

ArubaOS 8.5.0.4



Release Notes

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
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Contents	3
Revision History	5
Release Overview	6
Important Points Before Upgrading to ArubaOS 8.5.0.0	6
Related Documents	7
Supported Browsers	7
Contacting Support	8
New Features and Enhancements	9
Supported Platforms	10
Mobility Master Platforms	10
Mobility Controller Platforms	10
AP Platforms	11
Regulatory Updates	13
Resolved Issues	14
Known Issues and Limitations	15
Upgrade Procedure	25
Important Points to Remember and Best Practices	25

Memory Requirements	26
Backing up Critical Data	27
Upgrading ArubaOS	28
Downgrading ArubaOS	31
Before Calling Technical Support	33

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	Removed the Migrating from ArubaOS 6.x to ArubaOS 8.x section from Upgrade Procedure chapter, and removed Migration Guide from the documents listed under Related Documents section, as the Migration Tool is no longer be supported.
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 10](#)
- [Regulatory Updates on page 13](#)
- [Resolved Issues on page 14](#)
- [Known Issues and Limitations on page 15](#)
- [Upgrade Procedure on page 25](#)

For the list of terms, refer [Glossary](#).

Important Points Before Upgrading to ArubaOS 8.5.0.0

DPI classification is not initialized after a controller is upgraded from ArubaOS 8.4.0.0, 8.4.0.1, or 8.4.0.2 to ArubaOS 8.5.0.0. The affected platforms are 7200 Series controllers.

An additional reboot of the affected platform is required to initialize DPI classification.

To check the status of DPI classification after upgrading an affected platform from ArubaOS 8.4.0.0, 8.4.0.1, or 8.4.0.2 to ArubaOS, 8.5.0.0, issue the **show firewall | include dpi** command. In the following example, DPI classification is disabled:

```
(host) #show firewall | include dpi
DPI Classification      Disabled [Cfg: enabled, PEF license: installed]
```

If DPI classification is enabled, further action is not needed. However, if DP classification is disabled, issue the **show datapath utilization** and check if the DPI classification CPUs are initialized. In the following example, the DPI classification CPUs are disabled:

```
(host) #show datapath utilization

Datapath CPU Allocation Summary
Slow Path (SP) : 1,  Slow Path Gateway (SPGW) : 1
Fast Path (FP) : 17,  Fast Path Gateway (FPGW) : 1
DPI : 0, Crypto (CRYP) : 0
Slow Path Spare (SPSPARE) : 0
```

If the DPI classification CPUs are not initialized, reboot the affected platform by:

- Issuing the **reload** command.
- Power cycling the controller.

Related Documents

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

- [ArubaOS Getting Started Guide](#)
- [ArubaOS User Guide](#)
- [ArubaOS CLI Reference Guide](#)
- [ArubaOS API Guide](#)
- [Aruba Mobility Master Licensing Guide](#)
- [Aruba Virtual Appliance Installation Guide](#)
- [Aruba AP Software Quick Start Guide](#)

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 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 8, 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 enhancements introduced in this release.

Dual Uplink for AP-318, 340 Series, 370 Series, 510 Series, 530 Series, and AP-555 Access Points

Starting from ArubaOS 8.5.0.3, AP-318, 340 Series, 370 Series, 510 Series, 530 Series, and AP-555 access points can be provisioned as Campus APs with both the Ethernet ports connected.

In versions prior to ArubaOS 8.5.0.3, deploying APs in controller-managed networks as a Campus AP introduced a broadcast storm into the network when both the Ethernet ports were connected to the same VLAN. This occurred during the master discovery phase under the following configuration conditions:

- Both eth0 and eth1 ports were connected to the uplink switch in the same VLAN.
- LACP was not configured on the upstream access ports.
- The AP models were AP-318, 340 Series, 370 Series, 510 Series, 530 Series, and AP-555 access points.

The workaround for this issue was to use a single uplink while provisioning the APs. The issue was resolved once the AP became controller-managed. However, the issue is likely to re-appear in APs shipped with versions prior to 8.5.0.3 if they return to their factory default state, although the AP was successfully deployed in a controller-managed network using a higher version of code.

Enhancements to Datapath

Starting from this release, new counters are added for quicker debugging when unsupported DHCP options are detected in datapath.

Limitation of 510 Series Campus Access Points

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

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 8.5.0.4*

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

Mobility Controller Platforms

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

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.5.0.4*

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

AP Platforms

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

Table 5: *Supported AP Platforms in ArubaOS 8.5.0.4*

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
303H Series	AP-303H

Table 5: Supported AP Platforms in ArubaOS 8.5.0.4

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

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_72670

This chapter describes the issues resolved in this release.



We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Table 6: Resolved Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188962	—	<p>Symptom: Session timeout was observed for few clients connected to APs. Enhancements to the wireless driver resolved this issue.</p> <p>Scenario: This issue was observed in APs running ArubaOS 8.5.0.0 or later versions.</p>	AP-Wireless	All platforms	ArubaOS 8.5.0.0
AOS-194419 AOS-194916 AOS-195339 AOS-195129 AOS-195945	—	<p>Symptom: A few clients connected to APs were unable to pass traffic intermittently for a certain period of time. Enhancements to the wireless driver resolved this issue.</p> <p>Scenario: This issue was observed in AP-535 access points running ArubaOS 8.5.0.1 or later versions.</p>	AP-Wireless	AP-535 access points	ArubaOS 8.5.0.1
AOS-195520	—	<p>Symptom: An AP displayed fake active period before it went into off-channel scanning that lead to packet loss. Enhancements to the wireless driver resolved this issue.</p> <p>Scenario: This issue was observed in AP-555 running ArubaOS 8.5.0.0 or later versions.</p>	AP-Wireless	AP-555 access points	ArubaOS 8.5.0.0

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



We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in ArubaOS 8.5.0.4*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-125897 AOS-189036	151952	Symptom: When a managed device reboots, APs and clients boot without IP addresses and other fields. Scenario: This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. Workaround: None.	Monitoring	All platforms	ArubaOS 8.0.1.0
AOS-131325 AOS-146748	159222 179137	Symptom: The number of clients displayed in the active-standby IP field on the Mobility Master dashboard is incorrect. Scenario: This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running ArubaOS 8.1.0.0 or later versions. Workaround: None.	Base OS Security	All platforms	ArubaOS 8.1.0.0
AOS-144684 AOS-184346	176339	Symptom: A few 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

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145410 AOS-146962	177352 179430	Symptom: A managed device crashes and reboots with the following error message: Atleast 2000 MB free flash is recommended to keep system stable. Please clean up your flash file. Scenario: This issue occurs when a managed device receives IP packets larger than one segment. This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions. Workaround: None.	Controller-Platform	All platforms	ArubaOS 8.2.0.2
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-151022 AOS-188417	185176	Symptom: The output of the show datapath uplink command displays incorrect session count. Scenario: This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. Workaround: None.	Controller-Datapath	All platforms	ArubaOS 8.1.0.0
AOS-151355	185602	Symptom: A few 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-151541 AOS-185425	185851	Symptom: An idle SSH login session to a managed device does not time out. Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.1. Workaround: None.	Base OS Security	All platforms	ArubaOS 8.2.1.1

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-152326 AOS-187297 AOS-187406 AOS-187549	186957	Symptom: The beacon displays the country code information intermittently for 5 GHz non-DFS channel. Scenario: This issue occurs when 802.11h is enabled in the radio profile. This issue is observed in 510 Series access points running ArubaOS 8.3.0.0 or later versions. Workaround: None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.2
AOS-153185	188148	Symptom: The Dashboard > Security > Active rogue > Locate option does not function in the WebUI. Scenario: This issue is observed in Mobility Masters running ArubaOS 8.3.0.1 or later versions. Workaround: None.	WebUI	All platforms	ArubaOS 8.3.0.1
AOS-155037	190571	Symptom: A Remote AP fails to boot up. Scenario: This issue occurs in a Remote AP with EST key type X9.62/SECG curve . This issue is observed in AP-303H access points running ArubaOS 8.3.0.3 or later versions. Workaround: None.	CPsec	AP-303H access points	ArubaOS 8.3.0.3
AOS-155801	191726	Symptom: SNMP walk performed from AirWave does not produce correct results. Scenario: This issue is observed in managed devices running ArubaOS 8.3.0.3. Workaround: None.	SNMP	All platforms	ArubaOS 8.3.0.3
AOS-156085 AOS-157704	192119 194393	Symptom: A few 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-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 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157008	193358	<p>Symptom: The output of the show ap bss table command displays incorrect MTU value for a Remote AP.</p> <p>Scenario: This issue occurs when the default value of the rap-gre-mtu parameter under the ap system-profile <profile_name> command is changed to a new value. This issue is observed in APs running ArubaOS 8.2.0.0 or later versions.</p> <p>Workaround: None.</p>	AP-Platform	All platforms	ArubaOS 8.3.0.0
AOS-157011	193362	<p>Symptom: The output of show datapath papi counters command displays invalid tunnel endpoint information.</p> <p>Scenario: This issue is observed in Mobility Masters running ArubaOS 8.3.0.3.</p> <p>Workaround: None.</p>	Controller-Datapath	All platforms	ArubaOS 8.3.0.3
AOS-157492	194064	<p>Symptom: VRRP authentication fails in a managed device.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.2.1.0.</p> <p>Workaround: None.</p>	VRRP	All platforms	ArubaOS 8.2.1.0
AOS-157795	194516	<p>Symptom: A few managed devices are unable to process two APN usb-init string using the uplink cellular apn command with Huawei E3372 modem.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.3.0.6.</p> <p>Workaround: None.</p>	Controller-Platform	All platforms	ArubaOS 8.3.0.6
AOS-182073 AOS-183743	—	<p>Symptom: An 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.</p> <p>Scenario: This issue is observed in AP-315 access points running ArubaOS 8.3.0.5.</p> <p>Workaround: None.</p>	IPsec	AP-315 access points	ArubaOS 8.3.0.5

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-182847	—	<p>Symptom: A few users are unable to copy the WPA Passphrase field and High-throughput profile to a new SSID profile in the Configuration > System > Profiles > Wireless LAN > SSID > <SSID_Profile> option of the WebUI.</p> <p>Scenario: This issue occurs when a new SSID profile is created from an existing SSID profile in the WebUI. This issue is observed in managed devices running ArubaOS 8.4.0.0 in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	WebUI	All platforms	ArubaOS 8.4.0.0
AOS-183998 AOS-183999	—	<p>Symptom: A few users are unable to configure the PPPoE password when they provision a Remote AP in the Configuration > Access Points > Remote APs page of the WebUI.</p> <p>Scenario: This issue occurs because the Retype password field for PPPoE is missing from the Uplink option in the provisioning page of the WebUI. This issue is observed in Remote APs running ArubaOS 8.3.0.6.</p> <p>Workaround: None.</p>	WebUI	All platforms	ArubaOS 8.3.0.6
AOS-184135	—	<p>Symptom: A few users are unable to download applications from Google Play Store.</p> <p>Scenario: This issue occurs when the YouTube application is blocked. This issue is observed in stand-alone controllers running ArubaOS 8.4.0.0.</p> <p>Workaround: None.</p>	Controller-Datapath	All platforms	ArubaOS 8.4.0.0
AOS-184801	—	<p>Symptom: A few managed devices crash and reboot unexpectedly. The log files list the reason for the event as Datapath exception.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.0.</p> <p>Workaround: None.</p>	Controller - Datapath	All platforms	ArubaOS 8.4.0.0
AOS-184977 AOS-188242 AOS-188378	—	<p>Symptom: The output of basic commands such as show version, show clock, and show image version are unable to display any information and the default gateway details are missing in a managed device.</p> <p>Scenario: This issue occurs when the /tmp directory runs out of memory because of too many logs from the Policy Manager. This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	Routing	All platforms	ArubaOS 8.4.0.0

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185103	—	<p>Symptom: The Outstanding Requests parameter value is incremented unexpectedly in the output of the show aaa authentication-server radius statistics command.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.5.0.0 or later versions with EAP fragmentation enabled.</p> <p>Workaround: Restart the 802.1x process by issuing the following two commands:</p> <ul style="list-style-type: none"> ■ show processes include dot1x ■ process restart dot1x1 	802.1x	All platforms	ArubaOS 8.5.0.1
AOS-186133	—	<p>Symptom: A few managed devices display abnormally high multicast traffic in Performance Summary > All Radios 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-186303	—	<p>Symptom: A few Remote APs reboot unexpectedly. The log file lists the reason for the event as kernel panic: Fatal exception on PC is at netdev_run_todo+0x290/0x2b4.</p> <p>Scenario: This issue is observed in AP-305 access points running ArubaOS 8.4.0.2 or later versions.</p> <p>Workaround: None.</p>	RAP+BOAP	AP-305 access points	ArubaOS 8.4.0.2
AOS-186411	—	<p>Symptom: Users are unable to remove a VLAN from port channel trunk.</p> <p>Scenario: This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.</p> <p>Workaround: Execute the switchport trunk allowed vlan 1-4094 command to add the allowed VLAN range (1-4094). Then, execute the switchport trunk allowed vlan remove 259 command to remove the VLAN from the port channel trunk.</p>	Interface	All platforms	ArubaOS 8.3.0.0
AOS-186860	—	<p>Symptom: RADIUS authentication requests are sent in IP address of the managed device although they are configured to go through the loopback IP.</p> <p>Scenario: This issue is observed in managed devices running ArubaOS 8.4.0.1.</p> <p>Workaround: None.</p>	IPsec	All platforms	ArubaOS 8.4.0.1

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187114	—	<p>Symptom: The Pending Changes window displays additional changes when the user configures a new policy rule under Configuration > Roles & Policies > Policies window in the WebUI.</p> <p>Scenario: This issue is observed when the user configures a new rule for an existing policy under the Policies window and clicks the Submit button. This issue is observed in Mobility Masters running ArubaOS 8.3.0.4.</p> <p>Workaround: None.</p>	WebUI	All platforms	ArubaOS 8.3.0.4
AOS-187395 AOS-188564	—	<p>Symptom: The AAA test to the external server fails in the Diagnostics > Tools > AAA Server Test page of the WebUI.</p> <p>Scenario: This issue occurs when the user enters the ", %, and # special characters in the Password field and clicks the Test option. As a result, the WebUI displays the Authentication field as failed and Processing time (ms) field as N/A. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions.</p> <p>Workaround: None.</p>	WebUI	All platforms	ArubaOS 8.4.0.2
AOS-187422 AOS-189258	—	<p>Symptom: The output of show log all and show audit-trail commands displays the unencrypted password entered for non-profile commands such as aaa test-server command.</p> <p>Scenario: This issue is observed in a Mobility Master Virtual Appliance running ArubaOS 8.3.0.5.</p> <p>Workaround: None.</p>	Configuration	All platforms	ArubaOS 8.3.0.5
AOS-187479 AOS-188428	—	<p>Symptom: The authentication server configuration details are not forwarded from the primary Mobility Master to the secondary Mobility Master in Layer-3 redundancy configuration.</p> <p>Scenario: This issue is observed in a Mobility Master Virtual Appliance running ArubaOS 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	Configuration	All platforms	ArubaOS 8.4.0.2
AOS-187510	—	<p>Symptom: A managed device crashes and reboots unexpectedly.</p> <p>Scenario: This issue occurs when the 802.1X processes crash after a cluster live upgrade on the managed device. This issue is observed in managed devices running ArubaOS 8.4.0.2 or later versions in a cluster setup.</p> <p>Workaround: None.</p>	802.1X	All platforms	ArubaOS 8.4.0.2

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187820	—	<p>Symptom: The output of the show cpuload per-cpu command displays the same CPU load statistics for each processor.</p> <p>Scenario: This issue occurs after reboot of the controller. This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions.</p> <p>Workaround: None.</p>	Controller-Platform	All platforms	ArubaOS 8.4.0.0
AOS-187911	—	<p>Symptom: The Wireless Clients section of the Dashboard > Overview page in the WebUI displays incorrect client usage values.</p> <p>Scenario: This issue is observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions.</p> <p>Workaround: Add a tooltip over the usage tab to mention that the current client usage value accounts for the last 15 min.</p>	WebUI	All platforms	ArubaOS 8.4.0.0
AOS-188199	—	<p>Symptom: A few clients are unable to connect to a controller in Aruba Central because the ClearPass Policy Manager rejects the client authentication request.</p> <p>Scenario: This issue occurs when the branch gateway sends NAD-IP address or NAS-IP address as public IP address. This issue is observed in 7008 controllers running ArubaOS 8.4.0.0.</p> <p>Workaround: None.</p>	Base OS Security	7008 controllers	ArubaOS 8.4.0.0
AOS-188467	—	<p>Symptom: The AMON messages from a peer cluster display wrong value for cl_cluster_incompatible_reason.</p> <p>Scenario: This issue occurs when the incompatible reason is not reset after an incompatibility with a peer cluster member is resolved and the cluster is re-formed. This issue is observed in managed devices running ArubaOS 8.3.0.6 in a cluster topology.</p> <p>Workaround: None.</p>	Cluster Manager	All platforms	ArubaOS 8.3.0.6
AOS-188470	—	<p>Symptom: PPPoE does not work when a Remote AP is provisioned using ZTP and the Either ping is disabled on AP's uplink router or there are issues with AP's uplink connectivity error is displayed.</p> <p>Scenario: This issue is observed in AP-203R access points running ArubaOS 8.2.1.1 or later versions.</p> <p>Workaround: None.</p>	RAP+BOAP	AP-203R access points	ArubaOS 8.2.1.1

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188478	—	<p>Symptom: The Remote AP whitelist file does not contain the first MAC address entry.</p> <p>Scenario: This issue occurs when the user runs the show whitelist-db rap export-css <filename> command to export the Remote AP whitelist file to the controller directory. This issue is observed in standalone controllers running ArubaOS 8.3.0.5 or later versions.</p> <p>Workaround: None.</p>	Local Database	All platforms	ArubaOS 8.3.0.5
AOS-188485	—	<p>Symptom: The <code><ofald 237504> <ERRS> AP 32438@172.16.4.151 ofald sdn ERRS ofald_datapath_msg_rcv_cb:274 Invalid message type 126</code> error message is displayed every second in APs.</p> <p>Scenario: This issue is observed in APs running ArubaOS 8.4.0.0-FIPS in a Mobility Master-Managed Device topology.</p> <p>Workaround: None.</p>	SDN	All platforms	ArubaOS 8.4.0.0
AOS-189194	—	<p>Symptom: The 5 GHz and 2.4 GHz antenna values are swapped after AP provisioning rules configuration is committed in the Configuration > Access Points > Provisioning Rules page of the WebUI.</p> <p>Scenario: This issue occurs when the user selects the Set Antenna Gain for Dual Band mode option from the Actions drop-down list in the Configuration > Access Points > Provisioning Rules page, and enters the 5 GHz and 2.4 GHz field values in the WebUI. This issue is observed in Mobility Master Virtual Appliances running ArubaOS 8.4.0.3 or later versions.</p> <p>Workaround: None.</p>	WebUI	All platforms	ArubaOS 8.5.0.0

Table 7: Known Issues in ArubaOS 8.5.0.4

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189471	—	<p>Symptom: A few clients are unable to connect to APs that are configured with LACP and have allowed band of 5 GHz.</p> <p>Scenario: This issue is observed in AP-335 access points running ArubaOS 8.5.0.0.</p> <p>Workaround: None.</p>	AP Datapath	AP-335 access points	ArubaOS 8.5.0.0
AOS-189721	—	<p>Symptom: The Datapath process crashes in a controller. The log files list the reason for the event as Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4).</p> <p>Scenario: This issue is observed in 7210 controllers running ArubaOS 8.4.0.2 or later versions.</p> <p>Workaround: None.</p>	Controller-Datapath	7210 controllers	ArubaOS 8.4.0.2
AOS-190071 AOS-190372	—	<p>Symptom: A few users are unable to access the websites when WebCC is enabled on the user role.</p> <p>Scenario: This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in 7005 controllers running ArubaOS 8.4.0.0.</p> <p>Workaround:</p> <ul style="list-style-type: none"> ■ Remove web category from the ACL rules and apply any any any permit policy. ■ Disable WebCC on the user role. ■ Change the VLAN of user role from trunk mode to access mode. 	WebCC	7005 controllers	ArubaOS 8.4.0.0

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



CAUTION

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

Topics in this chapter include:

- [Important Points to Remember and Best Practices on page 25](#)
- [Memory Requirements on page 26](#)
- [Backing up Critical Data on page 27](#)
- [Upgrading ArubaOS on page 28](#)
- [Downgrading ArubaOS on page 31](#)
- [Before Calling Technical Support on page 33](#)

Important Points to Remember and Best Practices

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** section of 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 the 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 requirement:

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your 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 27](#) 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 27](#) 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 file:** 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 27](#) to copy the **logs.tar** files to an external server. Execute the **tar clean logs** command to delete the file from the managed device.



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

Deleting a File

You can delete a file using the WebUI or 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.

In the CLI

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

Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Logs
- Flashbackup

Backing up and Restoring Flash Memory

You can backup and restore flash using the WebUI or the 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 back up the contents of the flash memory to the **flashbackup.tar.gz** file.

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

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

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

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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.



CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see [Memory Requirements on page 26](#).



NOTE

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message 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 from 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 **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.



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

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

In the CLI

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

1. Download 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 if 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 [Memory Requirements on page 26](#) 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 to 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 27](#) for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see [Backing up Critical Data on page 27](#).
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved ArubaOS configuration file.
4. Set the Mobility Master or managed device to boot from the system partition that contains the pre-upgrade ArubaOS version.
When you specify a boot partition or copy an image file to a system partition, Mobility Master or managed device checks if the ArubaOS version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the ArubaOS version and configuration files.
5. After switching the boot partition, perform the following steps:
 - Restore 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 or TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
 - a. From the **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 the **Select destination file** drop-down list, enter a file name (other than default.cfg).
 - c. Click **Copy**.

- Determine the partition on which your pre-upgrade ArubaOS version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade ArubaOS version is not stored on your system partition, load it into the backup system partition by performing the following steps:



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

- Enter the FTP or TFTP server address and image file name.
 - Select the backup system partition.
 - Enable **Reboot controller after upgrade**.
 - Click **Upgrade**.
- 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.
 - 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 section describes how to downgrade the ArubaOS version.

- If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

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

or

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

- Set the controller to boot with your pre-upgrade configuration file.

```
(host) # boot config-file <backup configuration filename>
```
- 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
```
- Set the backup system partition as the new boot partition.

```
(host) # boot system partition 1
```
- Reboot the Mobility Master or managed device.

```
(host) # reload
```
- 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 any recent network changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with IP addresses and Interface numbers.
- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem 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.