

ArubaOS 8.4.0.3



Copyright Information

© Copyright 2020 Hewlett Packard Enterprise Development LP.

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	3
Revision History	5
Release Overview	6
Related Documents	6
Important Points	6
Supported Browsers	8
Contacting Support	8
New Features and Enhancements	9
Supported Platforms	11
Mobility Master Platforms	11
Mobility Controller Platforms	11
AP Platforms	11
Regulatory Updates	14
Resolved Issues	15
Known Issues and Limitations	34
Upgrade Procedure	46
Important Points to Remember	46

Memory Requirements	47
MIB Files	48
Syslog Files	48
Backing up Critical Data	48
Upgrading ArubaOS	50
Downgrading ArubaOS	53
Before Calling Technical Support	55

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	Removed the Migrating from ArubaOS 6.x to ArubaOS 8.x section from Upgrade Procedure chapter as the Migration Tool is no longer supported.
Revision 03	Added bug AOS-186076 in the Known Issues section.
Revision 02	Removed AOS-154581 from Known Issues section.
Revision 01	Initial release.

This ArubaOS release notes includes the following topics:



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

- [New Features and Enhancements on page 9](#)
- [Supported Platforms on page 11](#)
- [Regulatory Updates on page 14](#)
- [Resolved Issues on page 15](#)
- [Known Issues and Limitations on page 34](#)
- [Upgrade Procedure on page 46](#)

For the 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 Mobility Master Hardware Appliance Installation Guide](#)

Important Points

This section describes the important points to remember before you upgrade the managed device to this release of ArubaOS.

- If you use an image server to upgrade the managed device from the CLI, you must configure an upgrade profile on the Managed Network node.
- Ensure that the IANA timezone is configured exactly the same for each managed device. All the network nodes have to be NTP synchronized.

- Time changed manually in a managed device is not automatically adjusted for a scheduled upgrade.
- DST time change hour is not automatically adjusted for a scheduled upgrade.

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 58 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

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

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

AP Platform

510 Series Campus Access Points

The Aruba 510 Series Campus APs (AP-514 and AP-515) are high-performance, multi-radio wireless devices that can be deployed in either controller-based (ArubaOS) or controller less (ArubaInstant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting legacy 802.11 a/b/g/n/ac wireless services.

The Aruba 510 Series Campus APs are equipped with an integrated BLE and Zigbee radio that provide the following capabilities:

- Location beacon applications
- Wireless console access
- IoT gateway applications

Ethernet ports on the access points are used to connect the device to the wired networking infrastructure and provide (802.3at class 4) PoE power to the device. The access points are equipped with a USB-A port that is compatible with selected cellular modems and other peripherals. When active, this port can supply up to 5W/1A to a connected device.



The 510 Series Campus Access Points do not support UL MU-MIMO and DL MU-MIMO.

The following features are targeted for future releases and are currently not supported on the Aruba 510 Series Campus APs:

- Orthogonal Frequency Division Multiple Access (OFDMA)
- Transmit Beam Forming (TxBF)
- BSS Coloring
- Target Wait Time (TWT)
- Multi Band Operation (MBO)
- Spectrum analysis
- Mesh
- Cellular modem support
- 512 associated clients per radio (currently limited to 230 clients)

For complete technical details see the *Aruba 510 Series Campus APs Datasheet*. For installation instructions, see the *Aruba 510 Series Campus APs Installation Guide*.

Management Access

FIPS X509 Certificate Enhancements

The following are the enhancements for X509 server certificates in the FIPS mode:

- When OCSP is selected for certificate verification and the certificate in OCSP response does not have the OCSP signing purpose bit set in extended key usage, the OCSP response validation fails.
- When CRL is selected and the CA certificate to sign a CRL is not set to cRLsign key usage bit, the CRL validation fails.
- When a signed public key that is generated using CSR is imported into a managed device , all the associated CAs and sub-CAs must be available in the managed device's certificate manager store and imported individually. The import fails if the CAs and sub-CAs are bundled.

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 8.4.0.3*

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 controller platforms that are supported in this release.

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.4.0.3*

Controller Family	Controller Model
7000 Series	7005, 7008, 7010, 7024, 7030
7200 Series	7205, 7210, 7220, 7240, 7240XM, 7280

AP Platforms

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

Table 5: Supported AP Platforms in ArubaOS 8.4.0.3

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
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

Table 5: Supported AP Platforms in ArubaOS 8.4.0.3

AP Family	AP Model
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
510 Series	AP-514, AP-515
RAP 155 Series	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
RAP 3 Series	RAP-3WN, RAP-3WNP

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 support.arubanetworks.com.

The following DRT file version is part of this release:

- DRT-1.0_70537

This chapter describes the issues resolved in this release.



We have migrated to a new defect tracking tool and for tracking purposes, we will list both, the old and the new bug ids.

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-138677	168457	<p>Symptom: The license count in Mobility Master > Licenses page in the WebUI did not reflect the ACR license usage. The fix ensures that the WebUI reflects the license count.</p> <p>Scenario: This issue occurred when the license count was not communicated to the applications running on Standby Mobility Master. This issue was observed in Mobility Master running ArubaOS 8.2.0.0 or later versions.</p>	Licensing	All platforms	ArubaOS 8.2.0.0
AOS-141552 AOS-150776 AOS-155236	172339 184826 190869	<p>Symptom: Active APs were not displayed in the Dashboard > Access Points page in the WebUI. The fix ensures that the active APs are displayed in the WebUI.</p> <p>Scenario: This issue was observed in managed devices running ArubaOS 8.3.0.3 or later versions.</p>	Configuration	All platforms	ArubaOS 8.3.0.3
AOS-142208	173134	<p>Symptom: The Datapath process in a managed device crashed and the managed device rebooted unexpectedly. The fix ensures that the Datapath process does not crash and the managed device works as expected.</p> <p>Scenario: This issue was observed in managed devices running ArubaOS 8.2.0.0.</p>	Controller-Datapath	All platforms	ArubaOS 8.2.0.0
AOS-145876 AOS-157877	177969 194648	<p>Symptom: On a 2.4 GHz radio, channel utilization was very low for few APs. Enhancements to the wireless driver has resolved this issue.</p> <p>Scenario: This issue was observed in AP-203R, AP-207, AP-315, and 340 Series access points running ArubaOS 8.3.0.0 or later versions.</p>	AP-Wireless	AP-203R, AP-207, AP-315, and 340 Series access points	ArubaOS 8.3.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146331 AOS-183502 AOS-184796 AOS-185200	178574	Symptom: Managed Device crashed and rebooted unexpectedly. The fix ensures that the managed device works as expected. Scenario: This issue occurred due to datapath crash. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	Controller Datapath	All platforms	ArubaOS 8.3.0.0
AOS-146505 AOS-147661	178824 180650	Symptom: A client that was connected to an AP displayed low signal strength. The fix ensures that the correct signal strength is displayed. Scenario: This issue occurred when a client associated with the G radio of the AP. This issue was observed in AP-207 access points running ArubaOS 8.2.0.0 or later versions.	AP-Platform	AP-207 access points	ArubaOS 8.2.0.0
AOS-146624 AOS-155236	178976 190869	Symptom: Active APs were not displayed in the Dashboard > Access Points page in the WebUI. The issue is resolved by ensuring that the managed device uses actual IPv6 connection. Scenario: This issue occurred when the Mobility Master and managed devices communicated through IPv6. This issue was observed in managed devices running ArubaOS 8.3.0.3 or later versions.	Configuration	All platforms	ArubaOS 8.3.0.3
AOS-146663	179027	Symptom: Active VRRP managed devices were not forwarding traffic upstream through the GRE tunnel. The fix ensures that the traffic is forwarded upstream through the GRE tunnel. Scenario: This issue was observed in managed devices running ArubaOS 8.2.1.0 in a cluster setup.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0
AOS-147036 AOS-155499 AOS-158444	179623 191227 195448	Symptom: Mobility Master crashed and rebooted unexpectedly. The log file lists the reason for the event as Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:20) . The fix ensures that the Mobility Master works as expected. Scenario: This issue occurred due to a race condition while upgrading the hardware caches. This issue was observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions.	Controller Datapath	All platforms	ArubaOS 8.4.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-148921 AOS-153472	182383 188510	Symptom: A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as Error: Role 'default-iap-user-role' is Unknown . The fix ensures that the error does not occur even without the PEFNG license. Scenario: This issue occurred when the PEFNG license was not enabled but was used in the authentication default profile references. This issue was observed in 7000 Series controllers running ArubaOS 8.3.0.0 or later versions.	Role/VLAN derivation	7000 Series controllers	ArubaOS 8.3.0.0
AOS-150122 AOS-151764	183973 186151	Symptom: Wireless clients failed to reconnect to the SSID after being dropped from the network. The managed device listed the following error messages: <ul style="list-style-type: none"> ■ user repkey change failed ■ macuser repkey change failed The fix ensures that the wireless clients are able to reconnect to the SSID. Scenario: This issue occurred when the GSM slot in a user channel is not deleted, which reduced the available GSM slots to zero. This issue was observed in managed devices running ArubaOS 8.2.1.1.	Base OS Security	All platforms	ArubaOS 8.2.1.1
AOS-150202	184070	Symptom: VIA clients were unable to connect to Suite-B (AES-GCM) cryptographic algorithms with ECDSA certificates enabled on a managed device. The fix ensures that the VIA clients are able to connect to the managed device. Scenario: This issue occurred due to improper interaction of advanced cryptographic license with IKE module. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.2.0.0
AOS-150398	184327	Symptom: A client was displayed on the wrong managed device after association when there was no traffic flow from the client. This issue is resolved by ensuring that only User Anchor Controller (UAC) sends the L2 update on station association. Scenario: This issue occurred when the fdb-update-on-assoc parameter was enabled in an L2 cluster. This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	Station Management	All platforms	ArubaOS 8.2.1.1
AOS-152338	186981	Symptom: SNMP configuration on the controller displays an error message Not in life time window failure: Possible Privacy password mismatch. 663 . The fix ensures that the controller works as expected. Scenario: This issue occurred when AirWave sent empty messages to the controller. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.	SNMP	All platforms	ArubaOS 8.2.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-152427 AOS-153919	187098 189112	Symptom: A Mobility Master recorded high CPU utilization rate and affected services. This issue is resolved by optimizing the DNS lookup. Scenario: This issue occurred when a large number of netdestinations with name-based entries were configured on a Mobility Master. These netdestination names were resolved to the DNS IP address which in turn retained the firewall DNS names and led to high CPU utilization. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0
AOS-153533 AOS-179571 AOS-181276 AOS-181402 AOS-184537	188590 185520 192894 193585	Symptom: Incorrect memory corruption was detected during fast recovery process of an AP. Enhancements to wireless driver resolved the issue. Scenario: This issue occurred when an AP crashed and rebooted unexpectedly due to a kernel panic. This issue was observed in AP-305 access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-305 access points	ArubaOS 8.3.0.0
AOS-153573	188646	Symptom: Whitelist search in the Configuration > Access Points page in the WebUI displayed only 50 AP entries although there are more number of APs. The fix ensures that all the AP entries are listed. Scenario: This issue was observed in managed devices running ArubaOS 8.3.0.3 or later versions.	WebUI	All platforms	ArubaOS 8.3.0.3
AOS-153842	—	Symptom: Few APs were unable to connect to the 2.5 GHz or the 5 GHz radio. Enhancements to the wireless driver resolved this issue. Scenario: This issue was observed in 320 Series access points running ArubaOS 8.2.0.0 or later versions.	320 Series access points	All platforms	ArubaOS 8.2.0.0
AOS-153902	189090	Symptom: A client lost connectivity with an AP. The fix ensures that the AP works as expected. Scenario: This issue occurred when the client forwarded small bytes of packets but the managed device padded it with 0 bytes. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154386 AOS-157543	189716 194143	Symptom: A default crypto isakmp policy with a value above 10000 could be created but not deleted. The fix ensures that the default policies above 10000 cannot be edited or created. Scenario: This issue was observed in a Mobility Master Virtual Appliance running ArubaOS 8.2.2.1.	IPsec	All platforms	ArubaOS 8.2.2.1
AOS-154564 AOS-155770 AOS-156549	189952 191667 192768	Symptom: The SNMP process crashed in a managed device. The fix ensures that the managed device works as expected. Scenario: This issue occurred when the SNMP process received a request to query the table, wlsxSwitchAccessPointTable . This issue was observed in 7240XM controllers running ArubaOS 8.2.1.1 or later versions.	SNMP	7240XM controllers	ArubaOS 8.2.1.1
AOS-154647	190062	Symptom: Output of the show datapath frame all command did not display any values. The fix ensures that the correct values are displayed when the show datapath frame all command is executed. Scenario: This issue was observed in 7240XM controllers running ArubaOS 8.2.1.1.	Controller-Datapath	7240XM controllers	ArubaOS 8.2.1.1
AOS-154665	190094	Symptom: A client connected to an AP displayed low signal strength. The fix ensures that an error message is displayed where it confirms that the Front End Module (FEM) is defective. Scenario: This issue occurred in 340 Series access points running ArubaOS 8.3.0.3 or later versions.	AP-Wireless	340 Series access points	ArubaOS 8.3.0.3
AOS-154735	190181	Symptom: An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as kernel panic: softlockup: hung tasks . Enhancements to the wireless driver resolved the issue. Scenario: This issue was observed in AP-203H access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-203H access points	ArubaOS 8.3.0.0
AOS-155081	190642	Symptom: Post configuration changes, values of show configuration committed and show configuration effective commands were different. This issue is resolved by resetting the iterator to zero after processing auth server list in gdata. Scenario: This issue occurred if iterator was not reset after handling auth servers list in gdata. This issue was observed in a managed devices running ArubaOS 8.2.1.0	Configuration	All platforms	ArubaOS 8.2.1.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155170	190757	Symptom: SNMP query not working for datapath CPU utilization. The fix ensures that the SNMP query works for datapath CPU utilization. Scenario: This issue was observed in 7280 controllers running ArubaOS 8.4.0.0 or later versions.	Controller - Platform	7280 controllers	ArubaOS 8.4.0.0
AOS-155352	191031	Symptom: Bandwidth contract was not getting applied when clients disconnected and reconnected to an AP. The fix ensures that the bandwidth contract gets applied even if the clients disconnect and reconnect. Scenario: This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.0.0
AOS-155533	191269	Symptom: Managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20) . The fix ensures that the managed device works as expected. Scenario: This issue occurred because of corrupt neighbor entry in the forwarding path. This issue was observed in 7280 controllers running ArubaOS 8.3.0.0 or later versions.	Controller - Platform	7280 controllers	ArubaOS 8.3.0.0
AOS-155570 AOS-157636 AOS-182455	191405 194286	Symptom: A controller returned error message: Country Code file creation failed when saving configuration. The fix ensures that the controller works as expected. Scenario: This issue occurred during the initial setup of the controller because of an attempt to create the country code file in a directory that did not exist. This issue was observed in controllers running ArubaOS 8.4.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.4.0.0
AOS-155853	191785	Symptom: The ACLs based on netdestination entries stopped working in a managed device. This issue is resolved by making the netdestination entries case insensitive. Scenario: This issue occurred when the user entered domain names in lowercase or uppercase characters. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155880 AOS-156610	191821 192852	Symptom: Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as mcellsolverstart process error . The fix ensures that the Mobility Master does not crash when the database contains invalid timezone string but logs the error message. Scenario: This issue occurred because of an invalid timezone string. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	AirMatch	All platforms	ArubaOS 8.3.0.0
AOS-156117	192163	Symptom: The RTLS Server configuration field under Advanced accordion of Configuration > System > Profiles > All Profiles > AP > AP system profile <profile-name> page displayed incorrect value of the include unassoc-sta parameter. The fix ensures that the correct value of the include unassoc-sta parameter is displayed. Scenario: This issue occurred when the IP address or port of the RTLS server was configured. This issue was observed in 7205 stand-alone controllers running ArubaOS 8.3.0.2 or later versions in a master-standby topology.	WebUI	7205 controllers	ArubaOS 8.3.0.2
AOS-156162 AOS-158131	192223 195005	Symptom: Managed devices were rebooting intermittently. The log file listed the reason for the event as dds process died . The fix ensures that the managed devices work as expected. Scenario: This issue was observed in managed devices running ArubaOS 8.3.0.3 or later versions.	HA-Lite	All platforms	ArubaOS 8.3.0.3
AOS-156244 AOS-187898	192323	Symptom: Managed devices sent syslog packets with invalid facility levels. This issue is resolved by implementing a local logging facility. Scenario: This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	Logging	All platforms	ArubaOS 8.3.0.0
AOS-156247	192328	Symptom: Some managed devices were getting disconnected when the Mobility Master was rebooted. The fix ensures that the managed devices work as expected. Scenario: This issue occurred due to corruption of the device whitelist database when configuration changes were made to the managed devices. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions in a Mobility Master-Managed Device topology.	Configuration	All platforms	ArubaOS 8.2.0.0
AOS-156267	192349	Symptom: The mDNS process running in a managed device consumed more memory than the typical threshold limit. This issue is resolved by ensuring that the clients are created only when they send an AirGroup packet. Scenario: This issue was observed in managed devices running ArubaOS 8.4.0.0	AirGroup	All platforms	ArubaOS 8.4.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156282	192378	Symptom: A client faced connectivity problem. Scenario: This issue occurred when the enforce DHCP feature was enabled. This issue was observed in managed devices running ArubaOS 8.3.0.4.	Controller-Datapath	All platforms	ArubaOS 8.3.0.4
AOS-156283	192379	Symptom: APs were unable to connect to the stand-alone controller. The fix ensures that the APs work as expected. Scenario: This issue occurred because the synchronized licenses were lost when the standby controller rebooted. This issue was observed in stand-alone controllers running ArubaOS 8.3.0.4 in a stand-alone redundancy setup.	Licensing	All platforms	ArubaOS 8.3.0.4
AOS-156788 AOS-157820	193096 194558	Symptom: Users were unable to view Chromecast devices. The fix ensures that the username is case insensitive. Scenario: This issue occurs when the 802.1x username and the username shared in the ClearPass Policy Manager list used different cases. This issue was observed in AirGroup that is enabled with CPPM-based policies running ArubaOS 8.4.0.0.	AirGroup	All platforms	ArubaOS 8.4.0.0
AOS-156839 AOS-157104	193159 193492	Symptom: The output of the show aaa authentication-server radius statistics command displayed incorrect data for ExpAuthTm , Uptime , and SEQ columns. The fix ensures that the correct data is displayed for these columns. Scenario: This issue occurred when the RADIUS server did not send any request to the managed device. This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.4.0.0
AOS-156840 AOS-157049	193160 193416	Symptom: The CLI Command, halt did not work on the Mobility Master. The fix ensures that the command works as expected. Scenario: This issue occurred as the init process was killed when the halt command was executed. This issue was observed in Mobility Master running ArubaOS 8.3.0.4 or later versions.	Controller-platform	All platforms	ArubaOS 8.3.0.4
AOS-156874 AOS-156918 AOS-157515	193195 193249 194093	Symptom: Managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2) . The fix ensures that the managed device works as expected. Scenario: This issue was observed in 7240XM controllers running ArubaOS 8.2.2.0 or later versions.	Controller-Datapath	7240XM controllers	ArubaOS 8.2.2.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156878	193199	Symptom: A controller crashed when collecting support logs. The fix ensures that the controller works as expected. Scenario: This issue occurred when the show openflow debug ports command was executed. This issue is observed in 7240 controllers running ArubaOS 8.2.2.1.	SDN-Platform	7240 controllers	ArubaOS 8.2.2.1
AOS-157205	193617	Symptom: High Availability on the backup LMS configuration is displayed as disabled when the show ap debug system-status command was executed although High Availability was enabled on the controller. The fix ensures that the show ap debug system-status command displays the correct values. Scenario: This issue was observed in 7200 Series controllers running ArubaOS 8.3.0.0 or later versions.	HA-Lite	7200 Series controllers	ArubaOS 8.3.0.0
AOS-157288	193726	Symptom: The REST API returned the output in XML format instead of JSON format when the show ap arm state command was executed. The fix ensures that the REST API returned the output in JSON format. Scenario: This issue was observed in managed devices running ArubaOS 8.2.1.0.	ARM	All platforms	ArubaOS 8.2.1.0
AOS-157293	193731	Symptom: A VLAN was not preserved and a client got an IP address from a different VLAN that was configured in the VLAN pool. The fix ensures that the preserve VLAN feature works as expected. Scenario: This issue was observed in managed devices running ArubaOS 8.2.2.2.	Station Management	All platforms	ArubaOS 8.2.2.2
AOS-157308 AOS-158209	193755	Symptom: The wlsxWlanRadioTable SNMP did not show all radio types. The fix ensures that the wlsxWlanRadioTable SNMP displays all radio types. Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.0.	Station Management	All platforms	ArubaOS 8.2.1.0
AOS-157357	193834	Symptom: Static link aggregation was not formed correctly when switchport mode and VLAN STP were disabled. Enhancements to the driver resolved this issue. Scenario: This issue was observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions.	Port-Channel	All platforms	ArubaOS 8.0.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157573	194193	Symptom: Wireless clients were unable to access internet through the APs configured in PPPoE and split-tunnel mode. The fix ensures that the wireless client is able to pass traffic and access internet. Scenario: This issue occurred because linux detected one timed out neighbor and deleted the corresponding route cache table. This issue was observed in AP-305 access points running ArubaOS 8.3.0.0 or later versions.	RAP+BOAP	AP-305 access points	ArubaOS 8.3.0.0
AOS-157776	194495	Symptom: L3 redundancy was not working as expected when VPNC failed. The fix ensures that the L3 redundancy works as expected. Scenario: This issue occurred due to incorrect entries in the IPsec Routing table. This issue was observed in managed devices running ArubaOS 8.3.0.4 or later versions.	IPsec	All platforms	ArubaOS 8.3.0.4
AOS-157584	194205	Symptom: A client that was connected to the ENET port of an AP and having both IPv4 and IPv6 addresses lost the bandwidth-contract. This issue is resolved by ensuring that the bandwidth contract is deleted when the last ip-user is removed. Scenario: This issue occurred when the IPv6 entry was timed-out. This issue is observed in managed devices running ArubaOS 8.2.2.3.	IPv6	All platforms	ArubaOS 8.2.2.3
AOS-157600	194231	Symptom: AP crashed unexpectedly. The log file listed the reason for the event as Reboot reason: BadAddr:10000000000338 PC:wlc_tso_hdr_length+0x0/0x78 [wl] Warm-reset . The fix ensures that the APs work as expected. Scenario: This issue was observed in 340 Series access points running ArubaOS 8.3.0.3.	AP-Wireless	340 Series access points	ArubaOS 8.3.0.3
AOS-157606	194237	Symptom: A management user was unable to login to the managed device by authenticating through a Radius server. This issue is resolved by retrieving the current NAS-Port-type from the managed device at the start of the authentication process. Scenario: This issue occurred when the NAS-Port-type was changed to ASYNC from VIRTUAL. This issue was observed in managed devices running ArubaOS 8.3.0.3 or earlier versions.	Radius	All platforms	ArubaOS 8.3.0.3

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157767 AOS-155877 AOS-184056	191816	<p>Symptom: A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20). The fix ensures that the managed device works as expected.</p> <p>Scenario: This issue was observed in 7000 Series and 7200 Series controllers running ArubaOS 8.2.2.0 or later versions.</p>	Controller-Platform	7000 Series and 7200 Series controllers	ArubaOS 8.2.2.0
AOS-157815 AOS-158647	195690 194552	<p>Symptom: VOIP phones did not get ARP broadcasts randomly as the STM process was deleting existing VLANs from the tunnel. The fix ensures that the STM process does not delete VLANs from the tunnel when an update is received for a user from authentication server with initial VLAN and assigned VLAN.</p> <p>Scenario: This issue occurred when tunneled node was configured on the managed device. This issue was observed in managed devices running ArubaOS 8.2.2.3 or later versions.</p>	Tunnel-node-manager	All platforms	ArubaOS 8.2.2.3
AOS-157823	194561	<p>Symptom: Few 802.1X clients are displayed with an IP address instead of a user name in the Managed Network > Dashboard > Overview > Clients page of the WebUI.</p> <p>Scenario: This issue was observed in stand-alone controllers running ArubaOS 8.3.0.3 or later versions.</p>	Base OS Security	All platforms	ArubaOS 8.3.0.3
AOS-158046	194884	<p>Symptom: Access points crashed unexpectedly. The log files listed the reason for the event as AP Reboot reason: BadAddr:b2de60c08681450d PC:wlc_send80211raw_stateful+0x1ee8/0x2288 [wl] Warm-reset. Enhancements to the wireless driver resolved the issue.</p> <p>Scenario: This issue was observed in 340 Series access points running ArubaOS 8.3.0.4 or later versions.</p>	AP-Wireless	340 Series access points	ArubaOS 8.3.0.4
AOS-158093	194946	<p>Symptom: The WEP key ID of multicast packets in a managed device was incorrect. This issue is resolved by ensuring that the WEP key ID to set to 1.</p> <p>Scenario: This issue occurred when AirMatch changed the channel. This issue was observed in managed devices running ArubaOS 8.2.2.1.</p>	Base OS Security	All platforms	ArubaOS 8.2.2.1
AOS-158157	195039	<p>Symptom: AP groups created were not listed in the AP group drop-down list in the Managed Network > Configuration > Access Points > Whitelist > Campus AP Whitelist > Add New Campus AP whitelist page of the WebUI. The fix ensures that all the AP groups are listed in the AP group drop-down list.</p> <p>Scenario: This issue was observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions.</p>	WebUI	All platforms	ArubaOS 8.4.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-158180 AOS-158565 AOS-182719 AOS-183629 AOS-184955 AOS-185312 AOS-185342 AOS-185428	195080 195592	<p>Symptom: The licenses within the AP licensing pool were consumed every time the mesh point was rebooted or was disconnected from its parent. The fix ensures that the license count does not get exhausted.</p> <p>Scenario: This issue was observed in APs in mesh portal and mesh point mode running ArubaOS 8.2.0.0 or later versions.</p>	AP-Platform	All platforms	ArubaOS 8.2.0.0
AOS-158204	195106	<p>Symptom: OFA process crashed in a controller unexpectedly. The fix ensures that the controllers work as expected.</p> <p>Scenario: This issue was observed in 7240 controllers running ArubaOS 8.2.2.3 in a cluster setup.</p>	Controller-Platform	7240 controllers	ArubaOS 8.2.2.3
AOS-158254 AOS-184144	195177	<p>Symptom: Some managed devices dropped ARP packets while trying to route traffic to a specific hop IP address. The fix ensures that the managed devices work as expected.</p> <p>Scenario: This issue occurred when policy-based routing picked the incorrect next-hop destination address to route the packets. This issue was observed in managed devices running ArubaOS 8.4.0.0 in a Mobility Master-Managed Device topology.</p>	Policy-Based Routing	All platforms	ArubaOS 8.4.0.0
AOS-158603	195637	<p>Symptom: Some APs failed to come up on the managed device. The fix ensures that the AP functions as expected.</p> <p>Scenario: This issue occurred when the managed device was upgraded from ArubaOS 8.3.0.4 to ArubaOS 8.4.0.0. This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p>	AP-Platform	All platforms	ArubaOS 8.4.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-158311	195264	<p>Symptom: A managed device did not prompt an error or show restriction when configuring a VRRP authentication key. The fix ensures that an error is displayed if a VRRP authentication key is configured with more than 8 characters.</p> <p>Scenario: This issue occurred when the VRRP authentication key contained more than 8 characters. This issue was observed in managed devices running ArubaOS 8.2.1.0.</p>	VRRP	All platforms	ArubaOS 8.2.1.0
AOS-158455	195461	<p>Symptom: The output of the show configuration system-commands pending command displayed committed configuration details instead of pending configuration details. The fix ensures that the command displays the pending configuration details.</p> <p>Scenario: This issue was observed in a Mobility Master Virtual Appliance running ArubaOS 8.2.1.0 or later versions.</p>	Controller-Platform	All platforms	ArubaOS 8.2.1.0
AOS-158599 AOS-182977	195633	<p>Symptom: Mobility Master crashed and rebooted unexpectedly. The log file lists the reason for the event as, Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4). The fix ensures that the Mobility Master works as expected.</p> <p>Scenario: This issue was observed in Mobility Master running ArubaOS 8.2.0.0 or later versions.</p>	Controller-Datapath	All platforms	ArubaOS 8.2.0.0
AOS-181971	—	<p>Symptom: The video paused for a few seconds on random clients. Enhancements to the wireless driver resolved this issue.</p> <p>Scenario: This issue occurred when the clients were playing a DDMO converted 500 Kbps video stream broadcasted by Windows Media Server and the radio resets were triggered by PSM watchdog every few seconds. This issue was observed in 510 Series access points running ArubaOS 8.4.0.1.</p>	AP-Wireless	510 Series access points	ArubaOS 8.4.0.1
AOS-181974	—	<p>Symptom: The packetin_dispatcher process crashed multiple times on a Mobility Master Virtual Appliance. The fix ensures that the Mobility Master Virtual Appliance works as expected.</p> <p>Scenario: This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.2.2.3 or later versions.</p>	SDN-Platform	All platforms	ArubaOS 8.2.2.3
AOS-182023	—	<p>Symptom: The Dashboard page in the WebUI displayed the A controller is required for information to be displayed error message. The fix ensures that the Dashboard page does not display the error message.</p> <p>Scenario: This issue was observed in Mobility Master running ArubaOS 8.2.1.0 or later versions.</p>	Configuration	All platforms	ArubaOS 8.2.1.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-182091 AOS-183253 AOS-183255	—	<p>Symptom: The mDNS process in a managed device crashed unexpectedly. The fix ensures that the managed devices work as expected.</p> <p>Scenario: This issue occurred because of memory corruption. This issue was observed in a Mobility Master Hardware Appliance running ArubaOS 8.2.2.3.</p>	AirGroup	All platforms	ArubaOS 8.2.2.3
AOS-182221	—	<p>Symptom: Some Remote APs took a longer time to come up on a controller during initial provisioning or after a reboot. Reducing the idle time between the AP and controller resolved this issue.</p> <p>Scenario: This issue occurred due to poor CPU performance of the AP causing a delay in AP boot phase and image check phase. This issue was observed in AP-303H access points running ArubaOS 8.2.1.0 or later versions.</p>	AP-Platform	AP-303H access points	ArubaOS 8.2.1.0
AOS-182294	—	<p>Symptom: When the show ip route command was executed, IPsec route table displayed IP route entries although the IPsec map configuration was disabled. The fix ensures that the stand-alone controller works as expected.</p> <p>Scenario: This issue occurred after the stand-alone controller was rebooted. This issue was observed in stand-alone controllers running ArubaOS 8.2.2.3 or later versions.</p>	IPsec	All platforms	ArubaOS 8.2.2.3
AOS-182928 AOS-183355	—	<p>Symptom: A managed device crashed due to MDNS memory leak. The fix ensures that the managed device works as expected.</p> <p>Scenario: This issue occurred due to a race condition causing memory allocation failure. This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p>	AirGroup	All platforms	ArubaOS 8.4.0.0
AOS-182929	—	<p>Symptom: The PIM module in 7200 Series controller crashed unexpectedly. Enhancements to the PIM module has resolved this issue.</p> <p>Scenario: This issue occurred due to a condition of dangling reference. This issue was observed in 7200 Series controllers running ArubaOS 8.2.2.3 or later versions in a Mobility Master - Managed Device topology with clustering and IGMP enabled.</p>	PIM-SM	7200 Series controllers	ArubaOS 8.2.2.3

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183023 AOS-185198 AOS-185429	—	<p>Symptom: A client was unable to view AirGroup servers in a centralized AirGroup deployment. The fix ensures that the client is able to view AirGroup servers.</p> <p>Scenario: This issue occurred because of an error in the policy lookup. This issue was observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions.</p>	AirGroup	All platforms	ArubaOS 8.4.0.0
AOS-183148 AOS-183454 AOS-183782 AOS-184700 AOS-185163	—	<p>Symptom: APs crashed and rebooted unexpectedly. The log file lists the reason for the event as Reboot reason: fatal exception in interrupt. The fix ensures that the APs work as expected.</p> <p>Scenario: This issue is observed in AP-214, AP-215 and AP-315 access points running ArubaOS 8.0.0.0 or later versions.</p>	AP-Platform	AP-214, AP-215 and AP-315 access points	ArubaOS 8.0.0.0
AOS-157921 AOS-158238 AOS-183152	194705 195151 188356	<p>Symptom: Clients reconnected to the AP frequently as the effective rates and advertised rates were not the same. Enhancements to the wireless driver resolved this issue.</p> <p>Scenario: This issue was observed in 510 Series access points running ArubaOS 8.4.0.0.</p>	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-183468 AOS-183550 AOS-183551 AOS-184610	—	<p>Symptom: The managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:2). This issue is resolved by optimizing the ARP data that is sent to Mobility Masters.</p> <p>Scenario: This issue occurred because OpenFlow from the managed device was sending all ARP packets to the Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.4.0.0.</p>	Controller - Datapath	All platforms	ArubaOS 8.4.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183445	—	<p>Symptom: The usage graph was not displayed in the Dashboard > Overview page of a managed device. The fix ensures that the usage graph is displayed as expected.</p> <p>Scenario: This issue occurred because of invalid data for the BSSID statistics and a large number of AMON_BSSID_TUNNEL_STATS_MESSAGE packets. This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p>	Controller-Datapath	All platforms	ArubaOS 8.4.0.0
AOS-183601	—	<p>Symptom: Some APs advertised incorrect protection flag in their beacons. Enhancements to the wireless driver resolved the issue.</p> <p>Scenario: This issue occurred when 802.11g, 802.11n, or 802.11ac clients were connected to 2.4 GHz radios and low rates of 1 Mbps were removed from the Tx rate of SSID profiles. This issue was observed in AP-305 and AP-315 access points running ArubaOS 8.3.0.0 or later versions.</p>	AP-Wireless	AP-305 and AP-315 access points	ArubaOS 8.3.0.0
AOS-183962 AOS-184518	—	<p>Symptom: IKE Overlay routes for client traffic were missing from the VPN Concentrator and the managed device. Hence, the managed device got disconnected from the Mobility Master. The fix ensures that the IKE Overlay routes are available and the connection is restored between the managed device and the Mobility Master.</p> <p>Scenario: This issue was observed in 7220 and 7008 controllers running ArubaOS 8.3.0.0 or later versions.</p>	IPsec	7220 and 7008 controllers	ArubaOS 8.3.0.0
AOS-184032	—	<p>Symptom: An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as Reboot caused by kernel panic: Fatal exception in interrupt: PC is at asap_bw_mgmt_reset_desc_count. Enhancements to the wireless driver resolved the issue.</p> <p>Scenario: This issue was observed in AP-315 access points running ArubaOS 8.3.0.0 or later versions.</p>	AP-Wireless	AP-315 access points	ArubaOS 8.3.0.0
AOS-184093	—	<p>Symptom: The cellular handoff assist feature did not work even though the clients reached the Signal-to-Noise Ratio threshold rate. The fix ensures that the cellular handoff assist feature is triggered.</p> <p>Scenario: This issue was observed in access points running ArubaOS 8.2.0.0 or later versions.</p>	ARM	All platforms	ArubaOS 8.2.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184265 AOS-184964	—	<p>Symptom: A Mobility Master displayed Name-server already exists error message when more than one DNS server was added using the Configuration > System > General > Domain Name System page in the WebUI. The fix ensures that more than one DNS server can be added.</p> <p>Scenario: This issue occurred due to an error in API response for ipv6_domain_lookup. This issue was observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions.</p>	Configuration	All platforms	ArubaOS 8.4.0.0
AOS-184269 AOS-185202	—	<p>Symptom: APs were unable to join a cluster and were rebooting with the error, unable to contact switch: HELLO-TIMEOUT. The fix ensures that the APs are able to join the cluster.</p> <p>Scenario: This issue occurred when the cluster leader received a dormant add to DDS from a different managed device that was a previous leader. This issue was observed in managed devices running ArubaOS 8.3.0.6.</p>	Cluster Manager	All platforms	ArubaOS 8.3.0.6
AOS-184287	—	<p>Symptom: The command show ap client trail-info displayed the de-auth reason as Client- match instead of cellular handoff assist. The fix ensures that the command works as expected.</p> <p>Scenario: This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.</p>	ARM	All platforms	ArubaOS 8.0.0.0
AOS-184296	—	<p>Symptom: An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as Reboot caused by kernel panic: Fatal exception in interrupt. The fix ensures that the AP works as expected.</p> <p>Scenario: This issue was observed in AP-325 access points running ArubaOS 8.3.0.0 or later versions.</p>	AP Datapath	AP-325 access points	ArubaOS 8.3.0.0
AOS-184432	—	<p>Symptom: Managed devices crashed and rebooted unexpectedly. The log file listed the reason for the event as Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2). The fix ensures that the managed devices work as expected.</p> <p>Scenario: This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p>	Controller - Datapath	All platforms	ArubaOS 8.4.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184441	—	<p>Symptom: The output of the show boot history command displayed incorrect user information in the Reboot Cause message. However, the correct information was logged in the Controller Reboot initiated message before the reload. The fix ensures that the Reboot Cause message displays the appropriate information.</p> <p>Scenario: This issue occurred because the managed device incorrectly used the current user information who had logged in and executed the show boot history command for the Reboot Cause message. This issue was not limited to any specific controller model or ArubaOS version.</p>	Controller-Platform	All platforms	ArubaOS 8.3.0.4
AOS-184675	—	<p>Symptom: Datapath process crashed in a managed device during L3 mobility. The fix ensures that the managed device works as expected.</p> <p>Scenario: This issue occurred when a client roamed to the managed device. This issue was observed in managed devices running ArubaOS 8.3.0.0.</p>	Controller-Datapath	All platforms	ArubaOS 8.3.0.0
AOS-184851	—	<p>Symptom: The login-fcgi process in a controller crashed unexpectedly. This issue is resolved by increasing the array size to 128K for processing request parameters.</p> <p>Scenario: This issue occurred when http requests larger than 8k were processed, leading to a segmentation fault. This issue was observed in stand-alone controllers running ArubaOS 8.4.0.0 or later versions.</p>	Captive Portal	7280 controllers	ArubaOS 8.4.0.0
AOS-185089	—	<p>Symptom: Unable to setup an IPsec tunnel because Mobility Masters are using port 500 instead of port 4500 to form L3 redundancy. The fix ensures that the IKE connection initiates on port, 4500.</p> <p>Scenario: This issue occurred as IKE started negotiating on port 500. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0</p>	Master-Redundancy	All platforms	ArubaOS 8.3.0.0
AOS-186113	—	<p>Symptom: Mesh wired AP did not work as expected. The fix ensures that the mesh wired AP works in bridge trunk mode.</p> <p>Scenario: This issue occurred when the DHCP packet had a VLAN tag. This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p>	Mesh	All platforms	ArubaOS 8.4.0.0
AOS-186667	—	<p>Symptom: Clients were unable to associate to AP because AP stops beaconing. The fix ensures that the APs work as expected.</p> <p>Scenario: This issue was observed in 100 Series, 110 Series, and 130 Series access points running ArubaOS 8.3.0.0.</p>	AP-Wireless	100 Series, 110 Series, and 130 Series access points	ArubaOS 8.3.0.0

Table 6: Resolved Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187087	—	<p>Symptom: APs rebooted frequently. The log files listed the reason for the event as BUGFailureAt:net/core/skbuff.c:1609/consume_skb(! Warm-reset. Enhancements to the wireless driver resolved this issue.</p> <p>Scenario: This issue occurred when the APs were in AM mode. This issue was observed in 510 Series access points running ArubaOS 8.3.0.0.</p>	AP-Wireless	510 Series access points	ArubaOS 8.3.0.0
AOS-187113 AOS-187451	—	<p>Symptom: APs were using 40MHz channels on 2.4 GHz instead of 20 MHz. The fix ensures that the channel is switched back to 20 Mhz.</p> <p>Scenario: This issue occurred because in 2.4 GHz, the channels are always scanned in 40 MHz but if the scan channel and home channel share the same control channel, channel is switched back to the configured channel after scan. This issue was observed in 510 Series access points running ArubaOS 8.4.0.0.</p>	AP-Wireless	510 Series access points	ArubaOS 8.4.0.2
AOS-187750	—	<p>Symptom: APs were unable to discover the nearby AP list. This issue is resolved by increasing the dwell time of the DFS channels to 60 ms.</p> <p>Scenario: This issue occurred because the dwell time of the DFS channels were set to 20 ms. This issue was observed in 510 Series access points running ArubaOS 8.4.0.0 or later versions.</p>	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0

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



NOTE

We have migrated to a new defect tracking tool and for tracking purposes, we will list both, the old and the new bug ids.

Limitations

Following is the limitation observed in this release.

No Support for Captive Portal

Captive portal is not supported for the split-tunnel mode Virtual APs and wired APs, when cluster is enabled.

Known Issues

Following are the known issues observed in this release.

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-141831	172680	Symptom: The MIB files and IDS logs have references to an unnecessary URL. Scenario: This issue is observed in MIB files and IDS logs of managed devices running ArubaOS 8.2.0.0. Workaround: None.	SNMP	All platforms	ArubaOS 8.2.0.0
AOS-144684 AOS-184346	176339	Symptom: Managed devices are getting log files that contain incorrect or garbled essid and bssid values. Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions. Workaround: None.	Station Management	All platforms	ArubaOS 8.2.1.0
AOS-145566	177559	Symptom: A Mobility Master is unable to forward the traffic that is sourced from an IP interface in the gateway. Scenario: This issue occurs when netdestinations are used in the routing ACL rule. This issue is observed in Mobility Masters running ArubaOS 8.0.1.0 or later versions. Workaround: None.	Policy-Based Routing	All platforms	ArubaOS 8.0.1.0
AOS-145876 AOS-157877	177969 194648	Symptom: On a 2.4 GHz radio, channel utilization is very low for few APs. Scenario: This issue is observed in AP-203R, AP-207, AP-315, and 340 Series access points running ArubaOS 8.3.0.0 or later versions. Workaround: None.	AP-Wireless	AP-203R, AP-207, AP-315, and 340 Series access points	ArubaOS 8.3.0.0
AOS-145910	178014	Symptom: Managed devices send RADIUS accounting request packets to ClearPass without class attributes. Scenario: This issue is observed in managed devices running ArubaOS 8.2.0.2. Workaround: None.	Base OS Security	All platforms	ArubaOS 8.2.0.2
AOS-146118	178291	Symptom: CLI dir command is missing some basic options like sorting by date, name, size and filtering by keyword Scenario: This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions Workaround: None.	Controller-Platform	All platforms	ArubaOS 8.2.1.0

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146720	179107	<p>Symptom: A stand-alone controller displays the Module licenssemgr is busy. Please try later error message while adding licenses.</p> <p>Scenario: This issue is observed in stand-alone controllers running ArubaOS 8.1.0.4 in a master-local topology.</p> <p>Workaround: None.</p>	Licensing	All platforms	ArubaOS 8.1.0.4
AOS-147018	179516	<p>Symptom: AP crashes and reboots unexpectedly. The log file lists the reason for the event as Kernel panic - not syncing: softlockup: hung tasks.</p> <p>Scenario: This issue is observed in AP-203H access points running ArubaOS 8.3.0.2.</p> <p>Workaround: None.</p>	AP-Wireless	AP-203H access points	ArubaOS 8.2.0.2
AOS-147511	180406	<p>Symptom: Clients are receiving IPv6 router advertisements randomly from different VLANs.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p> <p>Workaround: None.</p>	IPv6	All platforms	ArubaOS 8.2.1.0
AOS-148642 AOS-156454 AOS-158502 AOS-158515	182031 192618 195518 195534	<p>Symptom: The Postgres process crashes on a managed device unexpectedly.</p> <p>Scenario: This issue is observed in 7210 controllers running ArubaOS 8.5.0.0 or later versions.</p> <p>Workaround: None.</p>	Logging	7210 controllers	ArubaOS 8.5.0.0
AOS-148675	182073	<p>Symptom: An AP crashes and reboots unexpectedly. The log file lists the reason for the event as Kernel panic - not syncing: Rebooting the AP because of FW ASSERT: rcRateFind+229; ratectrl_11ac.c:2394.</p> <p>Scenario: This issue is observed in AP-315 access points running ArubaOS 8.2.1.0.</p> <p>Workaround: None.</p>	AP-Wireless	AP-315 access points	ArubaOS 8.2.1.0
AOS-149543	183200	<p>Symptom: During upgrade process, the image files are left on the flash drive and the user is unable to upgrade the ArubaOS image.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions.</p> <p>Workaround: None.</p>	Controller-Platform	All platforms	ArubaOS 8.2.1.1

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-150797	184849	Symptom: Clients are unable to make or receive calls. A Network busy error message is displayed. Scenario: This issue occurs when WMM is disabled on the managed device. This issue is observed in AP-315 access points running ArubaOS 8.2.1.1. Workaround: None.	WMM	AP-315 access points	ArubaOS 8.2.1.1
AOS-151012 AOS-146980	185165	Symptom: A managed device crashes unexpectedly. The log file lists the reason for this event as Reboot Cause: Reboot by Upgrade Manager Intent:cause:register 60:86:50:60 . Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. Workaround: None.	Controller-Platform	All platforms	ArubaOS 8.2.1.1
AOS-151275	185499	Symptom: Managed devices at the branch office are unable to receive IP address from the branch uplink pool. Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions. Workaround: None.	IPsec	All platforms	ArubaOS 8.2.1.0
AOS-151355	185602	Symptom: Managed Devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. Scenario: This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. Workaround: None.	Policy-Based Routing	All platforms	ArubaOS 8.0.1.0
AOS-152076 AOS-150739	186605 184774 185405	Symptom: A managed device fails to establish IPsec tunnel on its primary uplink. Scenario: This issue occurs because the socket descriptor slots are not reused when the IP address is flapped in the isakmpd process. This issue is observed in managed devices running ArubaOS 8.0.1.0. Workaround: None.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
AOS-152745	187566	Symptom: Some APs detect false radar signals and changes radio channels frequently Scenario: This issue is observed in AP-228, AP-305, 320 Series, and 340 Series access points running ArubaOS 8.3.0.1 or later versions. Workaround: None.	AP-Wireless	AP-228, AP-305, 320 Series, and 340 Series access points	ArubaOS 8.3.0.1

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-152827	187685	<p>Symptom: User is unable to delete banner via configuration using CLI or WebUI.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.3.0.2 or later versions.</p> <p>Workaround: None.</p>	Configuration	All platforms	ArubaOS 8.3.0.2
AOS-153169	188130	<p>Symptom: AP crashes and reboots unexpectedly. The log files lists the reason for the event as kernel panic: softlockup: hung tasks.</p> <p>Scenario: This issue occurs because the firewall processes too many packets in one batch. This issue is observed in AP-303H access points running ArubaOS 8.3.0.1 or later versions.</p> <p>Workaround: None.</p>	AP Datapath	AP-303H access points	ArubaOS 8.3.0.1
AOS-155801	191726	<p>Symptom: SNMP walk performed from AirWave does not produce correct results.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.3.0.3.</p> <p>Workaround: None.</p>	SNMP	All platforms	ArubaOS 8.3.0.3
AOS-155879	191818	<p>Symptom: User is unable to delete or edit guest provisioning user on WebUI and CLI.</p> <p>Scenario: This issue occurs due to a trailing space that is added when adding a user. This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.2.0.2.</p> <p>Workaround: None</p>	Base OS Security	All platforms	ArubaOS 8.2.0.2
AOS-155880	191821	<p>Symptom: Mobility Controller Virtual Appliance crashes and reboots unexpectedly. The log file lists the reason for the event as mcellsolverstart processerror.</p> <p>Scenario: This issue is observed in Mobility Controller Virtual Appliance running ArubaOS 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	AirMatch	All platforms	ArubaOS 8.3.0.0
AOS-155927	191876	<p>Symptom: Clients are getting de-authenticated when the User Anchor Controller (UAC) is down.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions.</p> <p>Workaround: None.</p>	Station Management	All platforms	ArubaOS 8.2.1.1

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155987 AOS-157010	191958 193361	Symptom: The ap_name field appears blank in reporting_radio , radio_history , and ap_info collection parameters. Scenario: This issue is observed in APs running ArubaOS 8.3.0.3 or later versions. Workaround: None.	AirMatch	All platforms	ArubaOS 8.3.0.3
AOS-156079	192111	Symptom: The BTM request disassociation timer is incorrectly set to the value of 25600 instead of the default value of 100. Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0. Workaround: None.	ARM	All platforms	ArubaOS 8.4.0.0
AOS-156085 AOS-157704	192119 194393	Symptom: Managed devices are unable to get the controller-IP address during boot up after an upgrade. Scenario: This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. Workaround: None.	Configuration	All platforms	ArubaOS 8.1.0.0
AOS-156087	192121	Symptom: Some devices incorrectly trigger roaming behavior due to the static value of the BTM request disassociation timer. Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0. Workaround: None.	ARM	All platforms	ArubaOS 8.4.0.0
AOS-156182	192248	Symptom: AP crashes and reboots unexpectedly. The log file lists the reason for the event as Kernel panic: softlockup: hung tasks . Scenario: This issue is observed in AP-205 access points running ArubaOS 8.3.0.2 Workaround: None.	AP-Wireless	AP-205 access points	ArubaOS 8.3.0.2
AOS-156742 AOS-156977	193031 193319	Symptom: After pushing a complete configuration via API, the user is unable to make any change to IP Probe configuration. Scenario: This issue is observed in managed devices running ArubaOS 8.0.1.0. Workaround: None.	Configuration	All platforms	ArubaOS 8.0.1.0

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156838	193158	Symptom: User is unable to reprovision an AP. Scenario: This issue occurs when a special character in a German keypad is used in the AP name. This issue is observed in APs connected to managed devices running ArubaOS 8.2.2.1. Workaround: Hard reset the access point.	Configuration	All platforms	ArubaOS 8.2.2.1
AOS-156899	193229	Symptom: Multiple processes crash on a Mobility Master. The log files lists the reason for the event as PROCESS_NOT_RESPONDING_CRITICAL . Scenario: This issue is observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions. Workaround: None.	Controller-Platform	All platforms	ArubaOS 8.2.1.0
AOS-157011	193362	Symptom: The output of show datapath papi counters command displays invalid tunnel endpoint information. Scenario: This issue is observed in Mobility Masters running ArubaOS 8.3.0.3. Workaround: None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.3
AOS-157056	193423	Symptom: The Authentication module on a managed device crashes and the APs reboot. Scenario: This issue occurs when clients that are in bridge forwarding mode, communicate with a managed device, in the split-tunnel-mode. This issue is observed in managed devices running ArubaOS 8.2.1.0. Workaround: None.	Base OS Security	All platforms	ArubaOS 8.2.1.0
AOS-157233	193662	Symptom: Device model name is displayed incorrectly in the Dashboard > Controllers > Model page in the WebUI. Scenario: This issue is observed in managed devices running ArubaOS 8.2.2.0 or later versions. Workaround: None.	VRRP	All platforms	ArubaOS 8.2.2.0
AOS-157326	193781	Symptom: Users are unable to perform cluster upgrade using a specific file server. Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions. Workaround: None.	Upgrade	All platforms	ArubaOS 8.4.0.0

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157343 AOS-186055	193800	Symptom: The Mesh SSIDs are broadcasted and can be viewed by the clients. Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions. Workaround: None.	Mesh	All platforms	ArubaOS 8.4.0.0
AOS-157492	194064	Symptom: VRRP authentication fails in a managed device. Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions. Workaround: None.	VRRP	All platforms	ArubaOS 8.2.1.0
AOS-157770	194484	Symptom: The managed devices send TACACS login requests using OSPF IP instead of the loopback IP. Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0. Workaround: None.	TACACS	All platforms	ArubaOS 8.4.0.0
AOS-158274	195201	Symptom: The Override icon in the WPA passphrase and Retype fields in Configuration > System > Profiles > SSID profile appears even after manually entering the passphrase and enabling Remove Override . Scenario: This issue is observed in Mobility Master running ArubaOS 8.4.0.0 or later versions. Workaround: None.	WebUI	All platforms	ArubaOS 8.4.0.0
AOS-158285	195212	Symptom: The Health status of the Mobility Master in the dashboard displays as poor with the reason, At least 10% of this controller APs are down , although the managed device's health status is displayed as good. Scenario: This issue occurs as the Mobility Master lists standby APs as well in a cluster setup. This issue was observed in managed devices running ArubaOS 8.4.0.1 in a cluster-setup. Workaround: None.	WebUI	All platforms	ArubaOS 8.4.0.1
AOS-158299	195239	Symptom: The profmgr process crashes and the Mobility Master restarts unexpectedly. Scenario: This issue is observed in Mobility Masters running ArubaOS 8.0.1.0. Workaround: None.	Configuration	All platforms	ArubaOS 8.0.1.0

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-158350 AOS-157797 AOS-158521	195313 194518 195540	Symptom: mDNS process crashes in a managed device. Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions. Workaround: None.	AirGroup	All platforms	ArubaOS 8.4.0.0
AOS-158497	195513	Symptom: An AP reboots unexpectedly. The log file lists the reason for the event as Reboot caused by kernel panic: softlockup: hung tasks. Scenario: This issue is observed in AP-303H access points running ArubaOS 8.2.2.3. Workaround: None.	AP Datapath	AP-303H access points	ArubaOS 8.2.2.3
AOS-181925	195713	Symptom: The Dashboard > Access Points page of the Mobility Master WebUI does not display the AP Name, Status, IP address of an AP that is displayed as UP on the managed device. Scenario: This issue is observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions. Workaround: None.	WebUI	All platforms	ArubaOS 8.2.1.1
AOS-182073 AOS-183743	—	Symptom: AP crashes and reboots unexpectedly. The log files lists the reason for the event as Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT. Scenario: This issue is observed in AP-315 access points running ArubaOS 8.3.0.5. Workaround: None.	AP-Wireless	AP-315 access points	ArubaOS 8.3.0.5
AOS-182893	—	Symptom: The standby Mobility Master information is retained in the WebUI although the redundancy configuration is deleted on the active Mobility Master. Scenario: This issue is observed in Mobility Masters running ArubaOS 8.4.0.1. Workaround: None.	WebUI	All platforms	ArubaOS 8.4.0.1
AOS-183536	—	Symptom: Users are unable to connect to the wireless network. Scenario: This issue occurs as the RADIUS requests are not sent to authentication server from the managed device. This issue is observed in managed devices running ArubaOS 8.4.0.0. Workaround: None.	RADIUS	All platforms	ArubaOS 8.4.0.0

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184051	—	Symptom: Mobility Master keeps sending NTP sync packets every 15 seconds to NTP server. Scenario: This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. Workaround: None.	VLAN	All platforms	ArubaOS 8.4.0.0
AOS-184801	—	Symptom: Managed devices crashes and reboots unexpectedly. The log files lists the reason for the event as Datapath exception . Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0. Workaround: None.	Controller - Datapath	All platforms	ArubaOS 8.4.0.0
AOS-184519	—	Symptom: User is unable to delete the VLAN even though the VLAN is not mapped on any node or group. Scenario: This issue is observed in managed devices running ArubaOS 8.3.0.4. Workaround: None.	Configuration	All platforms	ArubaOS 8.3.0.4
AOS-184545	—	Symptom: An AP crashes and reboots unexpectedly. The log file lists the reason for this event as kernel panic: softlockup: hung tasks . Scenario: This issue is observed in AP-303H access points running ArubaOS 8.0.0.0 or later versions.	AP Datapath	AP-303H access points	ArubaOS 8.0.0.0
AOS-185500 AOS-186325	—	Symptom: The sapd process crashes in a managed device unexpectedly. Scenario: This issue is observed in managed devices running ArubaOS 8.3.0.6. Workaround: None.	AP-Wireless	All platforms	ArubaOS 8.3.0.6
AOS-186035	—	Symptom: Managed devices disconnected from the VPNC for 30 minutes unexpectedly. The log files lists the reason for the event as Bad LSA Checksum . Scenario: This issue is observed in managed devices running ArubaOS 8.2.2.0 or later versions. Workaround: None.	OSPF	All platforms	ArubaOS 8.2.2.3

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186076 AOS-187884 AOS-189850 AOS-191866 AOS-192310 AOS-193177 AOS-193387	—	<p>Symptom: The STM process crashes unexpectedly in a managed device in a cluster setup.</p> <p>Scenario: This issue occurs because some memory allocated for the client is not released after some clients disconnect from their UAC (User Anchor Controller) in a Cluster. This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	Station Management	All platforms	ArubaOS 8.4.0.0
AOS-186133	—	<p>Symptom: Managed devices display abnormally high multicast traffic in Performance Summary > All Radios in the monitoring page.</p> <p>Scenario: This issue is observed in 320 Series access points running ArubaOS 8.3.0.6.</p> <p>Workaround: None.</p>	AP-Wireless	320 Series access points	ArubaOS 8.3.0.6
AOS-186304	—	<p>Symptom: User is unable to connect to the Remote AP over IPv6 network.</p> <p>Scenario: This issue occurs because the AP is waiting to receive AP regulatory domain information from the managed device. This issue is observed in managed devices running ArubaOS 8.3.0.6.</p> <p>Workaround: None.</p>	IPv6	All platforms	ArubaOS 8.3.0.6
AOS-186422	—	<p>Symptom: Clients are unable to get IP addresses.</p> <p>Scenario: This issue occurs when the clients are connected to APs with forward mode set to Tunnel. This issue is observed in managed devices running ArubaOS 8.3.0.1 or later versions.</p> <p>Workaround: None.</p>	Controller - Datapath	All platforms	ArubaOS 8.3.0.1
AOS-186526	—	<p>Symptom: The profmgr process in a Mobility Master crashes unexpectedly.</p> <p>Scenario: This issue is observed in Mobility Masters running ArubaOS 8.4.0.0.</p> <p>Workaround: None.</p>	IPsec	All platforms	ArubaOS 8.4.0.0

Table 7: Known Issues in ArubaOS 8.4.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186860	—	Symptom: RADIUS Authentication requests are sent in IP address of the managed device although they are configured to go through the loopback IP. Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.1. Workaround: None.	IPsec	All platforms	ArubaOS 8.4.0.1
AOS-186969	—	Symptom: Acct-Authentic radius attribute is not sent from the managed device. Scenario: This issue occurs when the managed devices were upgraded to ArubaOS 8.4.0.2. This issue was observed in managed devices running ArubaOS 8.4.0.1. Workaround: None.	Radius	All platforms	ArubaOS 8.4.0.1
AOS-186979	—	Symptom: APs are unable to reboot automatically after an uplink or WAN link status change. Scenario: This issue is observed in APs running ArubaOS 8.3.0.6 or later versions. Workaround: None.	AP-Platform	All platforms	ArubaOS 8.3.0.6
AOS-187115	—	Symptom: Application name in the policy configuration is incorrect in the Configuration > Roles & Policies > Policies > <Policy name> WebUI page. Scenario: This issue occurs when the WebUI is accessed for the first time. This issue was observed in Mobility Masters running ArubaOS 8.2.2.0 or later versions. Workaround: None.	WebUI	All platforms	ArubaOS 8.2.2.0

This chapter details software upgrade procedures. Aruba best practices recommend 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, and/or stand-alone controller.

Topics in this chapter include:

- [Important Points to Remember on page 46](#)
- [MIB Files on page 48](#)
- [Syslog Files on page 48](#)
- [Memory Requirements on page 47](#)
- [Backing up Critical Data on page 48](#)
- [Upgrading ArubaOS on page 50](#)
- [Downgrading ArubaOS on page 53](#)
- [Before Calling Technical Support on page 55](#)

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 *Aruba Mobility Master Licensing Guide*.

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 the 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 file, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
 - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 48](#) 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 48](#) 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 48](#) 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 compact flash card. 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 the CLI.

In the WebUI

From the Mobility Master, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

In the CLI

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

MIB Files

To access ArubaOS MIB files:

1. Log in to the Aruba Support site.
2. Navigate to **Download Software > ArubaOS**.
3. Navigate to the desired release folder.
4. Download the MIB file corresponding to the release.
5. Uncompress the MIB file to a local directory.

Syslog Files

To generate syslog file:

1. Log in to CLI of Mobility Master.
2. Switch to config mode.
3. Configure the logging command. Example: `logging <ipv4addr> facility local0`. For additional information, see ArubaOS 8.4.0.0 Command-Line Interface Reference Guide.
4. Execute the `show logging` command. For additional information, see ArubaOS 8.4.0.0 Command-Line Interface Reference Guide.

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 Compact Flash file system, 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 backup 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 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 WebUI or CLI. Follow the below recommendations while upgrading:

- ArubaOS 8.4.0.0 supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for Mobility Master Virtual Appliance. If you have 4 network adapters on your ArubaOS 8.0.0.0 Mobility Master Virtual Appliance, you must remove one before upgrading to ArubaOS 8.4.0.0 to avoid upgrade failure. To remove a network adapter from ArubaOS 8.0.0.0 Mobility Master Virtual Appliance:



---

Before you remove the additional network adapter from the Mobility Master Virtual Appliance, ensure that you copy the ArubaOS 8.0.0.0 image on the system partition of Mobility Master Virtual Appliance.

---

1. Log in to the vSphere client.
  2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
  3. Click **Edit Virtual machine settings**.
  4. From the **Hardware** tab, select and remove a network adapter that is not active.
- Before upgrading to ArubaOS 8.4.0.0 from ArubaOS 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a Mobility Master Virtual Appliance or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
    1. From the **Managed Network** node hierarchy, select the managed device.
    2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
    3. Click **Submit**, and then click **Continue** in the reload popup.
    4. Click **Pending Changes**.
    5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Alternatively, you can execute the following CLI command on the Mobility Master at the device level:

```
(host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
```

- Before upgrading to ArubaOS 8.4.0.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

```
(host) [mm] (config) #license-pool-profile-root
(host) [mm] (License root(/) pool profile) #acr-license-enable
```



---

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see [Memory Requirements on page 47](#).

---



---

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 occurs 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 a TFTP server, FTP server, or local file:

1. Download the ArubaOS image from the customer support site.
2. Upload the new software 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** 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 the **Save Current Configuration**.
10. Click **Upgrade**.
11. Click **OK**, when **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 partitions. 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
```

## Verifying the ArubaOS Upgrade

Verify the upgrade using the WebUI or CLI.

### In the WebUI

Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the WebUI to verify all the managed devices are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.

3. Verify that the number of access points and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. 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 48](#) for information on creating a backup.

### In the CLI

Execute the **show version** command to verify the ArubaOS image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the CLI and verify that all your managed devices are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. 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 48](#) for information on creating a backup.

## Downgrading ArubaOS

If necessary, you can return to your previous version of ArubaOS.

### Pre-requisites

A Mobility Master or a managed device has two partitions, 0 and 1. If the upgrade fails on one of the partitions, you can reboot the Mobility Master or the managed device from the other partition. Before you reboot the Mobility Master or with the pre-upgrade ArubaOS version, you must perform the following steps:

1. Back up your Mobility Master or managed device. For details, see [Backing up Critical Data on page 48](#).
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 ArubaOS version and configuration files.

5. After switching the boot partition, perform the following steps:
  - 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 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/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, enter a file name (other than default.cfg).
  - c. Click **Copy**.
2. Determine the partition on which your previous ArubaOS version 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/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** option 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/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. You cannot load a new image into the active system partition (the default boot).

```
#show image version
```

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 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 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 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, if possible.