ArubaOS 8.5.0.1

aruba
a Hewlett Packard
Enterprise company

Release Notes

Open Source Code

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

Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 08	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 07	Updated the links in the **Related Documents** section.
Revision 06	Added **AOS-185103** under **Known Issues** section.
Revision 05	Added **AOS-186076** under **Known Issues** section.
Revision 04	Added a limitation regarding 510 Series access points in the **Features** section.
Revision 03	Removed **AOS-154581** from **Known Issues** section.
Revision 02	Added **AOS-190241** under **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.

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.

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 8.5.0.1*

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 8.5.0.1*

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 8.5.0.1*

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 8.5.0.1*

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

Chapter 4
Regulatory Updates

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_71313

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 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-135373 AOS-158456	164342 195462	**Symptom:** Clients connected to an AP were deauthenticated. The log files listed the reason for the event as **Denied; AP Disable Timerange active**. This issue is resolved by configuring the correct **timerange** parameters. **Scenario:** This issue was observed in 100 Series access points running ArubaOS 8.5.0.0 or later versions.	Base OS Security	100 Series access points	ArubaOS 8.5.0.0
AOS-147018 AOS-186071	179516	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: softlockup: hung tasks**. Enhancements to the wireless driver resolved this 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-148642 AOS-156454 AOS-158502 AOS-158515	182031 192618 195518 195534	**Symptom:** The **Postgres** process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in 7210 controllers running ArubaOS 8.5.0.0 or later versions.	Logging	7210 controllers	ArubaOS 8.5.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-152750 AOS-186035	187572	**Symptom:** A few managed devices sent OSPF LSA with '00' in LSA checksum field which caused the upstream routers to log OSPF errors. With the fix, the managed devices send OSPF LSA with calculated checksum. **Scenario:** This issue occurred when the managed device established OSPF neighbor relationship with routers other than Aruba routers. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	OSPF	All platforms	ArubaOS 8.3.0.0
AOS-155127 AOS-185571 AOS-186648	190702	**Symptom:** Users were unable to access the login page during captive portal authentication on the managed device. The fix ensures that the captive portal authentication login page is displayed. **Scenario:** This issue occurred when AP datapath sent HTTP requests to the AAC instead of the UAC in Split-Tunnel forwarding mode. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions in a cluster setup.	AP-Platform	All platforms	ArubaOS 8.3.0.0
AOS-155570 AOS-182455	191405	**Symptom:** A managed device displayed the **Country Code file creation failed** error message while saving the configuration. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred during the initial setup of the managed device when the user created the country_code file in a directory that did not exist. This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.4.0.0
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 clients are 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

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157823 AOS-185568	194561	**Symptom:** Few 802.1X clients were displayed with an IP address instead of a user name in the **Managed Network > Dashboard > Overview > Clients** page of the WebUI. The fix ensures that the correct information about the 802.1X clients are displayed in the WebUI. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.3.0.3 or later versions.	Base OS Security	All platforms	ArubaOS 8.3.0.3
AOS-181925	195713	**Symptom:** The **Dashboard > Access Points** page of the Mobility Master WebUI did not display updated information of an AP that is displayed as UP on the managed device. The fix ensures that the correct information of the AP is displayed on the Mobility Master WebUI. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.	WebUI	All platforms	ArubaOS 8.2.1.1
AOS-182294	—	**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. **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.	IPsec	All platforms	ArubaOS 8.2.2.3
AOS-182549	—	**Symptom:** The AP in an IAP-VPN configuration is assigned an IP address that is the inverse of an IP address configured in the **lc-rap-pool** in the Mobility Master. The fix ensures that the AP is assigned a valid IP address from the address pool. **Scenario:** This issue is observed in APs running ArubaOS 8.3.0.5 or later versions.	CPsec	All platforms	ArubaOS 8.3.0.5
AOS-183244 AOS-185673	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **FW assert at tbd.c:39**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred while enabling or disabling 802.11k profile. This issue was observed in AP-535 access points running ArubaOS 8.5.0.0.	AP-Wireless	AP-535 access points	ArubaOS 8.5.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183251	—	**Symptom:** The usage graph for individual APs was not updated on the AirWave server. The fix ensures that the usage graph is updated on the AirWave server. **Scenario:** This issue was observed in AP-225 and AP-325 access points running ArubaOS 8.3.0.0 or later versions.	Controller-Datapath	AP-225 and AP-325 access points	ArubaOS 8.3.0.0
AOS-183723 AOS-187678	—	**Symptom:** The SSL handshake for POST failed for clients performing captive portal authentication on a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when TLS 1.2 was enabled in Web Server profile within the SSL protocol. This issue was observed in managed devices running ArubaOS 8.2.0.0-FIPS or later versions in a Mobility Master-Managed Device topology.	Web Server	All platforms	ArubaOS 8.2.0.0
AOS-184269 AOS-186423	—	**Symptom:** A few APs were unable to join a cluster and rebooted with the **unable to contact switch: HELLO-TIMEOUT** error message. The fix ensures that the APs are able to join the cluster. **Scenario:** This issue occurred when the cluster leader received a Deactivate event from DDS of a different managed device that was a previous leader. This issue was observed in managed devices running ArubaOS 8.3.0.6.	Cluster-Manager	All platforms	ArubaOS 8.3.0.6
AOS-184289	—	**Symptom:** SNMP traps or syslog error messages were not generated when the VLAN probe failed on the managed device. The fix ensures that syslog messages are generated as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.2.0 or later versions in a cluster setup.	Cluster-Manager	All platforms	ArubaOS 8.2.2.0
AOS-184432	—	**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. **Scenario:** This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184441	—	**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. **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.	Controller-Platform	All platforms	ArubaOS 8.3.0.4
AOS-184787	—	**Symptom:** The **Authentication** process crashed in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to memory corruption. This issue was observed in 7240 and 7240XM controllers running ArubaOS 8.2.0.0 or later versions.	Base OS Security	7240 and 7240XM controllers	ArubaOS 8.2.0.0
AOS-184851 AOS-187529	—	**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. **Scenario:** This issue occurred when HTTP requests larger than 8k were processed, which led to a segmentation fault. This issue was observed in 7280 controllers running ArubaOS 8.4.0.0 or later versions.	Captive Portal	7280 controllers	ArubaOS 8.4.0.0
AOS-185089	—	**Symptom:** Users were unable to setup an IPsec tunnel because Mobility Masters were using port 500 instead of port 4500 to form L3 redundancy. The fix ensures that the IKE connection initiates on port 4500. **Scenario:** This issue occurred as IKE started negotiating on port 500. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0.	Master-Redundancy	All platforms	ArubaOS 8.3.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185127 AOS-187183	—	**Symptom:** The **CFGM** process in a Mobility Master stopped responding and went into **PROCESS_NOT_RESPONDING_ CRITICAL** state. As a result, the output of the **show switches** command displayed the **Module Configuration Manager is busy. Please try later** error message. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions.	Configuration	All platforms	ArubaOS 8.5.0.0
AOS-185202	—	**Symptom:** A few APs were unable to join a cluster and some of the AP's Cluster AAC Assignment data entries became dormant on the cluster leader. The fix ensures that the APs are able to join the cluster. **Scenario:** This issue occurred when the cluster leader received Deactivate event from DDS of a different managed device that was a previous leader. This issue was observed in managed devices running ArubaOS 8.3.0.6 or later versions.	DDS	All platforms	ArubaOS 8.3.0.6
AOS-185233 AOS-185696 AOS-186796	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 530 Series and 550 Series access points running ArubaOS 8.5.0.0 or later versions.	AP-Wireless	530 Series and 550 Series access points	ArubaOS 8.5.0.0
AOS-185259	—	**Symptom:** All radios displayed poor channel quality under **Dashboard > Overview > Radios > CHANNEL QUALITY** column. The fix ensures that the channel quality is displayed as **Good** or **Excellent**. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.0 or later versions.	Station Management	All platforms	ArubaOS 8.5.0.0
AOS-185597	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **WLAN FW exception at wal_ba_tx_sm()**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-555 and 530 Series access points running ArubaOS 8.5.0.0 or later versions.	AP-Wireless	AP-555 and 530 Series access points	ArubaOS 8.5.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185932	—	**Symptom:** A few clients deleted block acknowledge agreement leading to ping timeouts. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred randomly when clients were still connected. On re-negotiation, the traffic resumed normally. This issue was observed in 550 Series access points running ArubaOS 8.5.0.0.	AP-Wireless	550 Series access points	ArubaOS 8.5.0.0
AOS-185937	—	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **whal_recv_recovery.c:606 Assertion RX_ HW_WDOG_HANG failedparam0 :zero, param1 :zero, param2 :zero**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-555 and 530 Series access points running ArubaOS 8.5.0.0 or later versions.	AP-Wireless	AP-555 and 530 Series access points	ArubaOS 8.5.0.0
AOS-186095	—	**Symptom:** A few APs lost association and reconnected back immediately. Enhancements to the wireless resolved this issue. **Scenario:** This issue occurred due to a beacon drift. This issue was observed in 530 Series and 550 Series access points running ArubaOS 8.5.0.0 or later versions.	AP-Wireless	530 Series and 550 Series access points	ArubaOS 8.5.0.0
AOS-186111	—	**Symptom:** The price update of ESLs failed unexpectedly. This issue is resolved by optimizing the **COEX** method between WiFi radio and ESL radio. **Scenario:** This issue occurred when the SES-imagotag's Electronic Shelf Label (ESL) system stopped responding after running for a long time. This issue was observed in 300 Series, 303H Series, 310 Series, 320 Series, 330 Series, 340 Series, and 510 Series access points running ArubaOS 8.4.0.0 or later versions.	AP-Platform	300 Series, 303H Series, 310 Series, 320 Series, 330 Series, 340 Series, and 510 Series access points	ArubaOS 8.4.0.0
AOS-186113	—	**Symptom:** A few mesh wired APs did not work as expected. The fix ensures that the mesh wired APs work in bridge trunk mode. **Scenario:** This issue occurred when the DHCP packet had a VLAN tag. This issue was observed in APs running ArubaOS 8.4.0.0 or later versions.	Mesh	All platforms	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186233 AOS-186360	—	**Symptom:** The **Authentication** module in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions in a Mobility Master-Managed Device topology.	802.1X	All platforms	ArubaOS 8.4.0.0
AOS-186304	—	**Symptom:** Users were unable to connect to the Remote AP over IPv6 network in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred because the AP was waiting to receive AP regulatory domain information from the managed device. This issue was observed in managed devices running ArubaOS 8.3.0.6.	IPv6	All platforms	ArubaOS 8.3.0.6
AOS-186388	—	**Symptom:** A few clients were unable to connect to 5 GHz channel of APs. The fix ensures that the clients are able to connect to the APs. **Scenario:** This issue occurred during high availability deployment of APs. This issue was observed in AP-325 access points running ArubaOS 8.3.0.0 or later versions.	AP Datapath	AP-325 access points	ArubaOS 8.3.0.0
AOS-186422	—	**Symptom:** Clients were unable to obtain IP addresses from APs. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when the clients were connected to APs with tunnel forwarding mode. This issue was observed in AP-205 and AP-303 access points running ArubaOS 8.3.0.1 or later versions.	Controller-Datapath	AP-205 and AP-303 access points	ArubaOS 8.3.0.1
AOS-186614	—	**Symptom:** A managed device stopped responding unexpectedly due to packet drop. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred because of FTP traffic when DPI was enabled. This issue was observed in managed devices running ArubaOS 8.2.2.3 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.2.3

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186667	—	**Symptom:** Clients were unable to associate to AP because the AP stopped beaconing. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in 100 Series, 110 Series, and 130 Series access points running ArubaOS 8.3.0.0.	AP-Wireless	100 Series, 110 Series, and 130 Series access points	ArubaOS 8.3.0.0
AOS-187087	—	**Symptom:** A few APs rebooted frequently. The log files listed the reason for the event as **BUGFailureAt:net/core/skbuff.c:1609/consume_skb()! Warmreset**. Enhancements to the wireless driver resolved this issue. **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.	AP-Wireless	510 Series access points	ArubaOS 8.3.0.0
AOS-187113 AOS-187451	—	**Symptom:** A few APs used 40MHz channels on 2.4 GHz instead of 20 MHz. The fix ensures that the channel is switched back to 20 Mhz. **Scenario:** This issue occurred because in 2.4 GHz, the channels were always scanned in 40 MHz but if the scan channel and home channel shared the same control channel, the channel was switched back to the configured channel after scan. This issue was observed in 510 Series access points running ArubaOS 8.4.0.0.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-187331 AOS-188142	—	**Symptom:** An AP was unable to detect the nearby AP list. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-515 access points running ArubaOS 8.4.0.0 or later versions.	AP-Wireless	AP-515 access points	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187361	—	**Symptom:** The **LMS preemption** process failed when NAT was applied to the primary LMS IP address. The fix ensures that the LMS preemption failure does not occur when NAT is applied to the primary LMS IP address. **Scenario:** This issue was observed in APs running ArubaOS 8.5.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.5.0.0
AOS-187750	—	**Symptom:** A few 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. **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.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
AOS-188141 AOS-188641	—	**Symptom:** A few clients faced connectivity issues when they did not receive DHCP packets in an Open SSID or EAPOL packets in 802.1X SSID. The fix ensures that the clients are able to connect to the network. **Scenario:** This issue occurred due to a mismatch between tunnel IDs and virtual AP interface within the AP datapath. This issue was observed in AP-535 and AP-555 access points running ArubaOS 8.5.0.0 or later versions in a cluster setup.	AP Datapath	AP-535 and 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 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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
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-146118	178291	**Symptom:** The **dir** CLI 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 8.2.1.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.1.0

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-149543	183200	**Symptom:** During upgrade process, the image files are left on the flash drive and the user is unable to upgrade the ArubaOS image. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.0.0
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
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-154809	190272	**Symptom:** PPPoE does not work on a Remote AP. **Scenario:** This issue occurs when provisioning a remote AP using zero touch provisioning. This issue is observed in APs running ArubaOS 8.2.1.1. **Workaround:** None.	Remote AP	All platforms	ArubaOS 8.2.1.1
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

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155114	190678	**Symptom:** A user role under an ACL does not work as any other session ACL. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0
AOS-155780	191686	**Symptom:** A VIA client does not connect to a VIA server. **Scenario:** This issue occurs when the VIA client is wirelessly connected to the same managed device on which the VIA VPN terminates. This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.4.0.0
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-156727 AOS-156728 AOS-156834 AOS-158306	193015 193016 193152 195249	**Symptom:** The Cluster manager process crashes in a managed device unexpectedly. The log files lists the reason for the event as **Module Cluster Manager Process is busy. Please try later**. **Scenario:** This issue occurs because the lc-cluster exclude VLAN string has more than 256 characters, which results in memory corruption. This issue is observed in managed devices running ArubaOS 8.2.2.0 or later versions in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.2.2.0
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 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
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-157492	194064	**Symptom:** VRRP authentication fails in a managed device. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0. **Workaround:** None.	VRRP	All platforms	ArubaOS 8.2.1.0
AOS-157795	194516	**Symptom:** A few managed devices are unable to process two **APN usb-init** string using the **uplink cellular apn** command with Huawei E3372 modem. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.6. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.3.0.6
AOS-158656	195704	**Symptom:** The password in the Active configuration is displayed in cleartext in the log files when the **show log all | include phonehome** command is executed. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.6. **Workaround:** None.	Logging	All platforms	ArubaOS 8.3.0.6
AOS-182073 AOS-183743	—	**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**. **Scenario:** This issue is observed in AP-315 access points running ArubaOS 8.3.0.5. **Workaround:** None.	IPsec	AP-315 access points	ArubaOS 8.3.0.5

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183656	—	**Symptom:** The WebUI displays incorrect AP count in the **Dashboard > Performance > Access Points** page. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.3.0.0
AOS-183883 AOS-183989	—	**Symptom:** The output of the **show ap database long** command displays the AP status as **Inactive** and **Dirty** when the managed device receives AP_READY message from AP through unsecured port 8211. **Scenario:** This issue occurs after an AP reboots but the IP address of the managed device and LMS-IP address of the AP are different. The AP entry in PAPI table is removed when the AP is redirected from one interface to another within the same managed device. As a result, the PAPI packets move to unsecured port 8211 instead of secure port 8209. This issue is observed in managed devices running ArubaOS 8.3.0.5 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.5
AOS-184051	—	**Symptom:** A Mobility Master keeps sending NTP sync packets every 15 seconds to the 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-184135	—	**Symptom:** A few users are unable to download applications from Google Play Store. **Scenario:** This issue occurs when the YouTube application is blocked. This issue is observed in stand-alone controllers running ArubaOS 8.4.0.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.4.0.0
AOS-184288 AOS-188218	—	**Symptom:** The OpenFlow profile is enabled automatically in a managed device immediately after upgrade of the managed device. **Scenario:** This issue occurs when OpenFlow is disabled on the managed device prior to its upgrade. This issue is observed in managed devices running ArubaOS 8.3.0.6 or later versions. **Workaround:** After the upgrade, verify and configure the OpenFlow state on Mobility Master and managed devices.	SDN	All platforms	ArubaOS 8.3.0.6

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184519	—	**Symptom:** A 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-184707 AOS-185647	—	**Symptom:** A few Remote APs fail to come up on the managed device after reboot of the APs, and are getting the same inner IP which has already been assigned to other Remote APs. **Scenario:** This issue occurs because most of the remote AP whitelist database entries are removed from the Mobility Master. This issue is observed in APs running ArubaOS 8.2.1.0 or later versions. **Workaround:** Purge the RAP whitelist database entries on Mobility Master and managed device and add them again. However, this will reboot the Remote APs and can cause network disruption.	CPsec	All platforms	ArubaOS 8.2.1.0
AOS-184801	—	**Symptom:** A few managed devices crash and reboot unexpectedly. The log files list 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-184977 AOS-188242 AOS-188378	—	**Symptom:** The output of the 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. **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. **Workaround:** None.	Routing	All platforms	ArubaOS 8.4.0.0

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185103	—	**Symptom:** The **Outstanding Requests** parameter value is incremented unexpectedly in the output of the **show aaa authentication-server radius statistics** command. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.0 or later versions with EAP fragmentation enabled. **Workaround:** Restart the **802.1x** process by issuing the following two commands: ■ **show processes | include dot1x** ■ **process restart dot1x1**	802.1x	All platforms	ArubaOS 8.5.0.1
AOS-185500 AOS-186325 AOS-188413	—	**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-186076 AOS-187884 AOS-189850 AOS-191866 AOS-192310 AOS-193177 AOS-193387	—	**Symptom:** The **STM** process crashes unexpectedly in a managed device in a cluster setup. **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 8.5.0.0 or later versions. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.5.0.0
AOS-186133	—	**Symptom:** A few managed devices display abnormally high multicast traffic in **Performance Summary > All Radios** monitoring page. **Scenario:** This issue is observed in 320 Series access points running ArubaOS 8.3.0.6. **Workaround:** None.	AP-Wireless	320 Series access points	ArubaOS 8.3.0.6
AOS-186160	—	**Symptom:** A few users are unable to move the managed device with LACP port configuration to the new node path. The log files lists the reason for the event as **Illegal Operation: Interface belongs to lacp group**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.2.4 or later versions. **Workaround:** Before moving the device, ■ remove LACP configuration from the Gigabit Ethernet port. ■ configure jumbo frame support by using the **firewall jumbo** global command in the new group.	Interface	All platforms	ArubaOS 8.2.2.4

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186207	—	**Symptom:** The **Unexpected HCM runtime error at hcm_gsm_update_section_ip_probe 167 Failed to update section for probe IP 10.120.128.1 src_intf 0 probe default, error error_htbl_key_not_found** error message is displayed in the log file of a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.1 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.4.0.1
AOS-186411	—	**Symptom:** A few users are unable to remove a VLAN from port channel trunk. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. **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.	Interface	All platforms	ArubaOS 8.3.0.0
AOS-186526	—	**Symptom:** The **profmgr** process in a Mobility Master crashes unexpectedly. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.4.0.0
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:** The **Acct-Authentic radius** attribute is not sent from the managed device. **Scenario:** This issue occurs when the managed devices are upgraded to ArubaOS 8.4.0.2. This issue is observed in managed devices running ArubaOS 8.4.0.1. **Workaround:** None.	Radius	All platforms	ArubaOS 8.4.0.1

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186979	—	**Symptom:** A few 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 is observed in Mobility Masters running ArubaOS 8.2.2.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.2.2.0
AOS-187510	—	**Symptom:** A managed device crashes and reboots unexpectedly. **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. **Workaround:** None.	802.1X	All platforms	ArubaOS 8.4.0.2
AOS-187820	—	**Symptom:** The output of the **show cpuload per-cpu** command displays the same CPU load statistics for each processor. **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. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.4.0.0
AOS-187911	—	**Symptom:** The **Wireless Clients** section of the **Dashboard > Overview** page in the WebUI displays incorrect client usage values. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions. **Workaround:** Add a tooltip over the usage tab to mention that the current client usage value accounts for the last 15 min.	WebUI	All platforms	ArubaOS 8.4.0.0

Table 7: *Known Issues in ArubaOS 8.5.0.1*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188170	—	**Symptom:** The Common Name of CP certificate is changed from **mc.ggnet.umn.edu** to **securelogin.arubanetworks.com** after upgrade of the managed device. **Scenario:** This issue occurs because of expired switch certificates. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions. **Workaround:** Replace the expired switch certificate with captive portal certificate. Then, save the configuration changes and replace again with custom certificates.	Certificate Manager	All platforms	ArubaOS 8.3.0.7
AOS-189227	—	**Symptom:** The **datapath** process in a Virtual Mobility Controller crashes unexpectedly when the Remote APs with wired users connected fail over to Backup LMS IP. **Scenario:** This issue occurs when the wired user VLAN is same as the controller VLAN of the Virtual Mobility Controller. This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.5.0.0 or later versions. **Workaround:** Ensure that the wired user VLAN and controller VLAN of the Virtual Mobility Controller are configured with different values.	Controller-Datapath	All platforms	ArubaOS 8.5.0.0
AOS-189604	—	**Symptom:** A few APs with CPsec enabled are not responding and are stuck with **D** flag (dirty mode) in an IPv6 cluster. **Scenario:** This issue occurs when VRRP IPv6 address is configured and CPsec is enabled. As a result, the AP goes into **D** flag mode due to incorrect port selection in the **SAPD** process. This issue is observed in APs running ArubaOS 8.5.0.0 or later versions in a cluster setup. **Workaround:** Disable the VRRP IPv6 address.	IPv6	All platforms	ArubaOS 8.5.0.0
AOS-190184 AOS-190241 AOS-190347 AOS-190468 AOS-190487 AOS-190776	—	**Symptom:** The database synchronization fails between primary and secondary Mobility Masters in L3 redundancy. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.4.0.3

This chapter details software upgrade procedures. It is 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, or stand-alone controller.

Topics in this chapter include:

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 36 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
  - **Flash backups:** Use the procedures described in Backing up Critical Data on page 36 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log 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 36 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 flashbackup.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: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>

(host) #copy flash: flashbackup.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: 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 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 35.

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 35 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 36 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 36.
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**.

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

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** 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 section describes 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 controller:
   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```
   or
   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the controller 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 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.