ArubaOS 8.6.0.9

a Hewlett Packard
Enterprise company

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

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	The bug, **AOS-220568** has been added to the **Known Issues and Limitations** section.
Revision 01	Initial release.

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

This ArubaOS release notes includes the following topics:

Throughout this document, branch controller and local controller are termed as managed device.

For a list of terms, refer to the Glossary.

Important Point Before Upgrading to ArubaOS 8.6.0.0

Your CPU should support version SSE4.2. For deployments on versions prior to ArubaOS 8.5.0.0, SSSE3 is the minimum supported version. Additionally the CPU should also support Intel VT.

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

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

New Features and Enhancements in ArubaOS 8.6.0.9

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

CLI

show datapath frame debug command

Starting from ArubaOS 8.6.0.9, the output of the **show datapath frame debug** command has been modified to display **vlan bcmc drop frames** instead of **vlan bcmc check fails**.

Support for Huawei E3372h-320 modem

Starting from ArubaOS 8.6.0.9, users should issue the **uplink cellular profile e3372h-320** command to provision the Huawei E3372h-320 modem. It is recommended to issue the command, reload and then insert the modem for a successful provisioning.

Supported Platforms in ArubaOS 8.6.0.9

This chapter describes the platforms supported in this release.

Mobility Master Platforms

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

Table 3: *Supported Mobility Master Platforms in ArubaOS 8.6.0.9*

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

Mobility Controller Platforms

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

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.6.0.9*

Mobility Controller Family	Mobility Controller Model
7000 Series Hardware Mobility Controllers	7005, 7008, 7010, 7024, 7030
7200 Series Hardware Mobility Controllers	7205, 7210, 7220, 7240, 7240XM, 7280
9000 Series Hardware Mobility Controllers	9004
MC-VA-xxx Virtual Mobility Controllers	MC-VA-10, MC-VA-50, MC-VA-250, MC-VA-1K, MC-VA 4K, MC-VA 6K

MC-VA-4K and MC-VA-6K are not orderable SKUs. However, you can scale up by installing multiple instances of MC-VA-1K. For example to deploy 4K APs on a single Mobility Controller Virtual Appliance, you need to add four MC-VA-1K licenses.

AP Platforms

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

Table 5: *Supported AP Platforms in ArubaOS 8.6.0.9*

AP Family	AP Model
100 Series	AP-104, AP-105
103 Series	AP-103
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135
170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1
200 Series	AP-204, AP-205
203H Series	AP-203H
205H Series	AP-205H
207 Series	AP-207
203R Series	AP-203R, AP-203RP
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277

Table 5: *Supported AP Platforms in ArubaOS 8.6.0.9*

AP Family	AP Model
300 Series	AP-304, AP-305
303 Series	AP-303, AP-303P
303H Series	AP-303H
310 Series	AP-314, AP-315
318 Series	AP-318
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377
AP-387	AP-387
500 Series	AP-504, AP-505
510 Series	AP-514, AP-515
530 Series	AP-534, AP-535
550 Series	AP-555
RAP 3 Series	RAP-3WN, RAP-3WNP
RAP 100 Series	RAP-108, RAP-109
RAP 155 Series	RAP-155, RAP-155P

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 asp.arubanetworks.com.

Regulatory Updates in ArubaOS 8.6.0.9

The following DRT file version is part of this release:

- DRT-1.0_79703

Resolved Issues in ArubaOS 8.6.0.9

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-192364	The output of the **show ap database** command displayed the **Switch role changed; reload required.** error message. This issue was observed after a reboot of the **CFGM** process in Mobility Masters running ArubaOS 8.6.0.0 or later versions. The fix ensures that the **show ap database** command displays the correct output.	ArubaOS 8.6.0.0
AOS-195526	Some clients were unable to get DHCP addresses. This issue occurred when ACE entries of the logon role ACL was changed to **Deny all** when the PEFNG feature was disabled. The fix ensures that the clients are able to receive DHCP addresses. This issue was observed in managed devices running ArubaOS 8.3.0.8 or later versions.	ArubaOS 8.3.0.8
AOS-196399	DDS traffic caused IP reassembly failures in datapath. The fix ensures that the Mobility Master works as expected. This issue is observed in Mobility Masters running ArubaOS 8.3.0.6 or later versions.	ArubaOS 8.3.0.6
AOS-197548 AOS-209545	MAC authentication was not initialized when IPv6 was globally disabled. The fix ensures that MAC authentication works as expected. This issue was observed in managed devices running ArubaOS 8.3.0.13 or later versions.	ArubaOS 8.3.0.13
AOS-201003 AOS-212135	Some Remote APs were unable to come up in a cluster. The fix ensures that Remote APs can come up in a cluster. This issue is observed in managed devices running ArubaOS 8.0.2.0 or later versions.	ArubaOS 8.0.2.0
AOS-201233 AOS-214547	The **Dashboard > Overview > Clients** page in **Managed Network** node hierarchy of the WebUI displayed an incorrect client bandwidth. The fix ensures that the WebUI displays the correct bandwidth. This issue was observed in Mobility Masters running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-202497 AOS-212608	Some APs running ArubaOS 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as, **Kernel panic: PC is at wlc_apps_psp_resp_complete+0x24**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.5
AOS-203926 AOS-217462 AOS-217578	Voice traffic using NOE protocol was not getting tunneled in split-tunnel forwarding mode. This issue occurred when openflow was enabled. The fix ensures that the voice traffic is tunneled in split-tunnel forwarding mode. This issue is observed in managed devices running ArubaOS 8.6.0.3 or later versions.	ArubaOS 8.6.0.3

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-206355	LLDP process crashed during ZTP in managed devices running ArubaOS 8.2.2.6 and later versions. This issue occurred due to memory corruption. The fix ensures that the managed devices work as expected.	ArubaOS 8.2.2.6
AOS-206801	A managed device running ArubaOS 8.2.2.3 or later versions contacted the Activate server more than once during ZTP. The fix ensures that the managed device work as expected. This issue was observed in managed devices running ArubaOS 8.2.2.3 or later versions.	ArubaOS 8.2.2.3
AOS-207664 AOS-213842	The login banner text was not displayed after upgrading the managed device to ArubaOS 8.5.0.0 or later versions. The fix ensures that the login banner is displayed.	ArubaOS 8.5.0.0
AOS-207795	Users were unable to access the WebUI of the Mobility Master. The fix ensures that users are able to access the WebUI. This issue was observed in Mobility Masters running ArubaOS 8.2.2.6 or later versions.	ArubaOS 8.2.2.6
AOS-208337 AOS-209348 AOS-212655 AOS-213442	The **airmatch_recv** process crashed on Mobility Controller Virtual Appliances running ArubaOS 8.5.0.7 or later versions. The fix ensures that the Mobility Controller Virtual Appliances work as expected.	ArubaOS 8.5.0.7
AOS-208515	The radio usage graph in AirWave got reset to zero. This issue occurred while downloading large files. The fix ensures that the radio usage graph does not reset to zero. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-209069	The control plane security configuration, **auto-cert-allowed-addrs** pushed from a Mobility Master to the managed devices was not visible in the **Configuration > System > CPSec** page of the WebUI. The fix ensures that the control plane security configuration, **auto-cert-allowed-addrs** is visible in the WebUI. This issue is observed in managed devices running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-209127	Internal server timeout was observed during an authentication request. The fix ensures successful authentication. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-209196 AOS-213746	Some AP-345 access points running ArubaOS 8.5.0.8 or later versions rebooted unexpectedly. The issue occurred due to memory leak when tunnel forwarding mode, dot11k, and WPA3 were enabled. The fix ensures that the APs work as expected.	ArubaOS 8.5.0.8
AOS-209352	Some managed devices terminating VIA connection displayed the error message, **httpd[30106]: Reached session limit: 64**. The fix ensures that all VPNC and VIA sessions are considered during session count. This issue was observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-209402	A few clients experienced dot1X timeout in split tunnel mode. This issue occurred when multiple wired clients were connected to an AP. The fix ensures that the clients don't experience a timeout. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-209748 AOS-215172 AOS-217181	Some users were unable to make configuration changes to the existing RADIUS server profile at the device level. The log file listed the reason for the event as **Reference retrieval error**. The fix ensures that profmgr process does not get stuck if it's unable to retrieve a profile reference and the devices work as expected. This issue was observed in Mobility Masterrunning ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-210273 AOS-217372	Some managed devices running ArubaOS 8.6.0.7 or later versions logged the message, **<INFO> |dot1x-proc:1| Sending a request for Switch IP6** repeatedly even when there are no IPv6 configurations in the network. The fix ensures that the managed devices send **Switch IPv6** request only for 60 times and this avoids repeated printing of log messages.	ArubaOS 8.6.0.7
AOS-210342	The VRRP authentication password was not encrypted in the output of the **show running config** command. The fix ensures that the VRRP authentication password is encrypted. This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-210404	The **Pending Changes** option did not appear in the WebUI. This issue occurred when there were too many unsaved nodes and the **show configuration unsaved-nodes** command had on output of more than 1024 characters. The fix ensures that the **Pending Changes** option appears in the WebUI. This issue was observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-210481	The **Dashboard > Infrastructure > Clusters** page of the WebUI did not list all the clusters. The fix ensures that the WebUI displays the list of all clusters. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-210484	Some managed devices running ArubaOS 8.0.0.0 or later versions do not display the 802.11k measurements from clients. The fix ensures that the managed devices display the 802.11k measurements from clients.	ArubaOS 8.3.0.6
AOS-210845 AOS-217214 AOS-217871	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.	ArubaOS 8.6.0.6
AOS-210896	Hotspot 2.0 IEs were not present in beacons frames. The fix ensures that the Hotspot 2.0 IEs are present beacons frames. This issue was observed in APs running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-211256	The SFP J8177D, JD089B, and Cisco GLC-TE transceivers did not work with 7205 controllers running ArubaOS 8.6.0.3. The fix ensures that the SFP J8177D, JD089B, and Cisco GLC-TE transceivers work with 7205 controllers.	ArubaOS 8.6.0.3

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-211324	Some iPads were unable to connect to SSIDs. The log file listed the reason for the event as **STA Requesting Association without authentication**. The fix ensures seamless connectivity. This issue was observed in AP-535 access points running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-211389	Users were unable to install evaluation licenses. This issue occurred when the Mobility Master displayed an expired installation date. The fix ensures that the users are able to install evaluation licenses. This issue was observed in Mobility Masters running ArubaOS 8.5.0.4 or later versions.	ArubaOS 8.5.0.4
AOS-211430	The WebUI did not display the list of APs and clients. This issue occurred when VRRP IPv4 / IPv6 dual stack was used to form an IPsec tunnel between the Mobility Master and managed device. The fix ensures that the WebUI displays the list of APs and clients. 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	The **rsync** process was stuck after a boot up and hence, the Mobility Master took a long time to come up. The fix ensures that the timeout of **rsync** process is set to 120 seconds and the Mobility Master functions as expected.	ArubaOS 8.6.0.8
AOS-211448	Some APs running ArubaOS 8.6.0.0 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the reboot as **BadPtr:00000028 PC:anul_aon_buf_release+0x14/0x70 [anul] Warm-reset.** The fix ensures that the APs work as expected.	ArubaOS 8.7.0.0
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-211841	The **Dashboard > Infrastructure** page of the WebUI displayed the client status as **Unknown**. The fix ensures that the WebUI displays the appropriate client status. This issue was observed in managed devices running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-212039	User debug logging information was not available in **Configuration > System > Logging > Logging Levels** page of the WebUI. The fix ensures that the WebUI displays the user debug logging information . This issue was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-212063 AOS-216153	Licenses got installed with incorrect dates in Mobility Masters running ArubaOS 8.5.0.10 or later versions. The fix ensures that licenses are installed using correct dates.	ArubaOS 8.5.0.10
AOS-212123	The SNMP trap **wlsxNUserAuthenticationFailed** was not generated upon failed authentication in a termination-enabled dot1X configuration. The fix ensures that the SNMP trap is generated upon a failed authentication. This issue occurred in stand-alone controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.3.0.0

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-212203 AOS-213878 AOS-213879 AOS-212560	Some users experienced poor network performance. This issue occurred due to 2.4G beacon power fluctuations in AP-505 access points running ArubaOS 8.6.0.5 or later versions. The fix ensures optimal network performance.	ArubaOS 8.6.0.5
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-212458 AOS-215059	Some AP-535 and AP-555 access points running ArubaOS 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **NOC_error.c:476 NOCError: FATAL ERRORparam0 :zero, param1 :zero, param2 :zero**. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.5
AOS-212486 AOS-216471	L2TP IP address leak was observed and the VLAN pool was exhausted. 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
AOS-212568	The **aaa / certmgr / cpsec** security categories in the **Configuration > System > Logging > Logging Levels** page of the WebUI displayed **None** even if values were configured. The fix ensures that the WebUI displays the correct **aaa / certmgr / cpsec** values. This issue was observed in Mobility Masters running all ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.3.0.13
AOS-212576	Some APs running ArubaOS 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: rcu_sched detected stalls (pc is at __schedule+0x78/0x360).** The fix ensures that the APs work as expected.	ArubaOS 8.6.0.5
AOS-212599 AOS-211699 AOS-212564 AOS-212567 AOS-215978 AOS-217452	Some APs running ArubaOS 8.6.0.5 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: jiffies stall (pc is at __schedule+0x78/0x360).** The fix ensures that the APs work as expected.	ArubaOS 8.6.0.5
AOS-212656 AOS-212696 AOS-215107	The custom captive portal page did not load completely. This issue occurred when the **use http authentication option** was enabled. The fix ensures that the captive portal works as expected. This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-212686	Some APs sent higher SAP MTU frames than the configured value. The fix ensures that APs work as expected. This issue was observed in APs running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-212707	Some Mobility Masters running ArubaOS 8.5.0.10 logged the error message, **Fri Oct 16 23:58:53 2020, 0, 0, 0, 0, 0, 0, 0**. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.5.0.10

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-212843	Some users were randomly assigned the default role. This issue occurred when 802.11r feature was enabled. The fix ensures that users are not assigned incorrect roles. This issue was observed in managed devices running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-212861 AOS-215350 AOS-215522 AOS-216305	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.** The fix ensures that the APs work as expected.	ArubaOS 8.6.0.6
AOS-212885 AOS-214735	Some AP-345 access points running ArubaOS 8.7.1.0 or later versions rebooted unexpectedly. The log file listed the reason for the event as, **BUG in aruba_wlc.c:4527/aruba_radio_update()**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.0
AOS-212980	The **show datapath session dpi counters** table did not display any output. The fix ensures that the command works as expected. This issue was observed in Mobility Masters running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
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-213089	Some managed devices running ArubaOS 8.3.0.0 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:f0:2)**. The fix ensures that the managed devices work as expected. **Duplicates:** AOS-213044, AOS-213295, AOS-214238, AOS-214431, AOS-214678, AOS-215123, AOS-215572, AOS-216951, AOS-217734	ArubaOS 8.3.0.0
AOS-213099	The **dpagent** process crashed on managed devices running ArubaOS 8.5.0.10 or later versions. The fix ensures that the managed devices work as expected. **Duplicates:** AOS-214123, AOS-215367, AOS-216451, AOS-216612, AOS-217647, AOS-217960, AOS-217721, AOS-217942, AOS-217943, AOS-218204	ArubaOS 8.5.0.10
AOS-213132 AOS-216300	Users were unable to upload server certificates in PEM or DER format. The fix ensures that users are able to upload server certificates. This issue is observed in Mobility Masters running ArubaOS 8.6.0.6-FIPS.	ArubaOS 8.6.0.6-FIPS
AOS-213242 AOS-215607 AOS-218659	High noise level and channel utilization were observed on AP-535 and AP-555 access points running ArubaOS 8.6.0.6 or later versions. This issue occurred in channels operating in 2.4 Ghz mode. The fix ensures that the APs work as expected.	ArubaOS 8.6.0.6

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-213558	Users were unable to add a new node to an existing cluster of eight nodes. The fix ensures that users are able to add new nodes. This issue was observed in managed devices running ArubaOS 8.5.0.6 or later versions.	ArubaOS 8.5.0.6
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.	ArubaOS 8.6.0.5
AOS-213865	The WebUI displayed the message, **one or more settings have been overridden at bottling** and displays the older folder name after an override. The fix ensures that the WebUI does not displays the older folder name. This issue was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-214255	Older 802.11b clients were unable to connect to a few APs. This issue occurred when VAPs on 2.4 GHz radio were configured with different basic rates and when few VAPs did not include 802.11b CCK rates. The fix ensures seamless connectivity. This issue was observed in AP-203R, AP-203RP, AP-203H, and AP-207 access points running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-214261	Some clients experienced connectivity issues while roaming. The fix ensures seamless connectivity. This issue was observed in AP-535 access points running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
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-214714	A few stand-alone controllers running ArubaOS 8.5.0.11 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.5.0.11
AOS-214835 AOS-218512	Some wireless clients connected to APs experienced slow network speed. Enhancements to the driver resolved the issue. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-215022	Clients authenticated using wpa3-sae-aes with MAC authentication were disconnected from the network. This issue occurred when a 4-way handshake was not initiated. The fix ensures that clients are not disconnected from the network. This issue was observed in managed devices running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
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

Table 6: *Resolved Issues in ArubaOS 8.6.0.9*

Bug ID	Description	Reported Version
AOS-215641 AOS-215642 AOS-217268 AOS-217362 AOS-217640	The **ISAKMPD** process crashed on managed devices running ArubaOS 8.6.0.0 or later versions in a PSK-RAP setup. The fix ensures that the managed devices work as expected.	ArubaOS 8.7.1.1
AOS-216204	Some AP-535 access points running ArubaOS 8.5.0.10 or later versions crashed unexpectedly. The log file listed the reason for the event as, **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**.The fix ensures that the APs work as expected.	ArubaOS 8.5.0.10
AOS-216281	Some APs did not display any information related to crash. This issue occurred when the APs crashed twice. The fix ensures that the APs displays information related to crash and APs work as expected. This issue was observed in APs running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.7.1.1
AOS-217035	A few APs were down and were unable to connect to the managed device. This issue occurred when UDP traffic was sent without establishing IPsec tunnels. The fix ensures that APs are able to connect to the managed device. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.6.0.7

Known Issues and Limitations in ArubaOS 8.6.0.9

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

Limitation

Following are the limitations observed in this release:

Port-Channel Limitation in 7280 Controllers

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

No Support for Unique Local Address over IPv6 Network

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

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in ArubaOS 8.6.0.9*

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

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-155404 AOS-207878	191106	An AP is unable to establish IKE/IPsec tunnel with the managed device. This issue occurs when the AP is enrolled with EST certificates. This issue is observed in AP-515 access points running ArubaOS 8.5.0.0 or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.6.0.4
AOS-156068	192100	The **DDS** process in a managed device running ArubaOS 8.2.1.1 or later versions crashes unexpectedly.	ArubaOS 8.2.1.1
AOS-182847	—	A few users are unable to copy the **WPA Passphrase** field and **High-throughput** profile to a new SSID profile in the **Configuration > System > Profiles > Wireless LAN > SSID > <SSID_Profile>** option of the WebUI. This issue occurs when a new SSID profile is created from an existing SSID profile using WebUI. This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.4.0.0
AOS-183706	—	The TX radio power of a few APs are lesser than the TX radio power of other APs in the same network. This issue is observed in APs running ArubaOS 8.3.0.6 or later versions.	ArubaOS 8.3.0.6
AOS-184947 AOS-192737	—	The jitter and health score data are missing from the **Dashboard > Infrastructure > Uplink > Health** page in the WebUI. This issue is observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions.	ArubaOS 8.4.0.4
AOS-185538 AOS-195334	—	High number of EAP-TLS timeouts are observed in a managed device. This issue occurs when multiple IP addresses are assigned to each client. This issue is observed in managed devices running ArubaOS 8.3.0.8 or later versions.	ArubaOS 8.3.0.8
AOS-187395 AOS-188564	—	The AAA test to the external server fails when executed from the **Diagnostics > Tools > AAA Server Test** page of the WebUI. This issue occurs when the user enters the ", %, and # special characters in the **Password** field and clicks the **Test** option. As a result, the WebUI displays the **Authentication** field as **failed** and **Processing time (ms)** field as **N/A.** This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-188972 AOS-194746 AOS-208631 AOS-213627	—	Mobility Master displays the blacklisted clients although the clients were removed from the managed device. This issue is observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions in a cluster setup.	ArubaOS 8.4.0.4

Table 7: *Known Issues in ArubaOS 8.6.0.9*

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

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-194911	—	Incorrect flag output is displayed for APs configured with 802.1X authentication when the **show ap database** command is executed. This issue is observed in APs running ArubaOS 8.5.0.2 or later versions.	ArubaOS 8.5.0.2
AOS-194964	—	A few users are unable to clone configuration from an existing group to a new group in a Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.4.0.1 or later versions. **Workaround:** Execute the **rf dot11a-radio-profile <profile name>** command to change the operating mode of the AP from am-mode to ap-mode.	ArubaOS 8.5.0.2
AOS-195089	—	The DNS traffic is incorrectly getting classified as **Thunder** and is getting blocked. This issue occurs when the DNS traffic is blocked and peer-peer ACL is denied for users. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-195100 AOS-198302 AOS-204455 AOS-206735	—	The health status of a managed device is incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master's WebUI. This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-195177	—	Some managed devices frequently generate internal system error logs. This issue occurs when the **sapd** process reads a non-existent interface. This issue is observed in 7220 controllers running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-195434	—	An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is observed in APs running ArubaOS 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.5.0.2
AOS-196457	—	High radio noise floor is observed on APs. This issue is observed in AP-515 access points running ArubaOS 8.5.0.2 or later versions.	ArubaOS 8.5.0.2
AOS-196864	—	Although a new VLAN ID is successfully connected, the managed device displays that the VLAN ID fails with a different ID. This issue is observed when new VLANs are added and the total number of VLANs are 100/101, 200/201, 300/301 and so on. This issue is observed in managed devices running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-196878 AOS-197216	—	The **Datapath** process crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.** This issue is observed in managed devices running ArubaOS 8.5.0.2 or later versions.	ArubaOS 8.5.0.2

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-197023	—	Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions. **Workaround:** The following are recommended: ■ In the CLI, execute the **ap regulatory-domain-profile** command to create an AP regulatory-domain- profile without any channel configuration, save the changes, and later add or delete channels as desired. ■ In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes, and later add or delete channels as desired in the **Configuration > AP Groups** page.	ArubaOS 8.5.0.4
AOS-197323 AOS-212920	—	The **Dashboard > Infrastructure** page of the WebUI does not display the static channel details assigned to an AP. This issue is observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-197497	—	AirMatch selects the same channel for two neighboring APs even after radar detection. This issue is observed in managed devices running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-197812	—	A mismatch of user roles is observed in the WebUI and CLI of the Mobility Master and managed device. This issue occurs when UDR is configured to assign user roles to clients. This issue is observed in Mobility Masters and managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-198024	—	Users are unable to access any page after the fifth page using the **Maintenance > Access Point** page in the WebUI. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-198281	—	The details of the **Up** time in **Managed network > Dashboard > Access Points > Access Points** table does not get updated correctly. This issue is observed in Mobility Masters running ArubaOS 8.2.2.6 or later versions.	ArubaOS 8.2.2.6
AOS-198483	—	WebUI does not have an option to map the **rf dot11-60GHz-radio-profile** to an AP group. This issue is observed in Mobility Masters running ArubaOS 8.5.0.4 or later versions.	ArubaOS 8.5.0.4
AOS-198849 AOS-198850	—	Users are unable to configure 2.4 GHz radio profile in the **Configuration > System > Profiles > 2.4 GHz radio profile** page and the WebUI displays an error message, **Feature is not enabled in the license.** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-198991	—	Users are unable to add a VLAN to an existing trunk port using the **Configuration > Interfaces > VLANs** page of the WebUI. This issue is observed in Mobility Masters running ArubaOS 8.6.0.1 or later versions.	ArubaOS 8.6.0.2
AOS-199492	—	Some APs do not get displayed in the **show airgroup aps** command output and the auto-associate policy stops working as expected. This issue occurs when the AirGroup domain is in distributed mode and is not validated in a cluster deployment. This issue is observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-200733 AOS-209999	—	Some APs running ArubaOS 8.5.0.3 or later versions crash and reboot unexpectedly. The log file list the reason for the event as **kernel page fault at virtual address 00005654, epc == c0bd7dd4, ra == c0bf95f8.**	ArubaOS 8.5.0.3
AOS-200765	—	Some managed devices running ArubaOS 8.3.0.7 or later versions in a cluster setup log the error message, **<199804> <4844> |authmgr| |cluster| gsm_auth.c, auth_gsm_publish_ip_user_local_section:1011: auth_gsm_publish_ip_user_local_section: ip_user_local_flags.**	ArubaOS 8.3.0.7
AOS-200781 AOS-210273	—	Some managed devices log the error message, **INFO> |dot1x-proc:1| Sending request for Switch IP6** although there are no IPv6 configurations in the network. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-201042	—	A large number of packet drops are observed in a few APs running ArubaOS 8.3.0.6 or later versions. This issue occurs when the AP SAP MTU datapath tunnel is set to 1514.	ArubaOS 8.3.0.6
AOS-201376	—	The measured power, **Meas. Pow** column in the **show ap debug ble-table** command does not get updated when the TX power of an AP is changed. This issue is observed in APs running ArubaOS 8.5.0.6 or later versions.	ArubaOS 8.5.0.6
AOS-201439 AOS-201448	—	Some AP-303H access points running ArubaOS 8.5.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**.	ArubaOS 8.5.0.5
AOS-202129 AOS-204127	—	The **Configuration > AP groups** page does not have the **Split radio** toggle button to enable the tri-radio feature. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.0
AOS-202210 AOS-218532	—	The **show iap table** and **show iap table long** commands do not display list of Instant APs. This issue is observed in controllers running ArubaOS 8.6.0.6 or later versions in a VPNC deployment.	ArubaOS 8.6.0.6
AOS-202426 AOS-203652	—	Some 510 Series access points running ArubaOS 8.6.0.4 crash and reboot unexpectedly. The log files lists the reason for the event as **PC is at: wlc_phy_enable_hwaci_28nm+0x938 - undefined instruction: 0 [#1]**.	ArubaOS 8.6.0.4
AOS-203077 AOS-203232	—	Configurations committed using the **firewall cp** command are not synchronized on the standby Mobility Master. This issue occurs when static firewall entries are deleted. 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 goes down and the error message, **Failed to create internal-iap IP user entry and user entry due to too many user entries 128** is displayed. This issue occurs when the user table has 128 entries. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-203201	—	A managed device is unable to download configurations from the Mobility Master using VPNC. This issue is observed in managed devices running ArubaOS 8.2.2.6 or later versions.	ArubaOS 8.2.2.6
AOS-203336	—	The **Dashboard > Infrastructure > Access Points** page of the WebUI and the **show log** command display different values for the last AP reboot time. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5
AOS-203438	—	The configuration for EIRP made using the WebUI is not visible in stand-alone controllers running ArubaOS 8.6.0.3 or later versions.	ArubaOS 8.6.0.3
AOS-203517 AOS-204709 AOS-213765	—	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-203910 AOS-209692	—	The stand-alone controllers running ArubaOS 8.6.0.3 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:0:2c)**.	ArubaOS 8.6.0.3
AOS-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
AOS-204241	—	Managed devices log spurious DHCP DBUG messages. This issue is observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-204414	—	The VLAN range configured using the **ntp-standalone vlan-range** command is not correctly sent to the managed devices. This issue occurs when the user repeatedly modifies the VLAN range. This issue occurs in Mobility Masters running ArubaOS 8.0.1.0 or later versions. **Workaround:** Delete the VLAN range configured on the Mobility Master and re-configure the **ntp-standlaone vlan-range.**	ArubaOS 8.3.0.8
AOS-204892	—	The upgrade of ArubaOS controllers is delayed due to slow uplink speed. This issue is observed in stand-alone controllers running ArubaOS 8.2.0.0 or later versions.	ArubaOS 8.2.0.0

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-205319 AOS-206993 AOS-216577 AOS-218524	—	Some APs running ArubaOS 8.6.0.5 or later versions crash and reboot unexpectedly. The log file listed the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**.	ArubaOS 8.6.0.5
AOS-206178	—	System logs do not display the reason why an AP has shut down. This issue is observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206537	—	The **H** flag indicating standby tunnel is not displayed in the output of the **show datapath tunnel-table** command and this results in a network loop. This issue is observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206541	—	The **Maintenance > Software Management** page does not display the list of all managed devices that are a part of a cluster. This issue is observed in Mobility Masters running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-206752	—	The console log of 7205 controllers running ArubaOS 8.5.0.9 or later versions displays the **ofald| |sdn| ERRS ofconn_rx:476 <10.50.1.26:6633> socket read failed, err:Resource temporarily unavailable(11)** message.	ArubaOS 8.5.0.9
AOS-206795	—	A user is unable to rename a node from the Mobility Master node hierarchy. This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions. **Workaround:** Restart **profmgr** process to rename the node.	ArubaOS 8.3.0.7
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-206907	—	Some AP-303H access points running ArubaOS 8.5.0.5 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: assert**.	ArubaOS 8.5.0.5
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 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-207337	—	After upgrading from ArubaOS 8.2.x.x to ArubaOS 8.5.0.0- FIPS or later versions, a few managed devices are stuck in the **LAST SNAPSHOT** state. This issue is observed in managed devices running ArubaOS 8.5.0.0 or later versions.	ArubaOS 8.5.0.9
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 occurred when the **configuration purge-pending-config** command was executed on group nodes. This issue is observed in managed devices running ArubaOS 8.3.0.8 or later versions. **Workaround:** Restart the **profmgr** process by issuing the **process restart profmgr** command 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-207775 AOS-215946		The **auth** process crashes on managed devices running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-208337 AOS-209348 AOS-212655 AOS-213442	—	The **airmatch_recv** process crashes on Mobility Controller Virtual Appliances running ArubaOS 8.5.0.7 or later versions.	ArubaOS 8.5.0.7
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-208740 AOS-213754	—	The **profmgr** process crashes on Mobility Masters running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-208846	—	Clients connected to bridge mode SSIDs are unable to receive IP addresses and pass traffic. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-209276	—	The **show datapath crypto counters** command displays the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. This issue is observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-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

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209977	—	SNMP query with an incorrect string fails to record the offending IP address. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-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-210638	—	The **ARM** process crashes on managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-210922	—	The **auth** process crashes on stand-alone controllers and APs reboot unexpectedly. The log file lists the reason for the reboot as **Unable to set up IPSec tunnel, Error:RC_ERROR_IKEV2_TIMEOUT.** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-210992	—	The Mobility Master displays an error message, **Flow Group delete: id not found** after an upgrade. This issue occurs when logging levels are not configured correctly. This issue is observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-211658	—	A few clients are unable to connect to AP-535 access points running ArubaOS 8.6.0.5 or later versions in a cluster setup. This issue occurs when WMM and HT configurations are enabled.	ArubaOS 8.6.0.5
AOS-211730	—	Users are unable to map server certificate as switch certificate on a secondary Mobility Master running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-211863	—	Some APs do not come up on managed devices. This issue occurs when ■ the forwarding mode is changed to bridge mode. ■ the name of the ACL is 64 bytes. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-211878 AOS-214377	—	Some APs fail to come up as Remote APs. This issue occurs when the MTU size is not adjusted automatically. This issue is observed in APs running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212198	—	Some RAP-3WN Remote APs running ArubaOS 8.5.0.8 or later versions reboot unexpectedly. This issue occurs when time between the controller and the Remote AP is not in synchronization. **Workaround:** Reboot the Remote AP.	ArubaOS 8.5.0.8
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

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212530	—	Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as**, reboot Intermittently-suspecting scb or rrm cubby corruption**. This issue was observed in AP-515 access points running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-212935	—	Temporary ACL is still applied to user roles even if the disaster-recovery mode is disabled. This issue occurs when configuration changes in disaster recovery mode are not submitted using the **write memory** command. This issue is observed in managed devices running ArubaOS 8.3.0.6 or later versions. **Workaround:** Ensure to submit the configuration changes made in the disaster-recovery mode.	ArubaOS 8.3.0.6
AOS-213011	—	Packet loss is observed for clients during a cluster failover. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-213115	—	Some managed devices running ArubaOS 8.5.0.10 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first.**	ArubaOS 8.5.0.10
AOS-213307	—	L2 GRE ICMP keepalive response is sent outside the tunnel and hence, gets dropped by the firewall. This issue is observed in managed devices running ArubaOS 8.5.0.1 or later versions.	ArubaOS 8.6.0.6
AOS-214243 AOS-215775	—	A managed device running ArubaOS 8.5.0.0 or later versions 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)**. This issue occurs due to a race condition.	ArubaOS 8.6.0.7
AOS-214391 AOS-217130 AOS-217832	—	STM process crashes on 7240XM controllers running ArubaOS 8.4.0.0 or later versions.	ArubaOS 8.5.0.11
AOS-214434	—	Some APs are unable to come up on a managed device running ArubaOS 8.5.0.8 or later versions. This issue occurs when UDP 8209 traffic is sent without establishing IPsec tunnels.	ArubaOS 8.5.0.8
AOS-214963	—	Some APs running ArubaOS 8.5.0.11 or later versions detect false radar.	ArubaOS 8.5.0.11
AOS-215012 AOS-215567	—	The AP debug counters, **Total Bootstraps** and **Reboots** are not reset after upgrading the managed devices to ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-215021	—	The **Channel Width Capability** configured on AirWave is not available in the **Dashboard > Overview > Wireless Clients** page of the WebUI. This issue is observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6

Table 7: *Known Issues in ArubaOS 8.6.0.9*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-215073	—	Some AP-515 access points running ArubaOS 8.5.0.8 or later versions go down and keeps rebooting.	ArubaOS 8.5.0.8
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-217106	—	The **no valid** parameter of the ap regulatory-domain-profile command does not work while creating a new regulatory profile. This issue is observed in controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** Configure and save an ap regulatory-domain-profile and then issue the **no valid** commands.	ArubaOS 8.6.0.7
AOS-217382	—	VRRP flapping is observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions. This issue occurs when the VRRP master could not send periodic advertisements.	ArubaOS 8.6.0.5
AOS-217439 AOS-216752 AOS-217893	—	The **Impystart** process crashes on Mobility Controller Virtual Appliances running ArubaOS 8.5.0.4 or later versions.	ArubaOS 8.5.0.4
AOS-217678 AOS-218131	—	Some APs do not honour the user alias route src-nat ACL and tunnels the traffic to managed devices. The issue occurs when a netdestination alias is configured in the ACL. 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 running ArubaOS 8.6.0.7 or later versions take a long time to boot up after an upgrade.	ArubaOS 8.6.0.7
AOS-218117	—	The **show ntp servers** and **show ntp status** commands display the error message, **Address family for hostname not supported**. However, the WebUI displays the NTP servers. This issue is observed in managed devices running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-218277 AOS-214428	—	The **auth** process crashes on managed devices running ArubaOS 8.5.0.11 or later versions. Hence, the Remote APs reboot and VIA users face connectivity issues.	ArubaOS 8.5.0.11
AOS-219978 AOS-220568	—	iPhone 12 Pro users experience poor upstream network performance. This issue occurs when APs operate in tunnel mode. This issue is observed in APs running ArubaOS 8.6.0.9 or later versions in tunnel mode. **Workaround:** Disable AMSDU configuration.	ArubaOS 8.7.1.2

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.

Topics in this chapter include:

Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device?
  - Are all managed devices running the same version of ArubaOS?
  - What services are used on your managed device (employee wireless, guest access, Remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.

- If possible, use FTP to load ArubaOS images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Aruba Mobility Master Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Master, or two versions lower. For example multiversion is supported if a Mobility Master is running ArubaOS 8.5.0.0 and the managed devices are running ArubaOS 8.5.0.0, ArubaOS 8.4.0.0, or ArubaOS 8.3.0.0.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 36 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 36 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 36 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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


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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 35.

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

In the WebUI

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

1. Download the ArubaOS image from the customer support site.
2. Upload the ArubaOS image to a PC or workstation on your network.

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

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

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

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

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

In the CLI

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

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

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

or

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

or

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

4. Execute the **show image version** command to check if the ArubaOS image is loaded on the flash partition. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.
   ```
   (host) #show image version
   ```
5. Execute the **copy** command to load the new image to the non-boot partition.
   ```
   (host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
   ```
   or
   ```
   (host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
   ```
   or
   ```
   (host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
   ```
   or
   ```
   (host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
   ```
6. Execute the **show image version** command to verify that the new image is loaded.
   ```
   (host)# show image version
   ```
7. Reboot the Mobility Master.
   ```
   (host)#reload
   ```
8. Execute the **show version** command to verify that the upgrade is complete.
   ```
   (host)#show version
   ```

Verifying the ArubaOS Upgrade

Verify the ArubaOS upgrade in the WebUI or CLI.

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 36 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.

2. Execute the **show version** command to verify the ArubaOS image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 36 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

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

   When you specify a boot partition or copy an image file to a system partition, Mobility Master or managed device checks if the ArubaOS version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the ArubaOS version and configuration files.
5. After switching the boot partition, perform the following steps:
   - Restore the pre-upgrade flash backup from the file stored on the Mobility Master or managed device. Do not restore the ArubaOS flash backup file.
   - Do not import the WMS database.
   - If the RF plan is unchanged, do not import it. If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded ArubaOS version.
   - If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. From **Select destination file** drop-down list, select **Flash file system**, and enter a file name (other than default.cfg).
   c. Click **Copy**.
2. Determine the partition on which your pre-upgrade ArubaOS version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade ArubaOS version is not stored on your system partition, load it into the backup system partition by performing the following steps:

You cannot load a new image into the active system partition.

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot Controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, and click **Reboot**.
   The Mobility Master or managed device reboots after the countdown period.
4. When the boot process is complete, verify that the Mobility Master or managed device is using the correct ArubaOS version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, use the following command to copy it to the Mobility Master or managed device:
   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```
   or
   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the Mobility Master or managed device to boot with your pre-upgrade configuration file.
   ```
   (host) # boot config-file <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your pre-upgrade ArubaOS version is stored.
   ```
   (host) #show image version
   ```

CAUTION

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.