ArubaOS 8.3.0.0

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
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	■ Removed **Migration Guide** from the documents listed under **Related Documents** section as the Migration Tool is no longer supported. ■ Removed the **Migrating from ArubaOS 6.x to ArubaOS 8.x** section from **Upgrade Procedure** chapter as the Migration Tool is no longer supported.
Revision 03	Added bug 168645.
Revision 02	Added the **Disabling TLS RSA Cipher Suites** enhancement.
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.

Related Documents

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

- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- Aruba *Mobility Master Licensing Guide*
- *Aruba Virtual Appliance Installation Guide*
- *Aruba Mobility Master Hardware Appliance Installation Guide*

Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 58 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

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

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

AirMatch

AirMatch Channel and Power Allocation

The following AirMatch commands are introduced in ArubaOS 8.3.0.0:

- **show airmatch debug apinfo**
- **show airmatch debug pathloss history rep-radio**

The following AirMatch commands are modified in ArubaOS 8.3.0.0:

- **airmatch ap freeze** and **airmatch ap unfreeze** support both single radio and dual-radio APs.
- **airmatch runnow** - The **eirp** and **opmode** parameters are introduced.

The following fields are introduced in the output of the **show airmatch debug feasibility** command:

- Current Opmode
- HW Supported Opmodes
- Configured Opmodes
- Feasible Opmodes
- Eirp Range Chan 20MHz
- Eirp Range Chan 40MHz
- Eirp Range Chan 80MHz
- Eirp Range Chan 160MHz

Dual 5 GHz / Dual Band Operating Mode Selection

When **Dual 5GHz Mode** is set to **Automatic**, AirMatch automatically determines the optimal settings for dual 5 GHz capable APs to be either dual band (5 GHz and 2.4 GHz) or dual 5 GHz (both radios operating in 5 GHz), depending on AP density and RF environment. If **Dual 5GHz Mode** is set to **Enabled**, then AirMatch sets the AP to operate in dual 5 GHz band, and if set to **Disabled**, then the AP is set to dual band.

AP-Platform

Loop Protection

The loop protection feature detects and avoids the formation of loops on the Ethernet ports of Campus APs, Remote APs, or Mesh APs. The loop protection feature can be enabled on all APs that have multiple Ethernet ports and it supports tunnel, split-tunnel, and bridge modes.

303 Series Wireless Access Points

The 303 Series access points are high-performance dual-radio wireless devices that support IEEE 802.11ac Wave 2 standard. These APs use MIMO technology to provide secure wireless connectivity for both 2.4 GHz 802.11a/b/g/n wireless services and 5 GHz 802.11a/n/ac Wi-Fi.

These APs provide the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Integrated BLE radio

For complete technical details and installation instructions, refer to the *Aruba 303 Series Campus Access Points Installation Guide*.

AP-318 Wireless Access Points

The 318 Series wireless access points support IEEE 802.11ac Wave 2 standard, delivering high performance with the MU-MIMO technology, while also supporting 802.11a/b/g/n wireless services.

These APs provide the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatibility with IEEE 802.3at PoE

For complete technical details and installation instructions, refer to the *Aruba 318 Series Wireless Access Points Installation Guide*.

340 Series Access Points

The 340 Series access points (AP-344 and AP-345) are high-performance dual-radio wireless devices. These access points provide secure wireless connectivity for 2.4 GHz 802.11 b/g/n and 5 GHz 802.11a/n/ac Wi-Fi networks. The optional dual 5 GHz radio mode allows both radios to operate in the 5 GHz radio mode simultaneously, doubling the 5 GHz capacity of the access point. The 340 Series access points can be deployed in either a controller-based (ArubaOS) or controllerless (Instant) network environment.

These APs provide the following capabilities:

- Wireless access

- Wireless mesh
- AM
- SM
- Support for selected USB peripherals
- Integrated BLE radio
- MU-MIMO (Wave 2) support

For complete technical details and installation instructions, refer to the *Aruba 340 Series Access Points Installation Guide*.

370 Series Outdoor Access Wireless Access Points

The 370 Series outdoor wireless access points (AP-374, AP-375, and AP-377 access points) support IEEE 802.11ac Wave 2 standard. They also deliver high performance with the MU-MIMO technology, in addition to supporting 802.11a/b/g/n wireless services.

These APs provide the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatibility with IEEE 802.3at PoE

For complete technical details and installation instructions, refer to the *Aruba 370 Series Outdoor Access Points Installation Guide*.

AP Fast Recovery

Starting from ArubaOS 8.3.0.0, Aruba APs provide support for the AP Fast Recovery feature. On detecting a firmware assert, the AP executes the fast recovery process in the affected radio. This avoids rebooting the AP unnecessarily, thereby reducing the downtime of the AP in the network. If the AP detects a core dump with valuable information during a firmware assert, then it transfers the core dump to the managed device and reboots. A new parameter, **recovery-mode**, is introduced in the **ap system-profile** command to configure this feature.

Support for Huawei K5150 4G Modem

ArubaOS 8.3.0.0 supports Huawei K5150 4G modems on managed devices and Remote APs. This modem can be provisioned so that managed devices and Remote APs can choose the available network automatically.

Support for ZTE MF831 4G Modem

ArubaOS 8.3.0.0 supports ZTE MF831 4G modems on managed devices and Remote APs. This modem can be provisioned so that managed devices and Remote APs can choose the available network automatically.

Support for New ZTE 4G Modems on Remote APs

Starting from ArubaOS 8.3.0.0, ZTE MF832S and ZTE MF825C 4G modems are supported on Remote APs.

Support for Dual 5 GHz Mode on 340 Series Access Points

Starting from ArubaOS 8.3.0.0, 340 Series access points support dual 5 GHz radio operation. This is applicable to AP-344 and AP-345 access points. You can set this feature to enable, disable, or automatic mode using the WebUI or the CLI.

The **automatic** mode is only supported in Mobility Master-Managed Device deployments and is used with AirMatch.

The automatic dual 5 GHz selection mode is not supported on AP-344 access points.

Support for 3G/4G Provisioning

Starting from ArubaOS 8.3.0.0, APs support the use of 3G and 4G USB modems to provide Internet backhaul to a network.

Support for Hotspot 2.0 R2

Starting from ArubaOS 8.3.0.0, the Hotspot 2.0 R2 feature support is extended to 300 Series, AP-303H, 310 Series, 320 Series, 330 Series, 340 Series, AP-365, AP-367, and 370 Series access points in both controller-based and controllerless modes.

Support for IAP-VPN Termination on Mobility Controller Virtual Appliance

Starting from ArubaOS 8.3.0.0, Mobility Controller Virtual Appliance supports IAP-VPN termination by using custom certificates.

Disabling TLS RSA Cipher Suites

Starting from ArubaOS 8.3.0.0, the following TLS RSA cipher suites are disabled to ensure complete forward confidentiality and to prevent the Return of Bleichenbacher's Oracle Threat (ROBOT) attacks in APs:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

This enhancement impacts functionalities such as OpenFlow, RadSec, SSH, WebUI, Authentication, Captive Portal, AirWave,Central, and Activate.

AP-Wireless

Support for 802.3bz

Starting from ArubaOS 8.3.0.0, 330 Series access points are compliant with 802.3bz standard. This is an IEEE standard-based support for 2.5 Gbps or 5 Gbps.

ARM

Client Match Enhancement

Starting from ArubaOS 8.3.0.0, a new output field, **AS**, is supported in the output of the **show ap arm client-match history** command that displays the actual radio signal strength of the target AP at steer completion.

Load Balancing Interval

Starting from ArubaOS 8.3.0.0, a new parameter, **cm-lb-interval** is added to the **rf arm-profile** command to control the interval at which the Client Match performs load balancing. This parameter applies to both spectrum and MU-MIMO load balancing that is performed by the Client Match.

The default value of this parameter is 5 minutes and the valid range is 0-255, where 0 is used to disable load balancing.

To display the load balancing interval, a new output field, **LB Invl(minutes)** is added to the output of the **show ap arm client-match debug state** command.

Advanced Transmit Rate Statistics

Starting from ArubaOS 8.3.0.0, the output of the following commands include MCS bucket mapping information with channel width, number of spatial streams, and guard interval information of 802.11ac APs:

- **show ap debug radio-stats**
- **show ap debug bss-stats**
- **show ap debug client-stats**

Authentication

Enhancements to SSH Ciphers and MAC Algorithms

Starting from ArubaOS 8.3.0.0, administrators can configure SSH to enable or disable the following ciphers and MAC authentication algorithms:

- HMAC-SHA1-96
- HMAC-SHA1
- AES-CBC
- AES-CTR

This enhancement is only supported in the non-FIPS mode of operation.

Base OS Security

Support for ASCOM Device-Type

Starting from ArubaOS 8.3.0.0, ASCOM device-type is supported while performing device classification.

VIA Connection-Profile Enhancement

This enhancement provides the ability to mark outgoing IKE and ESP packets with custom DSCP, which is configured in managed devices by using the VIA connection-profile.

This enhancement is specifically for Android clients. This is already available for Windows clients.

A new parameter, **tos_dscp**, for marking custom DSCP is available under VIA connection-profile. The range of values allowed for this parameter is 0 to 63. This parameter is part of the **aaa authentication via connection-profile <profile>** command. You can configure this parameter by using the WebUI or CLI.

BLE

ZF Openmatics Support for ZF BLE Tag Communication

Starting from ArubaOS 8.3.0.0, you can manage ZF Tags and implement the BLE location service using the third-party ZF Openmatics. To support this feature, Aruba APs with built-in IoT-protocol radio (BLE) are required. You can configure the APs to support ZF Openmatics using the IoT profiles.

IoT Endpoints

Starting from ArubaOS 8.3.0.0, APs contain a built-in IoT protocol that can send BLE information containing payload messages to the endpoints over a WebSocket or HTTPS connection. An IoT Transport Profile is a global profile similar to the management server profile. It is used to transport state and statistics data to endpoints. Administrators can also restrict unauthorized profiles from being applied to the stand-alone and cluster-based APs.

Controller-Datapath

New Counter for Standby Managed Devices in a Cluster

Starting from ArubaOS 8.3.0.0, a new counter, **current standby entries**, is added to the **station** parameter of the **show datapath** command. This counter provides information on standby managed devices in a cluster.

Controller-Platform

Support for 7280 Controller Platform

The 7280 controller is a wireless LAN controller that connects, controls, and intelligently integrates wireless APs and AMs into a wired LAN system.

This controller has the following port configuration:

- 2 x 40 GbE (QSFP+) ports
- 8 x 10 GBase-X (SFP+) ports
- USB 2.0 interface
- Console port
- Micro USB console port
- Management port

For technical specifications and installation instructions, refer to the *7280 Controller Installation Guide*.

Cluster

Active AP Load Balancing Enhancement

Starting from ArubaOS 8.3.0.0, the APs are redistributed based on the Active AP count and the standby APs are not considered. This ensures that fewer APs fail over when a managed device fails over.

CPsec

Control Plane Security Enhancements

Starting from ArubaOS 8.3.0.0, a configurable parameter, **timer**, is added to the **control-plane-security** command. The default value of this parameter is 2 hours. When an AP does not come up on the controller within the configured or default value of the CPsec expiry timer, the CPsec entry is revoked and is moved to the **unapproved-no-cert** state in the whitelist database table. Use the following commands to configure the **timer** parameter:

```
(host) [md] (config) #control-plane-security
(host) [md] (Control Plane Security Profile) #timer <timer>
```

IPsec

TLS-RSA Cipher Suites

Ciphers are used to configure the strength of the cipher suites as high, medium, or low by executing the **web-server profile** command.

Starting from ArubaOS 8.3.0.0, the following ciphers are not supported only in FIPS builds:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_192_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246

- TLS_RSA_WITH_AES_192_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_192_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

The feature components that act as TLS clients do not propose the discontinued ciphers as part of the client **Hello** message.

The following subsections provide cipher-related details for FIPS and non-FIPS builds:

In FIPS Builds

- The static-key ciphers and static RSA ciphers are not supported but the web-server ciphers are always set to the default value, high.
- WebUI does not support static-key ciphers.
- EAP-TLS/EAP-PEAP for 802.1X termination supports static RSA ciphers.
- For RadSec, server-side changes are required to support ECDHE/DHE ciphers.

In non-FIPS Builds

- In web-server, different ciphers can be selected based on their strengths.
  - High – ECDHE and DHE ciphers
  - Medium – DHE and static RSA ciphers
  - Low – Only static RSA ciphers
- The WebUI does not support static-key ciphers.

Licensing

Support for Flex ACR License (LIC-ACR)

ArubaOS 8.3.0.0 provides support for Flex ACR License.

Logging

CEF Enhancement

Starting from ArubaOS 8.3.0.0, the syntax of a CEF message is enhanced to provide additional information. This allows ArcSight to interpret the CEF information more accurately.

The **Device Event Class ID**, **Name**, and **Severity** parameters are introduced in the syntax of the CEF message. The following example shows the CEF format in which controllers can send syslog messages.

```
CEF: Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|[Extension]
```

MultiZone

Client Match Support

Starting from ArubaOS 8.3.0.0, the Client Match features such as sticky-client and band steering are supported in a MultiZone deployment for Campus APs. Client Match in each zone functions independently by controlling clients that are associated to the Virtual APs owned by that zone.

Decrypt Tunnel Support

Starting from ArubaOS 8.3.0.0, MultiZone supports Decrypt Tunnel forwarding mode on the data zone Virtual APs.

RSDB and Dual 5 GHz Bands Support for MultiZone

Starting from ArubaOS 8.3.0.0, MultiZone supports RSDB on AP-203R, AP-203RP, and AP-203H access points. Also, MultiZone supports Dual 5 GHz on AP-344 and AP-345 access points.

RADIUS

Support for RADIUS Accounting Session ID in RADIUS Access Request

Starting from ArubaOS 8.3.0.0, the RADIUS access request, if configured, includes the RADIUS accounting session ID. Allow the RADIUS access-request to include the RADIUS accounting session ID by enabling the **radius-acct-session-id-in-access** parameter in the **aaa profile** command.

```
(host) [mynode] (config) #aaa profile default
(host) [mynode] (AAA Profile "default") #radius-acct-session-id-in-access
```

Tunnel Node

Support for Downloadable Roles for Per-user Tunneled Node Users

Starting from ArubaOS 8.3.0.0, this feature allows the managed device to get the user role from the Aruba ClearPass Policy Manager server while tunneling wired user's traffic to the managed device.

Web Server

Supported SSL/TLS Protocol in FIPS Mode of Operation

Starting from ArubaOS 8.3.0.0, the SSL or TLS protocol of the FIPS version supports only TLSv1.2 for secure communication with the web server. Use the **show web-server profile** command to display the configured TLS version. The output on execution of this command is as follows:

```
(host) [mynode]# show web-server profile

Web Server Configuration
------------------------
Parameter                                        Value
---------                                        -----
SSL/TLS Protocol Config                          tlsv1.2
Switch Certificate                               default
Captive Portal Certificate                       default
IDP Certificate                                  default
Management user's WebUI access method            username/password
User absolute session timeout <30-3600> (seconds)  0
User session timeout <30-3600> (seconds)         900
Maximum supported concurrent clients <25-320>    75
```

WebUI

WebUI Enhancements to Support Dual 5 GHz Mode

Starting from ArubaOS 8.3.0.0, you can find the new **Dual 5GHz mode** option in the following paths:

- Configuration > System > Profiles > AP > AP system profile.
- Configuration > AP Groups > Profiles > AP > AP system > AP system profile: <profile-name> (make sure the Username > Preference > show advanced profiles option in the WebUI is enabled).

For a stand-alone controller or a master controller, the **Dual 5GHz mode** option is available in the **Configuration > AP Groups > <AP group profile-name> > Radio > Advanced** path.

When you select an AP-344 access point model in the Access Points table, you can see two additional gain parameters to set for Radio 0 and Radio 1 for Dual 5 GHz mode. Find these parameters in the following paths:

- Configuration > Access Points > Campus APs.
- Configuration > Access Points > Remote APs.
- Configuration > Access Points > Mesh APs.

The **Dashboard** page now displays graphs for details on the radios of Dual 5 GHz mode APs. To view the lower band radio and upper band radio details of a Dual 5 GHz mode AP, navigate to **Dashboard > Access Points > Access Points table** and select a 340 Series AP.

Support for Viewing Inheritance History

Starting from ArubaOS 8.3.0.0, the WebUI allows you to view the inheritance details of any configuration at any group or node level. This feature is supported only for configurations that can be overridden. A blue color information icon is displayed in the respective rows of the configuration table under which some configurations are overridden. Clicking the icon displays the details of the inheritance with a link to the parent node. You can click on

the parent node link to navigate to the parent node level. You can choose to remove all the overrides under the selected node level from the pop-up window by clicking the **Remove Overrides** button. Else, you can choose to remove the individual configuration overrides at the field level.

Support for WLAN Forwarding Mode Options

Starting from ArubaOS 8.3.0.0, new WebUI options, **Split-Tunnel** and **Bridge** modes, are added to the **Forwarding mode** drop-down list in the **WLANs > General** page.

WebUI Support for Called Station ID in RADIUS Server Profile

Starting from ArubaOS 8.3.0.0, Mobility Master provides WebUI support for configuring the **Called Station ID** parameters, such as **Station ID type**, **Station ID delimiter**, and **Include SSID** for a RADIUS server under the **Configuration** > **Authentication** > **Auth Servers** page of the WebUI.

This chapter describes the hardware platforms supported in this release.

Controller Platforms

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

Table 3: *Supported Controller Platforms in ArubaOS 8.3.0.0*

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

AP Platforms

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

Table 4: *Supported AP Platforms in ArubaOS 8.3.0.0*

AP Family	AP Model
—	AP-103, AP-103H
100 Series	AP-104, AP-105
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

Table 4: *Supported AP Platforms in ArubaOS 8.3.0.0*

AP Family	AP Model
200 Series	AP-204, AP-205
—	AP-203H
—	AP-205H
—	AP-207
203R Series	AP-203R, AP-203RP
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
—	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
—	AP-303
—	AP-303H
310 Series	AP-314, AP-315
—	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

Table 4: *Supported AP Platforms in ArubaOS 8.3.0.0*

AP Family	AP Model
	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
—	RAP-3WN, RAP-3WNP

Chapter 4
Regulatory Updates

This chapter contains the Downloadable Regulatory Table (DRT) file version introduced in this release.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller 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_64450

This chapter describes the issues resolved in this release.

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
114524	**Symptom:** Some APs displayed 270% channel utilization in the AP tables. The fix ensures that the APs do not display excessive utilization. **Scenario:** This issue was observed in APs running ArubaOS 8.2.0.0.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
137108	**Symptom:** Users were unable to log in to VIA when they used special characters in the authentication password. This issue is resolved by configuring different encoding format types. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	RADIUS	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
156908	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **Kernel panic - not syncing: softlockup: hung tasks**. The fix ensures that the frames with sequence number 0 are inserted at the tail of the frames. **Scenario:** The issue occurred as the frames with sequence number 0 were inserted in an incorrect position. The issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
161383 173575 176409	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW HANG**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-305 and 320 Series access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-305 and 320 Series access points	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
162272	**Symptom:** A Mobility Master Virtual Appliance was unresponsive. This issue is resolved by disabling the serial console redirect. **Scenario:** This issue occurred during a kernel crash with the serial console redirect. This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.2.0.0 on Hyper-V.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
162735	**Symptom:** The **datapath** process in a managed device crashed and the managed device rebooted unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred because of packet-metadata corruption like invalid packet reference-count or invalid ingress-CPU information. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
164253	**Symptom:** The Remote AP console page, rapconsole.arubanetworks.com, displayed the old Aruba logo for a stand-alone Remote AP. The fix ensures that the new HPE-Aruba logo is displayed. **Scenario:** This issue was observed in Remote APs running ArubaOS 8.2.0.0.	Remote AP	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
165440	**Symptom:** An OpenFlow controller failed to identify clients that were connected to an AP. The AP also did not connect to the OpenFlow controller when the DNS server was not reachable. The fix ensures that upon availability of the DNS server, the AP resolves the FQDN and automatically tries to re-establish the connection. **Scenario:** This issue was observed in access points running ArubaOS 8.2.0.0 or later versions.	Aruba Aruba Central	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
165595	**Symptom:** A managed device displayed the following error messages: ■ **Unexpected stm (Station management) runtime error at wifi_refresh_assoc_drv**. ■ **An internal system error has occurred at file messenger.c function msgr_vap_stats_v2 line 5267 error msgr_vap_stats_v2**. The fix ensures that these incorrect error messages are not displayed in the logs. **Scenario:** This issue occurred when a backup Virtual AP was configured for another AP. This issue was observed in APs running ArubaOS 8.2.0.0.	Air Management-IDS	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
165788	**Symptom:** A user was unable to remove stale entries from a standby Mobility Master. The fix allows the user to delete stale entries from the standby Mobility Master. **Scenario:** This issue was observed in a standby Mobility Masters running ArubaOS 8.2.0.0 or later versions in a master-standby topology.	Station Management	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
166272 173020	**Symptom:** Clients were unable to connect to virtual IPs through the Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP). The fix ensures that clients are able to connect to virtual IPs. **Scenario:** This issue occurred when clients used the L2 GRE tunnel to connect to virtual IPs, and Broadcast and Multicast Optimization was enabled on the VLAN. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	Routing	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.3.0.0
167028	**Symptom:** The SNMP walk reported that an AP's port speed was greater than 1 Gbps on a 1 Gbps Ethernet Port. The fix ensures that the correct AP port speed is displayed. **Scenario:** This issue occurred because the **STM** process incorrectly calculated the Ethernet port speed. This issue was observed in APs running ArubaOS 8.0.1.0 or later versions.	Air Management - IDS	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167198 177034	**Symptom:** An AP crashed and rebooted. The log file listed the reason for the event as **Reboot caused by kernel panic: softlockup: hung tasks**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred due to an interruption while sending multicast data to the AP. This issue was observed in AP-303H, AP-304, AP-305, AP-365, and AP-367 access points running ArubaOS 8.2.0.0.	AP Datapath	AP-303H, AP-304, AP-305, AP-365, and AP-367 access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
167572	**Symptom:** A correct role was not assigned to a user. The fix ensures that a correct role is assigned to the user. **Scenario:** This issue occurred when a user role was configured in uppercase but the managed device identified the user role in lowercase. This issue was observed in managed devices running ArubaOS 8.1.0.1 or later versions.	Role/VLAN Derivation	All platforms	ArubaOS 8.1.0.1	ArubaOS 8.3.0.0
167706	**Symptom:** A managed device rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when few leaked packets were not handled properly in SOS. This issue was observed in 7200 Series controllers running ArubaOS 8.0.0.0 or later versions.	Controller-Datapath	7200 Series controllers	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
168146	**Symptom:** A Mobility Master Hardware Appliance failed to download the Activate whitelist from a managed device. The fix ensures that the Mobility Master Hardware Appliance successfully downloads the whitelist from a managed device. **Scenario:** This issue was observed in Mobility Master Hardware Appliances running ArubaOS 8.1.0.2 or later versions.	Controller-Platform	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.3.0.0
168457	**Symptom:** The ACR license count was not updated to the applications running on a standby Mobility Master until a failover happened. The fix ensures that the ACR license limits are updated to the applications as soon as the database synchronizes. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions in a master-standby topology.	Licensing	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168485	**Symptom:** The AeroScout Location Engine was unable to receive Wi-Fi tags from the server. The fix ensures that the AeroScout Location Engine is able to receive Wi-Fi tags from the server. **Scenario:** This issue occurred when the AP firewall blocked the UDP port 1144. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
168789	**Symptom:** APs with an 802.1X supplicant configuration failed to boot. The fix ensures that APs with the 802.1X configuration are able to boot. **Scenario:** This issue occurred when an ACL denied DNS response from a DNS server. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
168971 169581 169880 171920 173550	**Symptom:** An AP stopped responding and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. Improvements to the AP wireless driver resolved the issue. **Scenario:** This issue occurred due to a memory corruption of the AP. This issue was observed in 300 Series, AP-303H, 310 Series, 320 Series, and 330 Series access points running ArubaOS 8.1.0.0 in Mesh mode.	Mesh	300 Series, AP-303H, 310 Series, 320 Series, and 330 Series points	ArubaOS 8.1.0.0	ArubaOS 8.3.0.0
169010 169073 173330 175788	**Symptom:** An AP failed to respond and rebooted unexpectedly. The log file listed the reason for the event as **Unhandled fault: external abort on non-linefetch (0x1008) at 0xe6000000**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in 300 Series access points running ArubaOS 8.2.0.0.	AP-Platform	300 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
169029	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **panic-dump.apkys-invrec-pnt.2017-09-07_21-13-04**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-275 access points running ArubaOS 8.2.0.0.	Mesh	AP-275 access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169151	**Symptom:** Some Windows clients detected IP address conflict with a Mobility Master. The fix ensures that Windows clients do not detect IP address conflicts when OpenFlow is enabled. **Scenario:** This issue occurred if the client sent an ARP probe when OpenFlow was enabled on the Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
169327	**Symptom:** A Mobility Master displayed the **An internal system error has occurred at file server_group.c function cfg_server_group_item_int line 384 error Error: unknown server** error. The fix ensures that the repositioned server configurations are sent to the managed device. **Scenario:** This issue occurred when the authentication server in the server group was repositioned, but the new position was not sent to the managed device. This issue was observed in Mobility Masters running ArubaOS 8.1.0.3 or later versions.	Base OS Security	All platforms	ArubaOS 8.1.0.3	ArubaOS 8.3.0.0
169540 175490	**Symptom:** The **STM** process in a managed device crashed multiple times. The fix ensures that the number of virtual APs is set after validating that the AP is in mesh recovery mode. **Scenario:** This issue occurred when an AP switched to mesh recovery mode and the number of virtual APs was incorrectly set to the maximum number of SSIDs. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
169749	**Symptom:** A client was unable to connect to 5 GHz radio on some APs. Improvements to the wireless driver resolved this issue. **Scenario:** This issue occurred because radio 0 did not transmit traffic. This issue was observed in AP-325 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-325 access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
170037	**Symptom:** APs configured with static IP addresses failed to discover the WLAN controller through ADP or DNS. The fix ensures that APs are able to discover the WLANs accurately. **Scenario:** This issue occurred when an ACL denied Tx ADP packets. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170111 177361	**Symptom:** The **STM** process in a Mobility Master stopped responding after executing the **clear gap-db stale** command. The fix ensures that the **STM** process works as expected upon executing the command. **Scenario:** This issue occurred in a cluster topology with load balancing enabled. This issue was observed in Mobility Masters running ArubaOS 8.1.0.2 or later versions.	AP-Platform	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.3.0.0
170171	**Symptom:** A **web server** process that handles captive portal requests crashed intermittently in a managed device. The fix ensures that the **web server** process does not crash. **Scenario:** This issue occurred when there was an increase in the captive portal requests sent to the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Captive Portal	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
170346	**Symptom:** Some clients were unable to connect to an AP. The fix ensures that the clients connect to the APs without service interruption. **Scenario:** This issue occurred because the whitelist database of Campus AP was missing in the managed device and when irrelevant log messages in the log file consumed memory. This resulted in missing whitelist database entries. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Database	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
170457	**Symptom:** A managed device dropped VLAN probe requests causing the cluster to remain in L3 connected state. The fix ensures that the managed device does not drop VLAN probe requests when the **bcmc-optimization** parameter is enabled. **Scenario:** This issue occurred when **bcmc-optimization** parameter was enabled on the VLAN interface after reloading the managed device in the cluster. This issue was observed in cluster setups running ArubaOS 8.2.0.0 or later versions.	Cluster Manager	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170803 171109	**Symptom:** A managed device stopped responding and rebooted. The log file listed the reason for the event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to a memory leak on the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
171113	**Symptom:** Bandwidth contracts in the target role were not applied to a split-tunnel user. The fix ensures that bandwidth contracts are applied to the split-tunnel user. **Scenario:** This issue occurred when RFC 3576 CoA was used to change the role of the split-tunnel user. This issue was not limited to any specific platform or ArubaOS version.	AP Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
171316	**Symptom:** A managed device displayed the **dot1x_gsm_set_pmkcache(): GSM: Failed to publish PMK-cache object. Error:error_no_free_slots** error. The fix ensures that the managed device does not display the error. **Scenario:** This issue occurred when the PMK cache GSM channel was full. This issue was observed in cluster setups running ArubaOS 8.2.0.1.	Base OS Security	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0
171379	**Symptom:** Multiple core dumps were observed in AP-325 access points. The fix ensures that the packets with invalid lengths are not processed. **Scenario:** This issue occurred when the wireless driver sent packets with invalid lengths to the AP. This issue was observed in AP-325 access points running ArubaOS 8.0.0.0 or later versions.	Air Management - IDS	AP-325 access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
171521 175748	**Symptom:** The captive portal redirect was not triggered for a Linux-based client. The fix ensures that the captive portal redirect for Linux-based clients is successful. **Scenario:** This issue occurred when Linux-based clients used the additional Resource Record (RR) options in the DNS request and DNS response returned **no such name** instead of the IP address of the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171611	**Symptom:** Static route entries were missing in the managed device. Hence the managed device was disconnected from the Mobility Master. The fix ensures that the **ISAMKPD** process uses the correct crypto map during IKE or IPsec tunnel initiation. **Scenario:** This issue occurred when **masterip, vpnip,** and **vpn-peer peer-mac** commands pointed to the same MAC address and the **ISAMKPD** process used a wrong crypto map during IKE or IPsec tunnel initiation. This issue was observed in managed devices running ArubaOS 8.1.0.4 or later versions.	IPsec	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.3.0.0
171614 172310 174525 175401	**Symptom:** The **Datapath** process on a managed device crashed. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the process does not crash due to invalid memory access. **Scenario:** This issue occurred due to an invalid memory access. This issue was observed in managed devices running ArubaOS 8.1.0.4 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.3.0.0
171923	**Symptom:** A client that was connected to the second Ethernet port of an AP in bridge mode was not assigned an IP address and was unable to send or receive traffic. The fix ensures that the client obtains an IP address and can send or receive traffic. **Scenario:** This issue occurred because both wired and wireless clients had a common VLAN. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
172534	**Symptom:** WEP clients were unable to pass traffic after a cluster failover. The fix ensures that the clients are able to pass traffic after the cluster failover. **Scenario:** This issue occurred when dynamic WEP keys were not synchronized in a cluster. This issue was observed in cluster setups running ArubaOS 8.1.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172665	**Symptom:** A managed device did not clear the stale internal-user entries of IPsec tunnels from an HPE switch. The **aaa user delete** command displayed the following error message: **User delete for HP switches is not supported**. This issue is resolved by allowing deletion of the HPE switch user entries. **Scenario:** This issue occurred when a managed device included the HPE switch users as trusted users but omitted them from ageout user deletion. The HPE switch users were retained as stale internal-user entries even after IPsec sessions between users and the managed device were terminated. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
172801 175444 176229	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as, **kernel panic: Fatal exception**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-225 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-225 access points	ArubaOS8.0.0.0	ArubaOS 8.3.0.0
173083	**Symptom:** The WebUI displayed the Mobility Controller label for a standby Mobility Master. The fix ensures that the WebUI displays the Mobility Master label for the standby Mobility Master. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.0.1 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0
173230	**Symptom:** A Remote AP rebooted unexpectedly. The log file listed the reason for this event as **Missed heartbeats**. The fix ensures that the Remote AP works as expected. **Scenario:** This issue occurred when **Tx queue** in the **IPsec** process was stuck. This issue was observed in RAP-155 access points running ArubaOS 8.0.0.0.	AP-Platform	RAP-155 access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
173328	**Symptom:** The **block-redirect-url** configuration on an active Mobility Master did not synchronize with the standby Mobility Master. The fix ensures that the **block-redirect-url** configuration is updated on the standby Mobility Master. **Scenario:** This issue occurred in Mobility Masters running ArubaOS 8.0.0.0 or later versions in an active-standby topology.	WebCC	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173422 173483 173576	**Symptom:** The **Dashboard** page of a Mobility Master incorrectly displayed the status of some APs as DOWN although the APs were UP. The fix ensures that the Mobility Master correctly displays the status of APs. **Scenario:** This issue occurred when all SSIDs in an AP group were disabled. This issue was observed in Mobility Masters running ArubaOS 8.2.0.1 or later versions.	Monitoring	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0
173441	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as, **kernel panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
173554	**Symptom:** The IDS logs and SNMP traps included WVE ID hyperlinks that were invalid. The fix ensures that the WVE information is removed from all IDS logs. **Scenario:** This issue was not limited to any specific controller model or ArubaOS release version.	Air Management-IDS	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
173772	**Symptom:** When a user tried to map a VLAN name to a user role the CLI displayed **Invalid Named VLAN**. The fix ensures that the user is able to map the VLAN name to the user role. **Scenario:** This issue occurred when a VLAN name was automatically stored in lowercase. This issue was observed in managed devices running ArubaOS 8.1.0.4 or later versions.	VLAN	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.3.0.0
173868	**Symptom:** Users with the same static IP address failed to pass traffic when connected to an SSID. The fix ensures that the static IP address successfully passes traffic when connected to the SSID. **Scenario:** This issue occurred when **prohibit-ip-spoofing** parameter was disabled in the firewall settings. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173993	**Symptom:** IDS incorrectly detected rogue APs on a secure network. The fix ensures that wired clients do not introduce invalid wired MAC addresses into the Ethernet MAC list. **Scenario:** This issue occurred when a client moved from an external wireless network to a wired corporate network. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	Air Management-IDS	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
174001	**Symptom:** A Mobility Master failed to send SNMPv3 **INFORM** traps to AirWave. The fix ensures that the Mobility Master sends SNMPV3 **INFORM** traps to AirWave. **Scenario:** This issue occurred after the Mobility Master rebooted. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	SNMP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
174287	**Symptom:** An AP incorrectly operated in restricted mode (indicated by a flashing system LED) though the uplink speed was set to an optimal value. The fix ensures that the AP operates in the correct mode. **Scenario:** This issue was observed in 330 Series access points running ArubaOS 8.0.0.0 or later versions.	AP Platform	330 Series access points	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0
174336	**Symptom:** APs crashed and rebooted intermittently. The log file listed the reason for the event as **External watchdog reset** and **kernel panic: Fatal exception**. The fix ensures that APs do not crash and reboot. **Scenario:** This issue was observed in 200 Series access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	200 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
174337	**Symptom:** IDS tarpit containment was inconsistent in access points. The issue is resolved by ensuring that tarpit frames are sent on the same channel as that of the target device. **Scenario**: This issue occurred when APs were configured in AM mode and the tarpit frames were sent out on the wrong channel. This issue was observed in APs, but is not restricted to any ArubaOS version.	Air Management - IDS	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174495 176334	**Symptom:** The **show configuration effective** command output displayed **inherited from [/sc]** for some configuration details. This issue is resolved by fixing the command output to display **inherited from [/mm]**. **Scenario:** This issue occurred because **/sc** was not replaced with **/mm** in some file instances. This issue was observed in a Managed Device - Mobility Master Virtual Appliance topology.	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.0
174533	**Symptom:** SNMP traps with interface name and interface description were not available as part of **wlsxPortDown** and **wlsxPortUp**. The fix ensures that SNMP traps with the interface name and interface description are available. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0.	SNMP	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
174615	**Symptom:** Cluster VRRP flapping was observed when threshold values on a managed device were modified. This issue is resolved by retaining VRRP flaps when the cluster parameters are modified. **Scenario:** This issue occurred when the cluster manager added or deleted the VRRP instances multiple times. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	VRRP	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0
174644 174925	**Symptom:** AirGroup lost all the learned server and user details and also failed to learn any new user or server. The fix ensures that AirGroup learns all users and servers appropriately. **Scenario:** This issue occurred whenever an AirGroup service or profile was modified. This issue was observed in ArubaOS 8.2.0.0 or later versions.	AirGroup	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0
174670	**Symptom:** An LACP port channel received multiple warning messages, **LACP: Disabling Collection and Distribution on port 0/0/0 LAG 0**. The fix ensures that the port channel does not receive these warning messages. **Scenario:** This issue occurred when the port channel was in trusted mode and trusted VLAN list for the port channel did not have default VLAN in its list. This issue was observed in stand-alone controllers running ArubaOS 8.2.0.2 or later versions.	Port-Channel	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174788	**Symptom:** Mobility Masters incorrectly allowed users to execute the **aaa user delete** command from the **/mm** or **/mm/mynode** levels. However, the command was not effective because it was applicable only at the managed device level (**/md/<device>**). The fix ensures that an error message is displayed when executing the command from the **/mm** or **/mm/mynode** levels. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0
174823 175163	**Symptom:** The **Authentication** process in a managed device crashed unexpectedly. The fix ensures that the **Authentication** process does not crash. **Scenario:** This issue occurred when the **aaa test-server verbose** command was executed. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
174865	**Symptom:** Some clients moved to 802.1X authentication although they failed MAC authentication. This issue is resolved by not allowing clients that fail MAC authentication to move to 802.1X authentication. **Scenario:** This issue occurred when L2 fail-through was disabled. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
174955	**Symptom:** The **Dashboard** > **UCC** > **Calls Per Device Type** > **Table** tab displayed **0** call records under the **Last Hr** column. The fix ensures that the call records are displayed correctly. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.0
174979	**Symptom**: The size of the **ale.log** file on a Mobility Master was large. This issue is resolved by updating only the consolidated data to the **ale.log** file once a day. **Scenario**: This issue occurred due to frequent processing of AMON messages. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.	NBAPI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175061	**Symptom:** The system time of a managed device was displayed incorrectly. The fix ensures that correct time is displayed on the managed device. **Scenario:** This issue occurred when the **NTPD** process in a managed device used a local interface during boot time. The local interface did not have a route to the NTP server and hence the system time of the managed device was not synchronized. This issue was observed in a managed devices running ArubaOS 8.2.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
175268	**Symptom:** The output of **show ap debug client-table** command displayed incorrect Tx-Retries. The fix ensures that accurate Tx-Retries are displayed. **Scenario:** This issue was observed in 300 Series access points connected to managed devices running ArubaOS 8.0.0.0.	AP Datapath	300 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
175333	**Symptom:** Clients were unable to pass traffic. The fix ensures that clients can pass traffic. **Scenario:** This issue was observed in AP-325 access points running ArubaOS 8.0.0.0.	AP-Platform	AP-325 access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
175340	**Symptom:** The AP logs for a Remote AP displayed the error message, **connect-debounce failed, port 1 disabled**. The fix ensures that this error is not displayed. **Scenario:** This issue was observed in RAP-3WNP access points running ArubaOS 8.0.0.0.	AP-Platform	RAP-3WNP access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175387	**Symptom:** APs blocked ARP requests which had the same IP address as that of local DHCP server of AP. The fix ensures the following: ■ AP datapath does not block the ARP request from the AP with the DHCP VLAN address. ■ If there is a wired or wireless client connected to AP and has the same IP address, the ARP reply is dropped by ARP as an ARP spoof. But, if this IP address does not belong to a client that is connected to AP, the ARP reply is forwarded. **Scenario:** This issue occurred when a route-cache entry was added with the AP local DHCP address and VLAN. But, when an ARP request which was with the same IP address as that of the AP's DHCP server was received by the AP, the AP datapath dropped the ARP request due to a mismatch in VLAN information. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
175741	**Symptom:** LLDP-MED did not get enabled on the ports E1 through E3 of an AP although the configuration was applied on all ports. The fix ensures that LLDP-MED gets enabled on the ports E1 through E3. **Scenario:** This issue was observed in AP-203R and AP-203RP access points running ArubaOS 8.2.0.0 or later versions.	AP Datapath	AP-203R and AP-203RP access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
175763	**Symptom:** The **mDNS** process crashed and rebooted frequently on a managed device. The fix ensures that the crash does not occur. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.	AirGroup	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0
175841	**Symptom:** An AirGroup server table or AirGroup user table displayed stale entries. The fix ensures that the AirGroup server table or AirGroup user table does not display stale entries. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.0.2.	AirGroup	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0
175852	**Symptom:** A managed device displayed the **Save failed: Module Authentication is busy. Please try later** error when the user attempted to save the configuration. The fix ensures that users are able to save the configuration changes in the managed device. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175945	**Symptom:** A stand-alone controller acting as a DHCP server for multiple VLAN pools tagged DHCP-offer packets with the wrong VLAN. The fix ensures that the DHCP-offer packets are tagged with the correct VLAN. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.0.0.0.	VLAN	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.0
175974 176628	**Symptom:** The jumbo configuration on port channel did not apply to a 40 gibabitethernet member interface after a reload of the managed device. This issue is resolved by ensuring that the jumbo configuration to member ports is applied when ports are added. **Scenario:** This issue occurred because FPAPPS received the port channel configuration earlier than the member ports information from LAGM. After the managed device reloaded, the MTU size was 1752 bytes instead of 9216 bytes. This issue was observed in 7280 managed devices running ArubaOS 8.2.1.0.	Port-Channel	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.0
176001	**Symptom:** The output of the **show amon-receiver interest-table** command did not display AMON message registrations although the **nbapi_publish** parameter was enabled in the **ale-configuration** command. The fix ensures that AMON message registrations are displayed. **Scenario:** This issue occurred when a Mobility Master was reloaded immediately after enabling the **nbapi_publish** parameter. This issue was observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions.	NBAPI	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.0
176029	**Symptom:** The CLI help text for the **tunnel** parameter in the **via connection-profile** command did not show the maximum number of VIA tunneled networks that can be configured. This issue is resolved by modifying the CLI help text so that users are aware of the maximum limits. **Scenario:** Without this help text, users were unable to know the maximum number of allowed VIA tunneled network configurations. This issue was not limited to any specific platform or ArubaOS version.	CLI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176118	**Symptom:** Users were unable to save the changes that were made in the **Guest Email** tab under **Mobility Master** > **Configuration** > **Services** > **Guest Provisioning** > **Guest Email** page. The fix ensures that users are able to save the changes. **Scenario:** This issue occurred when users attempted to edit and save the changes that were already configured in the WebUI. This issue was observed in Mobility Masters running ArubaOS 8.2.0.2 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0
176322	**Symptom:** An AP received the IP address from an incorrect VLAN although the VLAN was changed through **device-profile** on the switch. This issue is resolved by ensuring that the AP receives the IP address from the correct VLAN. **Scenario:** This issue occurred because the switch VLAN configuration did not change before the AP sent the DHCP information. This issue was observed in APs running ArubaOS 8.1.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.3.0.0
176344	**Symptom:** The cached ACR licenses were not preserved on the licensing server after upgrading a Mobility Master. The fix ensures that the cached ACR licenses are preserved. **Scenario:** This issue occurred when a Mobility Master was upgraded to ArubaOS 8.2.0.0 or later versions. This issue was not limited to any specific platform.	Licensing	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
176404	**Symptom:** An AP did not send GARP, when initialization was in progress. The fix ensures that the AP sends GARP when an interface is UP. **Scenario:** This issue occurred when an IP address was assigned to the interface. So, when a new AP was statically allocated with an old AP's IP address, the devices on the LAN were not notified and the ARP table was not updated. As a result, devices had to wait for the ARP entry to expire or for the new AP to send a message. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176430	**Symptom:** Some APs sent ARP requests for a gateway with an incorrect IP address. The fix ensures that the APs send correct IP addresses for ARP request. **Scenario:** The issue occurred in the following scenarios: ■ When APs disconnected from the managed device. ■ When the DHCP server was unreachable. ■ When the gateway was unreachable. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
176444	**Symptom:** The startup wizard did not allow adding licenses to a stand-alone controller. The fix ensures that the licenses are added successfully. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.2.1.0.	Controller - Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.0
176607	**Symptom:** A client that was connected to an AP failed to obtain an IP address. The fix ensures that the client obtains an IP address. **Scenario:** This issue occurred due to a memory leak in the APs with onboard or USB-based BLE radios. This issue was observed in AP-203H, 203R Series, AP-205H, 210 Series, 220 Series, 300 Series, 310 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points running ArubaOS 8.2.0.0 or later versions.	BLE	AP-203H, 203R Series, AP-205H, 210 Series, 220 Series, 300 Series, 310 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
176801	**Symptom:** The LMS Preemption did not work in a cluster setup. This issue is resolved by configuring the LMS and Backup LMS correctly. **Scenario:** This issue was observed when a backup LMS was configured as master and **active load balance** was enabled on the backup cluster. This issue was observed in a cluster setup running ArubaOS 8.1.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176885	**Symptom:** The syslog server displayed the **problem retrieving http_session from db: PGRES_FATAL_ERROR** error that originated from a Mobility Controller Virtual Appliance. This issue is resolved by performing the following actions: ■ Clearing inactive WebUI sessions at the expiry of idle timeout. ■ Sending an enhanced error message to the syslog server. **Scenario:** This issue was observed in Mobility Controller Virtual Appliances running ArubaOS 8.2.0.1.	Web Server	Mobility Controller Virtual Appliance	ArubaOS 8.2.0.1	ArubaOS 8.3.0.0
176930	**Symptom:** The OpenFlow and AirGroup processes did not learn the Per User Tunnel Node (PUTN) users. The fix ensures that the OpenFlow and AirGroup processes learn the PUTN users. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.0.	SDN	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.0
177009 177268 177336 178427	**Symptom:** The output of the **show memory lagm** command displayed a loss of memory in the LACP component of the **LAGM** process. The issue is resolved by fixing a memory leak in the **LAGM** process. **Scenario:** This issue occurred when LACP was enabled on any interface. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Port-Channel	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.0
177199	**Symptom:** The ZTP port was not defined for a managed device. This issue is fixed by adding the ZTP port definitions for the managed device. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 8.2.0.2 or later versions.	Configuration	7200 Series controllers	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0
177204	**Symptom:** The following streaming API and the CLI command on a managed device returned a value of 0 for Minimum RTT: ■ The **stats_ip_probe_uplink** streaming API ■ The **show ip health-check verbose** CLI command This issue is resolved by setting the Minimum RTT value to the lowest measured latency. **Scenario:** This issue occurred in managed devices with the **Uplink Health-check** configuration enabled. This issue was observed in 7000 Series and 7200 Series managed devices running ArubaOS 8.0.1.0.	Controller-Datapath	7000 Series and 7200 Series managed devices	ArubaOS 8.0.1.0	ArubaOS 8.3.0.0

Table 5: *Resolved Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177052	**Symptom:** An **mDNS** process memory leak occurred on a Mobility Master. The fix ensures that there is no memory leak. **Scenario:** This issue occurred when an AirGroup client changed the IP address. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.	AirGroup	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0
177522	**Symptom:** The **Controller discovery** field in **Campus APs** and **Remote APs** pages of the WebUI displayed an irrelevant option. The issue is resolved by changing the **DHCP** option to **Use AP discovery protocol (ADP)** under **Configuration** > **Access Points** > **Campus APs** page of the WebUI. **Scenario:** This issue occurred when users tried to provision APs by using the **Controller discovery** field in **Campus APs** or **Remote APs** page of the WebUI. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.0
177575	**Symptom:** The output of the **show interface gigabitethernet <slot/module/port> counters** command displayed incorrect count of unicast and multicast packets. The fix ensures that the following show commands work appropriately: ■ The output of the **show interface gigabitethernet <slot/module/port> counters** command displays the correct count of unicast packets on 40 Gbps ports. ■ The **show interface gigabitethernet <slot/module/port> counters** command and any other command do not display the count of unicast packets on the 1 Gbps and 10 Gbps ports. **Scenario:** This issue was observed in 7280 managed devices running ArubaOS 8.3.0.0.	Controller-Platform	7280 managed devices	ArubaOS 8.3.0.0	ArubaOS 8.3.0.0
178438	**Symptom:** Temporary folder was full. This issue is resolved by disabling the debug logs to a file in /tmp location. **Scenario:** This issue occurred due to **ctrlmgmtdbg** log files getting too large. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.0

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

Limitations

Following are the limitations observed in this release.

IOS Device Connectivity Issue

The iPad gets disconnected when the channel is changed from one frequency to another on a Mobility Master.

This issue is observed only in the latest IOS version, iOS 11.3.

No Support for Cell Size Reduction

Starting from ArubaOS 8.3.0.0, the **cell-size-reduction** parameter in **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands does not take effect for 300 Series access points. If the **cell-size-reduction** parameter has any configured value, the 300 Series access points disregard the value.

Known Issues

Following are the known issues observed in this release.

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
143800 156149 161721 162902 166512 170300 172955 172967 174101 177773	**Symptom:** The **OFA** process in a managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	SDN	All platforms	ArubaOS 8.2.0.0
149222	**Symptom:** The WebUI of a Mobility Master does not display any devices. **Scenario:** This issue occurs when a user configures a managed device from the **/mm/mynode** node hierarchy by using the CLI. This issue is observed in the WebUI of a Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.0.0.0
151952	**Symptom:** When a managed device reboots, APs and clients boot without IP address and other fields. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None.	Monitoring	All platforms	ArubaOS 8.0.1.0
154893	**Symptom:** The **Postgres** process in a managed device that is deployed in the cluster topology crashes unexpectedly. **Scenario:** This issue is observed in 7200 Series controllers running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	Database	7200 Series controllers	ArubaOS 8.1.0.0
159973	**Symptom:** Certificates loaded on a managed device do not synchronize between Mobility Master and the standby Mobility Master. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.1.0.0 or later versions. **Workaround:** Load these certificates on the Mobility Master.	Certificate Manager	All platforms	ArubaOS 8.1.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
160281	**Symptom:** A managed device stops forwarding packets on 40 Gbps ports unexpectedly. **Scenario:** This issue occurs when both 40 Gbps and 10 Gbps ports are enabled for jumbo traffic in the 7280 managed device. The network engine in the managed device stalls when jumbo packets (frame size larger than 1380) egress on 40 Gbps and 10 Gbps ports simultaneously. This issue is observed in 7280 managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** Avoid simultaneous jumbo packets egress on 40 Gbps and 10 Gbps ports of the 7280 managed devices.	Controller-Datapath	7280 managed devices	ArubaOS 8.2.0.0
160432	**Symptom:** VIA clients are not displayed in the **Dashboard > Clients** page of the WebUI. **Scenario:** This issue is observed on VIA clients that are connected to stand-alone controllers running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS8.1.0.0
164530	**Symptom:** The APPRF feature does not block the traffic that originates from Android-based mobile phones. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.1. **Workaround:** None.	DPI	All platforms	ArubaOS 8.1.0.1
165908 170224 171074 171396 173372 174322 174370 174917 177151 177457 177662 178307	**Symptom:** The **kernel** process in a managed device crashes and the managed device reboots unexpectedly. The log file lists the reason for the event as **control processor kernel panic**. **Scenario:** This issue is observed in 7200 Series managed devices running ArubaOS 8.2.0.0. **Workaround:** None.	Controller-Platform	7200 Series managed devices	ArubaOS 8.2.0.0
165943	**Symptom:** The **Dashboard** > **Info** page in the WebUI of a Mobility Master displays incorrect country information. **Scenario:** This issue occurs when **global-geolocation-acl** is configured on the Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
167110	**Symptom:** An AP fails to establish an IPsec tunnel when LMS is set to the VRRP IP address. **Scenario:** This issue occurs due to a race condition between **IKE** and **FPAPPS**. This issue is observed in a managed device running ArubaOS 8.1.0.2 or later versions. **Workaround:** Restart the **ISAKMPD** process using the **process restart isakmpd core** command.	VRRP	All platforms	ArubaOS 8.1.0.2
168645 176421	**Symptom:** A managed device does not receive configuration from the secondary Mobility Master. **Scenario:** This issue occurs when a FQDN is configured for the secondary **masterip** and **l3-peer-ip** is configured as a FQDN. The primary and secondary Mobility Master do not synchronize and a managed device does not receive the configuration from the secondary Mobility Master at failover. This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** Reload the managed device.	Master-Redundancy	All platforms	ArubaOS 8.2.0.0
168725 168727	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0
169216	**Symptom:** Data transfer from a Mobility Master Virtual Appliance setup to a Hyper-V switch stops unexpectedly. **Scenario:** When the throughput rate exceeds the threshold rate, the Hyper-V switch runs out of memory due to unlimited packets getting queued. This issue is observed in controllers running ArubaOS 8.2.0.0 or later versions. **Workaround**: None	Controller- Datapath	All platforms	ArubaOS 8.2.0.0
170058	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7200 Series controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Datapath	7200 Series controllers	ArubaOS 8.0.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
170249 175830	**Symptom:** Clients are unable to connect to some APs as the APs report 100% CPU utilization. **Scenario:** This issue is observed in 100 Series access points running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	100 Series access points	ArubaOS 8.0.0.0
171719	**Symptom:** A managed device fails to send the EAP-TLS request to its clients. **Scenario:** This issue occurs when the TLS exchange takes more than 10 seconds to complete. This issue is observed in managed devices running ArubaOS 8.1.0.4 or later versions. **Workaround:** None.	802.1X	All platforms	ArubaOS 8.1.0.4
171839	**Symptom:** A managed device stops responding and reboots. The log file for the event lists the reason as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:2).** **Scenario:** This issue occurs due to a session table corruption. 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
172464 175355	**Symptom:** A managed device has high CPU utilization and APs get disconnected. **Scenario:** This issue is observed in 7200 Series controllers running ArubaOS 8.3.0.0. **Workaround:** None.	Web Server	7200 Series controllers	ArubaOS 8.3.0.0
172862	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.0.0
172942	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
173070	**Symptom:** The role and count of clients that are displayed in the **AppRF** dashboard are different from those that are displayed in the CLI command output. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Firewall Visibility	All platforms	ArubaOS 8.0.0.0
173283	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert).** **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.4 or later versions. **Workaround:** Upgrade to ArubaOS 8.2.1.0.	Controller-Datapath	All platforms	ArubaOS 8.1.0.4
173395	**Symptom:** Some APs terminating on a managed device stop responding to pings randomly. **Scenario:** This issue occurs when some ICMP echo packets are dropped by the AP Ethernet driver. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** Reboot the AP.	AP-Wireless	All platforms	ArubaOS 8.0.0.0
173580	**Symptom**: The **Date and time** field in the **Configuration** > **General** > **Clock** page of the WebUI does not display values even though the NTP server is configured and synchronized with the system clock. **Scenario**: This issue is observed in managed devices running ArubaOS 8.2.0.1 or later versions. **Workaround**: None.	WebUI	All platforms	ArubaOS 8.2.0.1
173645	**Symptom:** False detections of type-5 radars are triggered in the FCC domain. **Scenario:** This issue is observed in 200 Series, 210 Series, and 220 Series access points running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.0.0.0
173746	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
173799	**Symptom:** An AP reboots continuously. The log file lists the reason for the event as **AP rebooted Wed Dec 27 11:23:51 EST 2017; Critical process /aruba/bin/meshd [pid 2413] DIED, process marked as RESTART**. **Scenario:** This issue occurs because **WPA Hexkey** values of the mesh recovery profile are incorrectly set. This issue is observed when APs operate in the mesh portal mode. This issue is not limited to any specific AP model or ArubaOS release version. **Workaround:** Perform one of the following actions: ■ Set **WPA Hexkey** parameter values correctly in the **ap mesh-recovery-profile** command in support mode. ■ Reprovision the AP.	Mesh	All platforms	ArubaOS 8.0.0.0
173825 175778	**Symptom:** The client count does not get updated in AirWave. **Scenario:** This issue occurs because a managed device sends a value of 0.0.0.0 for **lms_ip**. This results in AirWave not updating the client count. This issue is not limited to any specific platform or ArubaOS version. **Workaround:** None.	Activate/AirWave	All platforms	ArubaOS 8.2.0.0
173885 173887	**Symptom:** An AP rebootstraps because managed devices fail to retain the VRRP master state. **Scenario:** This issue occurs when the LACP link flaps on the managed device. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** Reboot the managed device.	Port-Channel	All platforms	ArubaOS 8.0.0.0
174010	**Symptom:** The captive portal page is not displayed for the clients in split-tunnel forwarding mode. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.1 or later versions. **Workaround:** None.	Captive Portal	All platforms	ArubaOS 8.2.0.1
174445	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
174725	**Symptom:** A managed device stops responding and reboots. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).** **Scenario:** This issue occurs due to a memory corruption. This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. **Workaround:** Disable AMSDU.	Controller-Datapath	All platforms	ArubaOS 8.1.0.0
174856	**Symptom:** The output of the **show firewall dns-names** command displays the error, **Module Authentication is busy. Please try later**, along with an outdated IP address list. **Scenario:** This issue occurs when users execute the **netdestination wechat** command to define destination hosts. This issue is observed in a cluster setups running ArubaOS 8.1.0.2 version. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.1.0.2
174898	**Symptom:** Multiple APs crash and reboot unexpectedly. The log file lists the reason for the event as **kernel panic: NSS FW coredump: bringing system down**. **Scenario:** This issue is observed in 310 Series and 320 Series access points running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	310 Series and 320 Series access points	ArubaOS 8.3.0.0
174943	**Symptom:** The **tx rate** value is displayed incorrectly when the **show ap debug radiostats** command is executed. **Scenario:** This issue is observed in 300 Series, 310 Series, 320 Series, and 330 Series access points running ArubaOS 8.2.0.1 or later versions. **Workaround:** None.	AP-Wireless	300 Series, 310 Series, 320 Series, and 330 Series access points	ArubaOS 8.2.0.1
174989	**Symptom:** A stand-alone controller crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue occurs due to a POE stall caused by overutilization of the forwarding plane. This issue is observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
175391	**Symptom:** After exchanging VoIP packets, an AP delays the scanning of data packets by 1 second, instead of the intended 30 milliseconds. **Scenario:** This issue occurs when the VoIP-aware scanning feature is enabled and the voice call has been completed. This issue is observed in APs running ArubaOS 8.3.0.0. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.3.0.0
175589	**Symptom:** Users are disconnected from APs due to insufficient resources on both 802.11a and 802.11g radios. **Scenario:** This issue is observed in AP-365 access points running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	AP-365 access points	ArubaOS 8.2.0.0
175610	**Symptom:** The log file of a managed device frequently displays the following error message: **0:<4>__ratelimit: 596 callbacks suppressed**. **Scenario:** This issue is observed in a cluster setup running ArubaOS 8.2.0.2 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.0.2
175660	**Symptom:** VRRP MACs overlap multiple two-node clusters when configured in the same L2 domain with CoA. **Scenario:** This issue is observed in cluster setups running ArubaOS 8.2.0.0 or later versions. **Workaround:** Use different VLAN IDs during VRRP configuration.	Cluster-Manager	All platforms	ArubaOS 8.2.0.0
175714	**Symptom:** The **D** flag (indicates dirty mode) is displayed against an AP in the WebUI and clients lose connectivity. **Scenario:** This issue is observed during an upgrade, when an AP moves to a different managed device while the original managed device reboots. This issue is observed in access points running ArubaOS 8.2.0.2. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.2.0.2
175928	**Symptom:** A managed device reboots unexpectedly. The log files lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 8.2.0.1. **Workaround:** None.	Controller-Datapath	7220 controllers	ArubaOS 8.2.0.1

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
176062	**Symptom:** A configured port is not displayed in the static port channel mode when a stand-alone controller is rebooted. **Scenario:** This issue occurs when the user executes the **show running config** or **interface port-channel** command after rebooting the controller. This issue is observed in 7210 controllers running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Port-Channel	7210 controllers	ArubaOS 8.2.0.0
176207	**Symptom:** A managed device is unable to apply bandwidth contract to wired users. **Scenario:** This issue occurs when multiple IP addresses are used for each MAC address. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.0.0.0
176330 177428	**Symptom:** The **Diagnostics > Technical Support > Copy Files** page in the WebUI displays success message although the TFTP file transfer fails. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.0.0
178016	**Symptom:** Some APs detect false radar signals and change radio channels frequently. **Scenario:** This issue occurs when the false radar typeid is 36. This issue is observed in AP-105 access points running ArubaOS 8.3.0.0. **Workaround:** None.	AP-Wireless	AP-105 access points	ArubaOS 8.3.0.0
178297	**Symptom:** Users get the **Name of the country needs to be matching one of the countries listed under 'show ip-geolocation countries'** error when they enter country name with spaces in the name in the CLI. **Scenario:** This issue occurs when users try to configure a country by using the **ip access-list geolocation global-geolocation-acl** command and the country name includes spaces in it. This issue is observed in 7008 stand-alone controllers running ArubaOS 8.3.0.0. **Workaround:** For a country name that includes a space, enclose the country name within double quotes while configuring through the CLI.	Controller-Platform	7008 controllers	ArubaOS 8.3.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
178839	**Symptom:** When an AP with static channel or EIRP is rebooted, the opmode changes on other Dual-5 GHZ APs as well. This results in 2.4 GHz APs getting EIRP computed for 5 GHz AP and vice-verse. **Scenario:** This issue occurs when the following conditions are met: ■ The Dual-5G APs are configured with static channels or EIRP. ■ The AP is rebooted. ■ The value of **dual-5ghz-mode** is set to **automatic** in the **ap system-profile**. This issue is observed in APs running ArubaOS 8.3.0.0. **Workaround:** ■ Do not have static channel or EIRP for Dual-5G AP. ■ If static channel or EIRP configuration is needed, then once the AP is rebooted, remove the static configuration and redo the configuration.	AirMatch	All platforms	ArubaOS 8.3.0.0
179000	**Symptom:** A reduction of power is observed in AP-345 access points. **Scenario:** This issue occurs as the antenna polarization is incorrectly programmed to calculate maximum TX power. This issue is observed in AP-345 access points running ArubaOS 8.3.0.0. **Workaround:** None.	AP-Wireless	AP-345 access points	ArubaOS 8.3.0.0
179047	**Symptom:** An AP crashes due to configuration changes. The log files lists the reason for the event as **PC is at wlc_apps_bss_ps_off_done+0x54/0x118 [wl] and LR is at wlc_mbss_shm_ssid_upd+0x2f8/0x330 [wl]**. **Scenario:** This issue is observed in AP-345 access points running ArubaOS 8.3.0.0. **Workaround:** None.	AP-Wireless	AP-345 access points	ArubaOS 8.3.0.0
179064	**Symptom:** The status of the Virtual AP is temporarily DOWN, resulting in clients getting disconnected. **Scenario:** This issue occurs when the radio band of the AP changes. This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.3.0.0

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

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

Topics in this chapter include:

Important Points to Remember

To upgrade your Mobility Master or managed device:

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

- If possible, use FTP to load ArubaOS images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- 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 you may require. For a detailed description of these new license modules, *Aruba Mobility Master Licensing Guide*.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Deleted the following files 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 57 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 57 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 57 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or 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
- Log files
- Flash backup

Backing up and Restoring Flash Memory

You can backup and restore the flash using the WebUI or CLI:

In the WebUI

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

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

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

In the CLI

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

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

   ```
   (host) #write memory
   ```
2. Execute the following command to back up the contents of the flash memory to the **flashbackup.tar.gz** file.

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

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

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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 56.

When you navigate to the **Configuration** tab in the WebUI, the managed device may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade from the WebUI and navigate to the **Configuration** tab as soon as the managed device completes rebooting. This error is expected and disappears after clearing the Web browser cache.

Before you upgrade Mobility Master from ArubaOS 8.0.0.0 to ArubaOS 8.3.0.0, take a note of the following points:

- ArubaOS 8.3.0.0 supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for Mobility Master Virtual Appliance. If you have 4 network adapters on your ArubaOS 8.0.0.0 Mobility Master Virtual Appliance, you must remove one before upgrading to ArubaOS 8.3.0.0 to avoid upgrade failure.

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

To remove a network adapter from ArubaOS 8.0.0.0 Mobility Master Virtual Appliance:

1. Log in to the vSphere client.

2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
3. Click **Edit Virtual machine settings**.
4. From the **Hardware** tab, select and remove a network adapter that is not active.

- Before upgrading to ArubaOS 8.3.0.0 from ArubaOS 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a Mobility Master Virtual Appliance or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
  1. From the **Managed Network** node hierarchy, select the managed device.
  2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
  3. Click **Submit** and click **Continue** in the reload popup.
  4. Click **Pending Changes**.
  5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

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

  ```
  (host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
  ```
- Before upgrading to ArubaOS 8.3.0.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

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

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

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

4. Log in to the ArubaOS WebUI from the Mobility Master.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** from the **Upgrade using** drop-down list.

b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.

6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. Disable the same, if you do not want to reboot immediately.

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

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

In the CLI

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

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

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

or

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

or

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

4. Execute the **show image version** command to check if the ArubaOS image is loaded on the flash 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 Backing up Critical Data on page 57 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 compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 57 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 57.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the 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 the 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 the managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. From **Select destination file** drop-down list, enter a file name (other than default.cfg).
   c. Click **Copy**.
2. Determine the partition on which your 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 the managed device reboots after the countdown period.
4. When the boot process is complete, verify that the Mobility Master or the managed device is using the correct ArubaOS version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, use the following command to copy it to the Mobility Master or the managed device:

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

   or

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

2. Set the Mobility Master or the managed device to boot with your pre-upgrade configuration file.

   ```
   (host) # boot config-file <backup configuration filename>
   ```

3. Execute the **show image version** command to view the partition on which your pre-upgrade ArubaOS version is stored. You cannot load a new image into the active system partition (the default boot).

   ```
   #show image version
   ```

4. Set the backup system partition as the new boot partition.

   ```
   (host) # boot system partition 1
   ```

5. Reboot the Mobility Master or the managed device.

   ```
   (host) # reload
   ```

6. When the boot process is complete, verify that the Mobility Master or the managed device is using the correct ArubaOS version .

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

Before Calling Technical Support

Provide the following information when you call Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with the IP addresses and Interface numbers.

- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information.