AOS-211252, AOS-211715, AOS-211774, AOS-212111, AOS-212235, AOS-212557, AOS-212741, AOS-212930, AOS-212961, AOS-214656, AOS-214965, AOS-215250, AOS-215656. AOS-217649, and AOS-217692.	ArubaOS 8.6.0.4
AOS-208337	—	The **airmatch_recv** process crashed on Mobility Master Virtual Appliances running ArubaOS 8.5.0.7 or later versions. The fix ensures that the Mobility Master Virtual Appliances work as expected. **Duplicates:** AOS-209348, AOS-212655, AOS-213442, AOS-219341, and AOS-221406	ArubaOS 8.5.0.7
AOS-208421	—	Some managed devices running ArubaOS 8.5.0.10 crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Soft Watchdog reset**. The fix ensures that the managed devices work as expected. **Duplicates:** AOS-209367, AOS-209509, AOS-209606, AOS-211577, AOS-211772, AOS-211879, and AOS-212502.	ArubaOS 8.5.0.10
AOS-208740 AOS-213754	—	The **profmgr** process crashed on a few Mobility Master running ArubaOS 8.5.0.11 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.5.0.11
AOS-208846	—	Clients connected to bridge mode SSIDs were unable to receive IP addresses and pass traffic. The fix ensures that clients are able to receive IP addresses. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-209086 AOS-216862	—	The **Dot1x** process crashed on managed devices running ArubaOS 8.5.0.0 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.0
AOS-209093 AOS-210452	—	Some managed devices running ArubaOS 8.7.0.0 or later versions generated multiple AMON receiver errors. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.0.0

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209130	—	Stale user entries were not removed from the user-table and hence, new users could not connect to the managed device. The fix ensures that the managed device works as expected. This issue was observed in managed devices running ArubaOS 8..6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-209165		The **Configuration > AP Groups** page did not sort the list of AP groups based on when they were created, and hence the newly created AP groups were displayed at the bottom of the table. The fix ensures that the WebUI sorts the list of AP groups. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-209626	—	A few clients experienced connectivity issue. The fix ensures seamless connectivity. This issue was observed in managed device running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-209686	—	The **show ap remote client status** command displayed the **KRx** value as 0. The fix ensures that the command displays the correct **KRx** value. This issue was observed in Mobility Masters running ArubaOS 8.8.0.0.	ArubaOS 8.8.0.0
AOS-209797 AOS-218932	—	Some Mobility Master Hardware Appliance running ArubaOS 8.6.0.4 or later versions intermittently returned high values for SNMP walk for OID **ifOutDiscards.** The fix ensures that the Mobility Master Hardware Appliance does not return incorrect values for SNMP walk for OID **ifOutDiscards.**	ArubaOS 8.6.0.4
AOS-209912	—	A few managed devices failed to filter and drop spoofed ARP responses from the clients that sent ARP response for the IP address that did not belong to the clients. The user entry for the other IP address was present on the managed devices but not in the route cache table. The fix ensures that the managed devices are able to stop ARP spoofing attacks for such clients. This issue was observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-209996	—	Some APs running ArubaOS 8.5.0.9 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: __bug**. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.9
AOS-210198	—	The **Dashboard > Security > Detected Radio** page of the WebUI displayed incorrect number of **Clients**. The fix ensures that the WebUI does not display incorrect number of **Clients**. This issue was observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210515 AOS-219060	—	The **blmgr** process crashed on Mobility Masters running ArubaOS 8.6.0.5 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.6.0.5
AOS-210845	—	Some AP-535 and AP-555 access points running ArubaOS 8.6.0.6 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first.** Enhancements to the wireless driver resolved the issue. Duplicates: AOS-219154, AOS-220187, AOS-221165, AOS-217214, and AOS-217871	ArubaOS 8.6.0.6
AOS-210922	—	The **auth** process crashed on stand-alone controllers running ArubaOS 8.5.0.10 or later versions and APs rebooted unexpectedly. The log file listed the reason for the reboot as **Unable to set up IPSec tunnel, Error:RC_ERROR_IKEV2_TIMEOUT**. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.5.0.10
AOS-210945 AOS-213441	—	Some stand-alone controllers running ArubaOS 8.6.0.4 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:e0:2)**. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.6.0.4
AOS-210963	—	Some AP-203R access points running ArubaOS 8.7.0.0 or later versions did not send wireless tarpit / deauth frames even if IDS wireless containment is configured. The fix ensures that the APs work as expected.	ArubaOS 8.7.0.0
AOS-210990	—	Some managed devices sent BPDUs when STP was globally disabled. The fix ensures that the managed devices do not send BPDUs when STP is globally disabled. This issue was observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.4
AOS-210992	—	The Mobility Master displayed an error message, **Flow Group delete: id not found** after an upgrade. This issue occurred when logging levels were not configured correctly. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-211437 AOS-218454	—	It took a long time to synchronize configurations between a stand-alone controller and a standby controller running ArubaOS 8.6.0.8. The fix ensures that configurations between a stand-alone controller and a standby controller do not take a long time to synchronize configurations.	ArubaOS 8.6.0.8

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-211545 AOS-217654	—	Some APs running ArubaOS 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt.** The fix ensures that the APs work as expected.	ArubaOS 8.5.0.10
AOS-211587 AOS-216068 AOS-222052	—	High CPU utilization was observed in **udbserver** and **postgres** processes. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-211622 AOS-211728 AOS-220433	—	Some stand-alone controllers running ArubaOS 8.3.0.14 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:0:2c)**. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.3.0.14
AOS-211730 AOS-220327	—	Users were unable to map server certificate as switch certificate on a secondary Mobility Master running ArubaOS 8.5.0.10 or later versions. The fix ensures that users are able to map server certificate as switch certificate on a secondary Mobility Master.	ArubaOS 8.5.0.10
AOS-212198	—	Some RAP-3WN Remote APs running ArubaOS 8.5.0.8 or later versions rebooted unexpectedly. This issue occurred when the time between the controller and the Remote AP was not in synchronization. The fix ensures that the Remote APs work as expected.	ArubaOS 8.5.0.8
AOS-212423	—	High bandwidth usage was observed on a few clients. The fix ensures optimal bandwidth usage. This issue occurred when AP ports in split tunnel forwarding mode were moved to tunnel forwarding mode. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-212904	—	Users were unable to access the L3 redundant controller using CLI and the error message, **Permission path (/) is Invalid for user (ads.jvicentini)** was displayed. The fix ensures that the users are able to access the L3 redundant controller using CLI. This issue was observed in standby Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212935	—	Temporary ACL was applied to user roles even if the disaster-recovery mode was disabled. This issue occurred when configuration changes in disaster-recovery mode were not submitted using the **write memory** command. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.3.0.6 or later versions.	ArubaOS 8.3.0.6
AOS-212936	—	Some users experienced network outage. The fix ensures that users do not experience network outage. This issue was observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-212991	—	The **use-ip-for-calling-station** parameter of the **aaa authentication-server radius** command did not work as expected for VIA clients. The fix ensures that the **aaa authentication-server radius** command works as expected. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-213011 AOS-219946	—	Packet loss was observed for a few clients during a cluster failover. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.10
AOS-213041 AOS-215501	—	A managed device did not classify web-cc and DPI traffic. The fix ensures that the managed device classifies web-cc and DPI traffic. This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-213115	—	Some managed devices running ArubaOS 8.5.0.10 crashed and rebooted unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first.** The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.10
AOS-213307	—	L2 GRE ICMP keepalive response was sent outside the tunnel and hence, it was dropped by the firewall. This issue was observed in managed devices running ArubaOS 8.5.0.1 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.6
AOS-213337	—	A few AP-325 access points running ArubaOS 8.5.0.10 or later versions crashed unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.10
AOS-213492	—	Some APs running ArubaOS 8.6.0.6 logged the error message, **assoc response: try later** when MBO was enabled. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.6

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213784	—	A server received multiple **GSM radio lookup failed, error(error_htbl_key_not_found)** notifications for all BSSIDs. This issue is resolved by moving the GSM lookup failure logs to user-debug category. This issue was observed in a Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-213924 AOS-217233	—	Mobility Controller Virtual Appliances running ArubaOS 8.7.0.0 or later versions displayed incorrect VLAN ID details for some wired users. The fix ensures that the Mobility Controller Virtual Appliances display correct VLAN IDs.	ArubaOS 8.7.0.0
AOS-214243 AOS-215775	—	Some managed devices running ArubaOS 8.6.0.7 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**. This issue occurred due to a race condition. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.7
AOS-214391 AOS-217130 AOS-217832	—	Some APs were unable to come up on a managed device. This issue occurred when UDP 8209 traffic was sent without establishing IPsec tunnels. The fix ensures that the APs are able to come up on a managed device. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-214416	—	Some stand-alone controllers running ArubaOS 8.6.0.6 or later versions displayed the error message, **An internal system error has occurred at file main.c function rx_handler line 1517 error sxdr_read_str_ safe szFunctionName failed.** The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.6.0.6
AOS-214434	—	Some APs were unable to come up on a managed device. This issue occurred when UDP 8209 traffic was sent without establishing IPsec tunnels. The fix ensures that the APs are able to come up on a managed device. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-214510 AOS-219139	—	A few clients were disconnected from the network. The log files listed the reason for the event as **Wlan driver excessive tx fail quick kickout**. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-214963	—	Some APs running ArubaOS 8.5.0.11 or later versions detected false radar. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.11

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-214977 AOS-220420	—	Memory leak was observed in **arci-cli-helper** process. This issue occurred while running an API script. The fix ensures that the APs work as expected. This issue was observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-215012 AOS-215567	—	The AP debug counters, **Total Bootstraps** and **Reboots** were not reset after upgrading the managed devices to ArubaOS 8.5.0.11 or later versions. The fix ensures that the AP debug counters are reset. This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-215021	—	The **Channel Width Capability** configured on AirWave was not available in the **Dashboard > Overview > Wireless Clients** page of the WebUI. The fix ensures that the WebUI displays the **Channel Width Capability**. This issue is observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-215048 AOS-218412	—	A few clients were unable to connect to 802.1X SSIDs. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-215073	—	Some AP-515 access points running ArubaOS 8.5.0.8 or later versions went down and kept rebooting. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.8
AOS-215495	—	Some AP-535 access points running ArubaOS 8.5.0.5 or later versions displayed the error message, **ARM Channel 40 Physical_Error_Rate 0 MAC_Error_Rate 84 Frame_Retry_Rate 0 arm_error_rate_threshold 70 arm_error_rate_wait_time 90**. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.5
AOS-215498	—	Some AP-535 access points running ArubaOS 8.5.0.11 or later versions detected false radar. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.11
AOS-215546	—	The CLI did not trigger session timeout even if paging was enabled. The fix ensures that the CLI triggers session timeout. This issue was observed in Mobility Masters and managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.6.0.5
AOS-216525	—	A few 9012 controllers running ArubaOS 8.6.0.0 or later versions experienced traffic drop when the client and server were on different VLANs. The fix ensures that the 9012 controllers work as expected.	ArubaOS 8.6.0.4
AOS-216874 AOS-219841	—	The virtual MAC address of]VLAN got deleted from the bridge table and hence, resulted in a network outage. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216972	—	Some managed devices running ArubaOS 8.6.0.7 or later versions forwarded data frames that are larger than the configured IPsec tunnel MTU value. The fix ensures that the managed devices do not forward data frames that are larger than the configured IPsec tunnel MTU value.	ArubaOS 8.6.0.7
AOS-217104 AOS-219159	—	ESI redirect failed and traffic was forwarded to the default gateway. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-217106	—	The **no valid** parameter of the **ap regulatory-domain-profile** command did not work while creating a new regulatory profile. The fix ensures that the **no valid** parameter of the **ap regulatory-domain-profile** command works as expected. This issue was observed in controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.6.0.7
AOS-217382	—	VRRP flapping was observed in a few Mobility Masters. This issue occurred when the VRRP master could not send periodic advertisements. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-217539 AOS-219010 AOS-219952 AOS-220918 AOS-221298	—	The **auth** process crashed on managed devices running ArubaOS 8.6.0.6 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.6
AOS-217678 AOS-218131	—	Some APs did not honor the user alias route src-nat ACL and tunneled the traffic to managed devices. The issue occurred when a netdestination alias is configured in the ACL. The fix ensures that the APs work as expected. This issue is observed in APs running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-217703	—	Some managed devices took a long time to boot up after an upgrade. The fix ensures that the managed devices do not take a long time to boot up. This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-218012	—	The **Maintenance** tab of the WebUI displayed a list of clusters that were not configured for that particular node. The fix ensures that the WebUI does not display clusters that are not configured for a particular node. This issue was observed in Mobility Masters running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218070	—	The **auth** process crashed on managed devices running ArubaOS 8.6.0.0 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.0
AOS-218117 AOS-219179	—	The **show ntp servers** and **show ntp status** commands displayed the error message, **Address family for hostname not supported**. However, the WebUI displayed the NTP servers. The fix ensures that the commands do not display the error message. This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-218167	—	Users were unable to delete static OSPF aggregate routes. The fix ensures that the users are able to delete static OSPF aggregate routes. This issue was observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-218208	—	Some clients were unable to connect to APs. The log file listed the reason for the event as, **AP is resource constrained**. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-218231 AOS-216177	—	Wireless users were unable to find a few wired clients. The fix ensures that the wireless users are able to find the wired clients. This issue was observed in controllers running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-218277 AOS-214428	—	The **auth** process crashed on managed devices running ArubaOS 8.5.0.11 or later versions. Hence, the Remote APs rebooted and VIA users faced connectivity issues. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.11
AOS-218328 AOS-220026	—	VRRP flapping was observed on managed devices running ArubaOS 8.6.0.4 or later versions and hence, clients faced connectivity issues. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.4
AOS-218488	—	The management VLAN address of the Mobility Master was pointed to the Remote AP tunnel. The fix ensures that the management VLAN address is not available in the Remote AP tunnel. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-218518 AOS-218880	—	Some managed devices running ArubaOS 8.7.1.0 or later versions crasheed unexpectedly. The log files list the reason for the event as **Reboot reason Datapath timeout (SOS Assert).** The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.0

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218822	—	High flash memory utilization was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.5.0.10
AOS-219008	—	Some UI endpoints like API page and spectrum page displayed information even before authentication. This issue was observed when the API request came over port 443. The fix ensures that the managed devices work as expected.	ArubaOS 8.8.0.0
AOS-219098 AOS-219914	—	Some devices were unable to connect to the network. The fix ensures seamless connectivity. This issue was sobserved in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219328	—	SNMP configurations failed and the error message, **Error: User (itam_net) should be created before adding to the trap host** was displayed. This issue occurred when the SNMP server v3 trap host which had the engine-id same as the engine-id of the controller was removed and added again. The fix ensures that the SNMP configurations do not fail. This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-219365	—	Some APs running ArubaOS 8.7.0.0 or later versions rebooted sporadically. This issue occurred when the smart antenna feature was enabled. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.1
AOS-219390	—	The **datapath** process crashed on stand-alone controllers running ArubaOS 8.7.1.1 or later versions. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. This issue occurred when the op mode of the SSID profile was changed from WPA3-AES-CCM-128 to WPA3-CNSA. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.7.1.1
AOS-219423	—	Honeywell Handheld 60SL0 devices were unable to connect to 802.1X SSIDs. The fix ensures seamless connectivity. This issue was observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-219594	—	The **Logon-Webcc** process crashed on Mobility Masters running ArubaOS 8.7.1.2 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.7.1.2
AOS-219627 AOS-218851	—	Clients were unable to connect to 2.4 GHz SSID of some APs. This issue occurred when the MAC address of the Radio 1 was incorrect. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1

Table 6: *Resolved Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219978 AOS-220568	—	iPhone 12 Pro users experienced poor upstream network performance. This issue occurred when APs operated in tunnel mode. The fix ensures optimal network performance. This issue was observed in APs running ArubaOS 8.6.0.9 or later versions in tunnel mode.	ArubaOS 8.7.1.2
AOS-220996	—	The **switch_daemon** process crashed on Mobility Masters running ArubaOS 8.7.1.3 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.7.1.3
AOS-221018 AOS-220919	—	Some users are unable to connect to SSIDs. This issue occurred in 802.11r and MultiZone enabled configurations. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-221144	—	ARP packets were not forwarded to the uplink switch when bcmc-optimization was enabled on the controllers. This issue was observed in Mobility Masters and managed devices running ArubaOS 8.5.0.9 or later versions. The fix ensures that the Mobility Masters and managed devices work as expected.	ArubaOS 8.5.0.9

Chapter 7
Known Issues in ArubaOS 8.7.1.4

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

Limitation

Following are the limitations observed in this release:

Port-Channel Limitation in 7280 Controllers

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

No Support for Unique Local Address over IPv6 Network

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

Known Issues

Following are the known issues observed in this release:

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** command displays incorrect session count. This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions.	ArubaOS 8.1.0.0
AOS-151355	185602	A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.	ArubaOS 8.0.1.0
AOS-153742 AOS-194948	188871	A stand-alone controller crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in 7010 controllers running ArubaOS 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.5.0.1
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.	ArubaOS 8.4.0.0

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
		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.	
AOS-199545 AOS-212851	—	Some APs report low noise floor after upgrading the cluster to ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-199884	—	Mobility Master logs the following error message, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** This issue is observed in Mobility Masters running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5
AOS-201166 AOS-207939 AOS-209042	—	A controller crashes and reboots unexpectedly when the **HTTPD** process is restarted. The log files list the reason for the event as **Reboot cause: Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c)**. This issue is observed in stand-alone controllers running ArubaOS 8.2.0.0 or later versions.	ArubaOS 8.5.0.2
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-203517 AOS-204709	—	The **Datapath** process crashes on managed devices unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).** This issue occurs when data packets undergo multiple GRE encapsulation. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-203614 AOS-209261	—	The Mobility Master dashboard does not display the number of APs and clients present in the network. This issue is observed in Mobility Masters running ArubaOS 8.6.0.2 or later versions.	ArubaOS 8.6.0.2
AOS-204187	—	The command, **vpn-peer peer-mac** does not support Suite-B cryptography for custom certificates. This issue is observed in Mobility Masters running ArubaOS 8.2.2.8 or later versions.	ArubaOS 8.2.2.8

Table 7: *Known Issues in ArubaOS 8.7.1.4*

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-206765 AOS-208978	—	A few show commands fail to display any output. This issue is observed in managed devices running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
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-206890	—	The **body** field in the **Configuration > Services > Guest Provisioning** page of the WebUI does not allow users to add multiple paragraphs for email messages. This issue is observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206902 AOS-208241	—	AirGroup users are unable to connect to Sonos speakers. This issue is observed in managed devices running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-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

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
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-207691	—	CLI displays incorrect IP address for a TACACS server. This issue is observed in managed devices running ArubaOS 8.3.0.8 or later versions. **Workaround:** Restart the **profmgr** process for CLI to display the correct IP address.	ArubaOS 8.3.0.8
AOS-207692	—	Some managed devices running ArubaOS 8.6.0.4 or later versions log multiple authentication error messages.	ArubaOS 8.6.0.4
AOS-208420	—	Users are unable to log in to CLI of a controller. This issue occurs when the password has special characters, < and/or >. This issue is observed in controllers running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.5
AOS-208597	—	The **show ap mesh monitor stats** command returns 0 for output. This issue is observed in Mobility Masters running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
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
AOS-209276	—	The **show datapath crypto counters** command displays the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. This issue is observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-209879 AOS-220470	—	The **trusted vlan add** command removes all the existing trusted VLANs. This issue is observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-209936 AOS-215097	—	Mobility Masters running ArubaOS 8.6.0.6 or later versions display some BSSIDs as rouge BSSIDs even after manually white-listing the BSSIDs.	ArubaOS 8.6.0.6
AOS-209977	—	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

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-210416 AOS-210480	—	The **show ap client trail-info** command displays incorrect **VLAN(s)** values. This issue is observed in Mobility Masters running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-210482	—	Some managed devices running ArubaOS 8.3.0.6 or later versions display the error message, **Invalid set request** while configuring ESSID for a Beacon Report Request profile.	ArubaOS 8.3.0.6
AOS-210490	—	Some managed devices running ArubaOS 8.5.0.8 or later versions display the error message, **Error: Tunnel is part of a tunnel-group** while deleting a L2 GRE tunnel which is not a part of any tunnel group.	ArubaOS 8.5.0.8
AOS-210638	—	The **ARM** process crashes on managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-211658	—	A few clients are unable to connect to AP-535 access points running ArubaOS 8.6.0.5 or later versions in a cluster setup. This issue occurs when WMM and HT configurations are enabled.	ArubaOS 8.6.0.5
AOS-211720	—	The **STM** process crashes on managed devices and hence, APs failover to another cluster. This issue is observed in managed devices running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5
AOS-211863	—	Some APs do not come up on managed devices. This issue occurs when the forwarding mode is changed to bridge mode. the name of the ACL reaches the maximum size of 64 bytes. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212038	—	The **show memory <process-name>** command does not display information related to the **dpagent** process. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212255	—	Some APs are stuck in **Not in Progress** state during cluster live upgrade. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-212310 AOS-219441	—	**WebCC** and **NTPd** processes are in busy state in stand-alone controllers running ArubaOS 8.5.0.12 or later versions. This issue occurs when a DNS server or an NTP Server is unreachable.	ArubaOS 8.5.0.12
AOS-212591	—	Some managed devices running ArubaOS 8.7.1.0 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**.	ArubaOS 8.7.1.0

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212605 AOS-218721	—	Some APs running ArubaOS 8.6.0.9 or later versions crashes unexpectedly. The log files list the reason for the event as **wlc_key_get_info+0x4/0x60 [wl_v6]**.	ArubaOS 8.7.1.1
AOS-215461 AOS-220709	—	Database synchronization fails between standby and stand-alone controllers running ArubaOS 8.6.0.9 or later versions. The log files list the reason for the event as **Standby switch did not acknowledge the WMS database restore request**.	ArubaOS 8.6.0.9
AOS-215852	—	Mobility Masters running ArubaOS 8.6.0.6 or later versions log the error message, **ofa: 07765|ofproto|INFO|Aruba-SDN: 1 flow_mods 28 s ago (1 modifications).** This issue occurs when openflow is enabled and when 35 seconds is configured as UCC session idle timeout.	ArubaOS 8.6.0.6
AOS-216133	—	Clients are unable to connect to APs on A-band channels. This issue is observed in APs running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-216512	—	The DHCP client / station related AMON message sends the mask, server IP address, and client IP address in a reverse order to the AirWave server. This issue is observed in Mobility Masters running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-216622	—	A few APs incorrectly display the restricted flag, **p = Restriction mode in POE-AF/AT** in the AP database even if the Ethernet port is disabled. This issue is observed in APs running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-216764	—	Users are not redirected to the captive portal page. This issue is observed in managed devices running ArubaOS 8.7.1.0 or later versions in a cluster setup.	ArubaOS 8.7.1.0
AOS-216766	—	Some APs generate sapd coredump. This issue is observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-217807	—	Remote APs take a long time to come up on a managed device. This issue occurs due to a delay in whitelist-db synchronization between the Mobility Master and managed devices, and when external authentication is enabled for Remote APs. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions in a cluster setup.	ArubaOS 8.6.0.5
AOS-218162	—	The wired Ethernet port does not form GRE tunnel with the managed device. This issue is observed in managed devices running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218254 AOS-218875	—	Some managed devices running ArubaOS 8.7.1.0 or later versions crashes unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2).**	ArubaOS 8.7.1.0
AOS-218404 AOS-212330	—	Some APs are unable to ping a few clients. This issue is observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-218621	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **AP Reboot reason: BadAddr:6c0094119461 PC:wlc_ampdu_recv_ addba_resp+0x240/0x838 [wl_v6] Warm-reset**.	ArubaOS 8.7.1.1
AOS-218622	—	Some APs running ArubaOS 8.6.0.6 or later versions crashes unexpectedly. The log files list the reason for the event as **PC:aruba_wlc_ratesel_ getcurrate+0x24/0xd0 [wl_v6] Warm-reset**.	ArubaOS 8.7.1.1
AOS-218646	—	Ascom i63 phones connected to AP-515 access points running ArubaOS 8.6.0.7 or later versions experience degraded audio quality.	ArubaOS 8.6.0.7
AOS-218795	—	Downloadable user roles are not downloaded and hence, user roles are not assigned to the tunnel-node users. This issue is observed in managed devices running ArubaOS 8.7.1.2 or later versions.	ArubaOS 8.7.1.2
AOS-219034	—	Clients connecting to HT-enabled SSIDs connect as non-HT clients. This issue is observed in APs running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-219112	—	UBT clients hop between VLANs. This issue is observed in managed devices running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219178	—	Clients connecting to the anchor controller are unable to receive IP addresses. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-219214	—	The validuser acl list gets reordered in stand-alone controllers running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-219379	—	Some Mobility Controllers are unable to connect to Mobility Controller Virtual Appliance. 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 Mobility Controllers running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219383	—	The **Configuration > License > License Usage** tab does not display the license details. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.12 or later versions.	ArubaOS 8.5.0.12
AOS-219384	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **PC is at wlc_nar_dotxstatus+0x450**.	ArubaOS 8.7.1.1
AOS-219725	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **PC is at wlc_nar_detach+0x8c**.	ArubaOS 8.7.1.1
AOS-219936	—	The stand-alone controller displays 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-220108	—	The **OFA** process crashes on Mobility Master Virtual Appliances running ArubaOS 8.6.0.6 or later versions. This issue occurs when the **show openflow debug ports** command is executed.	ArubaOS 8.6.0.6
AOS-220183	—	The user table does not list the PUTN users and the error message, **Dropping bridge miss rcvd for dormant PUTN user** is displayed. This issue is observed in managed devices running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-220293	—	Some APs running ArubaOS 8.7.1.1 or later versions crash unexpectedly. The log files list the reason for the event as **aruba_wlc_ratesel_getmaxrate+0x34**.	ArubaOS 8.7.1.1
AOS-220398	—	A few clients in bridge mode are unable to connect to WPA2-PSK SSIDs. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-220552	—	The **Configuration > Services > Clusters** page of the WebUI does not display the status of live upgrade. This issue occurs when the cluster profile name has a blank spaces. This issue is observed in Mobility Masters running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-221005	—	Some stand-alone controllers running ArubaOS 8.7.1.2 or later versions are stuck in reboot loop. The log files list the reason for the event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**.	ArubaOS 8.7.1.2
AOS-221225	—	AP-387 access points running ArubaOS 8.7.1.1 or later versions reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**.	ArubaOS 8.7.1.1

Table 7: *Known Issues in ArubaOS 8.7.1.4*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-221352	—	Some mesh links report incorrect RSSI values. This issue is observed in APs running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-221478 AOS-221569 AOS-221572	—	The **auth** process crashes on managed devices running ArubaOS 8.5.0.9 or later versions. This issue occurs when the **show auth-tracebuf mac** command is executed.	ArubaOS 8.5.0.9
AOS-221507	—	Some AP-515 access points running ArubaOS 8.7.1.3 or later versions crashes unexpectedly. The log files list the reason for the event as **BadAddr:ffffffc12c30ca80 PC:__alloc_ skb+0x110/0x1c8 Warm-reset**.	ArubaOS 8.7.1.3

Chapter 8
Upgrade Procedure

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

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

Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device?
  - Are all managed devices running the same version of ArubaOS?
  - What services are used on your managed device (employee wireless, guest access, Remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load ArubaOS images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Aruba Mobility Master Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Master, or two versions lower. For example multiversion is supported if a Mobility Master is running ArubaOS 8.5.0.0 and the managed devices are running ArubaOS 8.5.0.0, ArubaOS 8.4.0.0, or ArubaOS 8.3.0.0.

Memory Requirements

All Aruba managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. Following are best practices for memory management:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 34 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 34 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 34 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 34.

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

In the WebUI

The following steps describe how to upgrade ArubaOS from a TFTP server, FTP server, or local file.

1. Download the ArubaOS image from the customer support site.
2. Upload the ArubaOS image to a PC or workstation on your network.
3. Validate the SHA hash for the ArubaOS image:
   a. Download the **Aruba.sha256** file from the download directory.
   b. Load the ArubaOS image to a Linux system and execute the **sha256sum <filename>** command. Alternatively, use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the customer support site.

The ArubaOS image file is digitally signed and is verified using RSA2048 certificates preloaded at the factory. The Mobility Master or managed device will not load a corrupted ArubaOS image.

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

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

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

In the CLI

The following steps describe how to upgrade ArubaOS from a TFTP server, FTP server, or local file.

1. Download the ArubaOS image from the customer support site.
2. Open an SSH session to your Mobility Master.
3. Execute the **ping** command to verify the network connection between the Mobility Master and the SCP server, FTP server, or TFTP server.

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

or

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

or

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

4. Execute the **show image version** command to check if the ArubaOS image is loaded on the flash partition. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(host) #show image version
```

5. Execute the **copy** command to load the new image to the non-boot partition.

```
(host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

6. Execute the **show image version** command to verify that the new image is loaded.

```
(host)# show image version
```

7. Reboot the Mobility Master.

```
(host)#reload
```

8. Execute the **show version** command to verify that the upgrade is complete.

```
(host)#show version
```

Verifying the ArubaOS Upgrade

Verify the ArubaOS upgrade in the WebUI or CLI.

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 34 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 34 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 34.
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.