ArubaOS 8.2.0.0

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
Attn: General Counsel
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 05	■ Removed the **Migrating from ArubaOS 6.x to ArubaOS 8.x** section from **Upgrade Procedure** chapter as the Migration Tool is no longer supported. ■ Removed **Migration Guide** from the documents listed under **Related Documents** section as the Migration Tool is no longer supported.
Revision 04	Added description of bug **168501** under **Known Issues**.
Revision 03	Added bug **168645**.
Revision 02	Added a limitation on cluster rolling upgrade.
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 for the Aruba user-centric network:

- *ArubaOS Release Notes*
- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- *ArubaOS 8.x Syslog Message Guide*
- *Aruba Mobility Master Licensing Guide*
- *Aruba Mobility Master and VMC Installation Guide*
- *Aruba Wireless Access Point 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 higher on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 8.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

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

The following features or enhancements are introduced in this release.

AirGroup

Support for Hierarchical Configuration and Profiles

Starting from ArubaOS 8.2.0.0, the AirGroup service can be configured hierarchically to run in centralized or distributed mode. In the centralized mode, AirGroup runs on the Mobility Master and in the distributed mode, AirGroup runs on the node where it is configured. Further, AirGroup can be configured through AirGroup profiles over the command-line interface or WebUI.

ArubaOS Software

Support for Multiversion ArubaOS

ArubaOS 8.2.0.0 introduces the infrastructure essential for Mobility Master to support managed devices running different versions of ArubaOS software.

To support this enhancement, the minimum required ArubaOS version for Mobility Master and the managed devices in the network is ArubaOS 8.2.0.0. Hence, the actual implementation of this feature in the network is possible with the next ArubaOS release.

The Mobility Master can run an earlier or later ArubaOS version as compared with the ArubaOS version on the managed devices in the network; however, it is recommended that you run a later ArubaOS version on Mobility Master.

Layer-3 Redundancy for Mobility Master

ArubaOS 8.2.0.0 introduces support for a redundant pair of Mobility Masters. This prevents a scenario where a Mobility Master acts as a single point of failure if the link to the Mobility Master goes down, or a co-located standby Mobility Master VRRP controller pair fails due to a network failure or local natural disaster.

Access Points

AP Discovery Logic

Starting from ArubaOS 8.2.0.0, APs can run in either Controller-based mode or Controller-less mode. Based on the selected mode, the AP runs a different image:

- Controller-based APs run an ArubaOS image.

- Controller-less APs run an Instant image.

AP Deployment Policy

Starting from ArubaOS 8.2.0.0, users can predefine the AP deployment mode using the AP deployment policy. The AP deployment policy redirects the specified APs to the Instant discovery process, ensuring that the APs run only in controller-less mode.

Blacklisting Wired Clients

ArubaOS 8.2.0.0 introduces the support for blacklisting wired clients.

The following are the limitations of this feature:

- Functions only for wired clients on tunnel-based remote APs for secure jack operation.
- Supports blacklisting wired clients based on number of ACL entry hits.
- Is not supported in a cluster topology.

802.1x Authentication Using EAP-TLS

Starting from ArubaOS 8.2.0.0, APs support 802.1X authentication, using EAP-TLS.

AP-Platform

AP-203H Hospitality Access Point

The AP-203H access point is a high-performance flex-radio (software configurable as either single radio dual-band or dual radio) wireless device for hospitality and branch deployments. This AP uses Multiple-Input, Multiple-Output technology to provide secure wireless connectivity for both 2.4 GHz 802.11 b/g/n and 5 GHz 802.11 a/n/ac WiFi. This AP provides the following capabilities:

- Supports PoE-in (E0 port)
- Integrated BLE radio
- Central management configuration

For complete technical details and installation instructions, see *ArubaAP-203H Hospitality Access Points Installation Guide*.

AP-203R Series Wireless Access Point

The AP-203R Series wireless access points (AP-203R and AP-203RP) are high-performance flex-radio wireless devices for hospitality and branch deployments.

These APs contain a dual band 802.11ac flex-radio and Ethernet ports to provide secure Wi-Fi. The wired Ethernet ports located on the back of this AP allow users to connect directly to the device when linked by an Ethernet cable. These APs provides 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 802.3 af PoE-out (E2 port) (AP-203RP only)
- Central management configuration
- Support for selected USB peripherals
- Integrated BLE radio

For complete technical details and installation instructions, see *ArubaAP-203R Series Wireless Access Points Installation Guide*.

AP-303H Series Hospitality Access Point

The AP-303H Series access point is a high-performance dual-radio wireless device for hospitality and branch deployments. This AP uses MIMO technology to provide secure wireless connectivity for both 2.4 GHz 802.11 b/g/n and 5 GHz 802.11 a/n/ac WiFi.

Alternatively, the wired Ethernet ports located on the bottom of the device allow users to connect to the device directly when linked by an Ethernet cable.

This AP can be attached to a standard single-gang wall box using the mount provided, or converted into a desk-mounted remote access point for branch office deployments using the AP-303H-MNTD mount kit (sold separately).

This AP provides 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/at PoE
- Central management configuration
- Supports PoE-in (E0 port)/PoE-out (E3 port)
- Support for selected USB peripherals
- Integrated BLE radio

For complete technical details and installation instructions, see *ArubaAP-303H Series Hospitality Access Points Installation Guide*

360 Series Outdoor Wireless Access Points

The 360 Series outdoor wireless access points (AP-365 and AP-367) support IEEE 802.11ac standards for high performance WLAN, and are equipped with two radios, which provide network access and monitor the network simultaneously. MIMO technology allows these APs to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services.

These outdoor wireless 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

- Compatible with IEEE 802.3af PoE
- Integrated BLE radio

For complete technical details and installation instructions, see *Aruba 360 Series Outdoor Wireless Access Points Installation Guide*.

Authentication

Bandwidth VSAs

Starting from ArubaOS 8.2.0.0, the managed device can assign per-user or per-group bandwidth rate on Layer 3 authenticated clients. To direct the managed device to enforce bandwidth rates for specific clients after successful Captive-Portal authentication, three RADIUS Vendor-Specific Attributes named Bandwidth-VSAs are added in the RADIUS Access-Accept packet.

Dynamic Data Support

Starting from ArubaOS 8.2.0.0, dynamic data for the included attributes in the RADIUS Attribute modifier is supported. Users can configure the dynamic value for each included attribute in the RADIUS modifier.

Support to Assign VLAN-ID to NAS Port for Dynamic RADIUS Modifier

Starting from ArubaOS 8.2.0.0, the client's VLAN ID can be assigned to the NAS port for the dynamic RADIUS modifier.

Certificate Enrollment Using EST

Starting from ArubaOS 8.2.0.0, support for enrollment of CA certificates using EST can be enabled using the CLI.

Configuration

Support for Moving and Renaming a Node

Starting from ArubaOS 8.2.0.0, a user-created node can be renamed using the WebUI and CLI.

SCP Server Support

Starting from ArubaOS 8.2.0.0, Mobility Master, managed devices, and controllers provide the Secure Copy (SCP) server support. By default, the SCP server functionality is disabled on Mobility Master, managed devices, andcontrollers. You can enable the SCP server functionality by using the Mobility Master or managed device CLI. There is no WebUI option to configure this functionality.

A new parameter, **scp**, is introduced in the **service** command to help configure the SCP server functionality. A new show command, **show scp**, is introduced to view the status of the SCP server functionality.

RADIUS COA RFC 5176 Support

Starting from ArubaOS 8.2.0.0 the following parameters are introduced:

- **event-timestamp-required**
- **replay-protection**
- **window-duration**

Controller-Datapath

Enhancement to interface gigabitethernet Command

Starting from ArubaOS 8.2.0.0, a new parameter, **none** is introduced in the **switchport trunk allowed** command for a Gigabitethernet interface. This parameter is used to remove all the VLANs from the list of allowed VLANs configured on a trunk port.

Controller-Platform

Infrastructure for Supporting Database Upgrade

ArubaOS 8.2.0.0 introduces the infrastructure to support database upgrade.

CLI

CLI Enhancements

The syntax for following parameters in the **interface gigabitethernet** command is updated:

```
ip access-group in <acl-name>
ip access-group out <acl-name>
ip access-group session <acl-name>
ip access-group vlan <vlanId> session <acl-name>
no ip access-group in
no ip access-group out
no ip access-group session
no ip access-group vlan <vlanId> session
```

The syntax for following parameters in the **interface range gigabitethernet** command is updated:

```
ip access-group in <acl-name>
ip access-group out <acl-name>
ip access-group session <acl-name>
ip access-group vlan <vlanId> session <acl-name>
no ip access-group in
no ip access-group out
no ip access-group session
no ip access-group vlan <vlanId> session
```

The syntax for following parameters in the **interface port-channel** command is updated:

```
ip access-group in <acl-name>
ip access-group out <acl-name>
ip access-group session <acl-name>
```

```
ip access-group vlan <vlanId> session <acl-name>
no ip access-group in
no ip access-group out
no ip access-group session
no ip access-group vlan <vlanId> session
```

The syntax for following parameters in the **interface vlan** command is updated:

```
ip access-group in <acl-name>
no ip access-group in
```

The syntax for following parameters in the **interface cellular** command is updated:

```
ip access-group session <acl-name>
no ip access-group session
```

The syntax for following parameters in the **interface tunnel** command is updated:

```
ip access-group in <acl-name>
no ip access-group in
```

The syntax for following parameters in the **crypto-local ipsec-map** command is updated:

```
ip access-group in <acl-name>
no ip access-group in
```

VRRP and LACP Logging and Debugging Commands

New logging commands are added to troubleshoot VRRP and LACP issues respectively. Additionally, you can also use the **show gsm debug channel vrrp_info** and **show gsm debug channel port_info** commands to debug VRRP and LACP related issues in the GSM channel.

Command to Show Rogue AP List

ArubaOS 8.2.0.0 introduces a new CLI command, **show wms rogue-ap list**. Executing this command shows the rogue AP list.

Modifications to IPM Priorities Commands

From ArubaOS 8.2.0.0, you can delete all configured IPM priorities for an AP system profile by executing a single command. In the CLI, the existing **ipm-power-reduction-step-prio delete-all** command is replaced with the **no ipm-power-reduction-step-prio all** command. This command deletes all configured IPM priorities for an AP system profile.x`

Starting from ArubaOS 8.2.0.0, the output of the **show ap system-profile <profile-name> | include IPM** command is modified to display a new output parameter, **IPM Steps delete all**.

Starting from ArubaOS 8.2.0.0, the **no ipm-power-reduction-step-prio ipm-step <ipm-step> priority <priority number>** subcommand for the **ap system-profile <profile>** command set is simplified. If you want to remove one step or priority, you only need to specify the step and not the priority. For example, **no ipm-power-reduction-step-prio ipm-step <ipm-step>**.

Cluster

Mesh AP and RSDB Support for Cluster

Starting from ArubaOS 8.2.0.0, cluster is now supported with Mesh APs and Real Simultaneous Dual Band (RSDB).

IPv6 Support

Starting from ArubaOS 8.2.0.0, IPv6 support for cluster is added. A WebUI option is also added for IPv6 support. Also, IPv6 related debug commands, **show gsm debug channel sectun** and **scm intiate audit <peerip>** are updated.

AP LACP Support

Starting from ArubaOS 8.2.0.0, Cluster LAG is used to stripe traffic on a per UAC basis.

Cluster UI Enhancement

A new parameter called **group** is added to the cluster configuration. This field can be configured to influence the S-UAC and S-AAC assignments made by the cluster leader.

DHCP

DHCP Lease Limits Enhancement

Starting from ArubaOS 8.2.0.0, by default, the DHCP lease limits for the 7000 SeriesControllers are increased to those of the user limits. Also, a new CLI command, **ip dhcp increase-lease-limit**, is introduced in ArubaOS 8.2.0.0 for additional DHCP scope.

The following table provides the changes in the DHCP lease limits for the 7000 SeriesControllers in ArubaOS 8.2.0.0 as compared with those in previous releases:

Table 3: *DHCP Lease Limits and Additional DHCP Scope for 7000 SeriesControllers*

Platform	Recommended DHCP Lease Limit in Previous Releases	DHCP Lease Limit in ArubaOS 8.2.0.0	Additional DHCP Scope with CLI Option Enabled
7005 Controller	512	1024	2048
7008 Controller	512	1024	2048
7010 Controller	1024	2048	4096

Platform	Recommended DHCP Lease Limit in Previous Releases	DHCP Lease Limit in ArubaOS 8.2.0.0	Additional DHCP Scope with CLI Option Enabled
7024 Controller	1024	2048	2048
7030 Controller	2048	4096	4096

The output of the **show ip dhcp statistics** command is enhanced to show a warning if the DHCP lease limit of a 7005, 7008, or 7010 Controller is increased beyond the user limit.

Firewall Visibility

FW_AGG Sessions Message Enhancement

A new field called **client mac address** is added to the FW_AGG sessions message table to establish a relationship between the Station MAC address and the application details.

IPv6

AP IPv6 Bridge Mode Support

Starting from ArubaOS 8.2, IPv6 support for bridge mode is added.

Centralized Image Upgrade

IPv6 address support is added for Centralized Image Upgrade.

IPv6 DNS Support

Starting from ArubaOS 8.2, DNSv6 is supported.

DHCPv6 Relay

Starting from ArubaOS 8.2, DHCPv6 relay is supported.

IPv6 Ping Support

ArubaOS 8.2 allows users to ping IPv6 address, in the **Mobility Master** node hierarchy, using the **Diagnostics > Tools > Ping** tab.

IPv6 ULA for Authentication Server Host

Support for IPv6 Unique Local Address is added to enable configuration of authentication-server hosts.

Decrypt-Tunnel DMO Enhancement

ArubaOS 8.2.0.0 introduces implementation of Decrypt-Tunnel Dynamic Multicast Optimization (DDMO) for IPv6 wireless clients. With this enhancement, ArubaOS will optimize the multicast traffic for IPv6 wireless clients in the D-Tunnel mode by converting multicast transmission to unicast transmission.

Licensing

Support for VIA Licenses

ArubaOS 8.2 introduces the VIA license to support Virtual Intranet Access (VIA) or 3rd party VPN clients. Each Virtual Intranet Access (VIA) or 3rd party VPN client consumes a single VIA license. VIA licenses are not consumed for site-to-site VPNs. If a managed device or standalone controller has a PEFV license, that device will not consume VIA licenses from a licensing pool, as a single PEFV license supports all VIA and 3rd party VPN clients, up to the full user capacity for that device.

MultiZone

Hybrid CPsec, Mesh AP, and Mobility Controller Virtual Appliance Support

Starting from ArubaOS 8.2.0.0, hybrid CPsec is supported. That is, CPsec can be enabled or disabled independently for each zone and all the zone need not have the same CPsec configuration.

Starting from ArubaOS 8.2.0.0, MultiZone is supported for Mobility Controller Virtual Appliance with CPsec enabled. Therefore, a combination of hardware controllers and Mobility Controller Virtual Appliance are supported.

Starting from ArubaOS 8.2.0.0, Mesh is now supported on MultiZone.

Licenses for MultiZone

Starting from ArubaOS 8.2.0.0, data zone managed devices will not consume any license and only the primary zone managed devices will consume licenses. MultiZone requires RFP license.

Remote AP

Enhancements in USB Initialization of 4G/LTE Modem

Starting from ArubaOS 8.2.0.0, you can configure two AP Name (APN) during USB initialization of a 4G/LTE USB modem. While the first APN initiates the connection to obtain an IP address, the second APN sends and receives data. Use semicolon (;) as a delimiter to create two separate strings for the APN configurations in the following commands under the AP provisioning profile:

```
(host) (config) #ap provisioning-profile <profile-name>
(host) (Provisioning profile "<profile-name>") #usb-init <APN1-string>; <APN2-string>
```

Example

The following sample configuration includes the string values for two APN configurations:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #usb-init "AT+CGDCONT=1,\"IP\",\"APN1\";1,1,\"APN2\""
```

You must obtain the APN from your ISP and ensure that each APN entry follows the manufacturer's AT command reference.

Tunnel Node

Tunnel Node

Starting from ArubaOS 8.2.0.0, the per-port tunnel node and per-user tunnel node support is added on Mobility Controller Virtual Appliance.

UCC

Support for WiFi-Calling Service Provider Name

The output of the **show ucc call-info cdrs** command is enhanced to show the WiFi-calling service provider name.

WebCC

WebCC Distributed Mode

Starting from ArubaOS 8.2.0.0, the WebCC feature can be enabled in **Distributed** mode in addition to the default **Centralized** mode. If you configure WebCC in **Distributed** mode, the managed devices can download the URLs directly from Webroot® even if Mobility Master becomes unreachable.

WebUI

AP Search and Filter on Full Data Set

Starting from ArubaOS 8.2.0.0, users can search and filter APs from the **Configuration > Access Points** page in the WebUI.

AP Status Update in Dashboard

Starting from ArubaOS 8.2.0.0, when an AP is down, the status is displayed in the **Dashboard**.

Clock Accordion Enhancements

ArubaOS 8.2.0.0 introduces support for automatic time zone updates that include the relevant daylight savings time across time zones. This is implemented in the **Configuration > System > General > Clock** path, in view with keeping the time up-to-date and precise with daylight savings time adjustments effected automatically.

Clients page in Dashboard

Starting from ArubaOS 8.2.0.0, the **Clients** page in **Dashboard** has two tabs, **Clients** and **Authenticated users**. Also, this page now displays wired clients along with wireless clients.

Enhancements for ArubaOS Multiversion Support

In ArubaOS 8.2.0.0, the following WebUI enhancements are made in the managed devices, when the managed devices and the Mobility Master run different ArubaOS versions:

- Presentation of WebUI elements.
- Display of ArubaOS versions for Mobility Master and the managed device.

For more details on the WebUI enhancements for ArubaOS Multiversion support feature, refer to the *ArubaOS 8.2.0.0 User Guide*.

Enhancements to Diagnostics and Maintenance Tabs in the WebUI

ArubaOS 8.2.0.0 provides usability enhancements to the **Diagnostics** and **Maintenance** tabs.

Enhancement to Local IPsec Controller Authentication Keys

In the Mobility Master node of ArubaOS 8.2.0.0, a new option, **Mac-based PSK** is added in the following WebUI path:

Configuration > Controllers > Local Controller IPSec Keys > + icon > Add New IPSec Controller > Authentication drop-down list.

Enhancements to Pending Configuration in WebUI

Starting from ArubaOS 8.2.0.0, the Mobility Master WebUI allows you to view the configuration changes that are pending before submitting the changes.

Preferences Option in WebUI

ArubaOS 8.2.0.0 now introduces a new option, **Preferences**, in the **User** drop-down menu in the Mobility Master node. You can select or clear the **Show advanced profiles** check box to enable or disable the display of WLAN and AP Group advanced profiles, respectively. By default, the **Show advanced profiles** check box is disabled.

When you enable the **Show advanced profiles** option, the **Profiles link** is displayed on the following pages in the Mobility Master node or the Managed Device node.

- Mobility Master node > Configuration > System > Profiles > All Profiles
- Managed Device node > Configuration > WLANs
- Managed Device Node > Configuration > AP Groups

WebUI Support for Overrides

Starting from ArubaOS 8.2.0.0, the Mobility Master WebUI allows you to retain or remove overrides for the fields configured under a node.

WebUI Terminology Correction

The **Node Readability from SC** string in the **Dashboard > Cluster** page of the WebUI for Managed Network is now updated as **Node Readability from MM**.

This chapter describes the platforms supported in this release.

Mobility Controller Platforms

The following table displays the Mobility Controller platforms supported in this release.

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.2.0.0*

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

AP Platforms

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

Table 5: *Supported AP Platforms in ArubaOS 8.2.0.0*

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
200 Series	AP-204, AP-205

Table 5: *Supported AP Platforms in ArubaOS 8.2.0.0*

AP Family	AP Model
—	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-303H
310 Series	AP-314, AP-315
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
360 Series	AP-365, AP-367
—	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
—	RAP-3WN, RAP-3WNP

Chapter 4
Regulatory Updates

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at support.arubanetworks.com.

The following DRT file version is part of this release.

- DRT-1.0_61527

This release includes fixes for vulnerability documented in:

- WPA2 Key Reinstallation Vulnerabilities (CVE-2017-13077) - CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, and CVE-2017-13088
- ArubaOS Multiple Vulnerabilities - CVE-2017-9000 ,CVE-2017-9003, CVE-2016-10229 and CVE-2016-5195.
- Multiple Vulnerabilities in 'dnsmasq' - CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, and CVE-2017-14496

Additionally, the following issues are resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126176	**Symptom:** LLDP requests from multiple clients triggered unnecessary wired authentication requests and the wired authentication requests failed. The fix ensures that unnecessary wired authentication requests are blocked. **Scenario:** This issue occurred when wired authentication was coupled with MAC authentication. This issue was observed in managed devices running ArubaOS 6.4.2.4.	LLDP	All platforms	ArubaOS 6.4.2.4	ArubaOS 8.2.0.0
130889	**Symptom:** The **show ip interface brief** command did not include the VRRP address. This fix ensures that the **show ip interface brief** command includes the VRRP IPv4 or IPv6 address. **Scenario:** This issue was observed managed devices running ArubaOS 8.1.0.0.	VRRP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0
134168	**Symptom:** A tunnel-node did not move to complete state. This issue is resolved by enabling Per Port Tunnel Node/Per User Tunnel Node (PPTN/PUTN) on MM-VA. **Scenario:** This issue was observed in MM-VA with tunnel-nodes between managed devices where PPTN/PUTN was disabled	Mux	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
138254	**Symptom:** The client which was not involved in UAC failover was deleted after its flapped uplink was up. The log files for the event listed the reason as **observed ip_user delete** in Mobility Master. The fix ensures that client is not deleted **Scenario:** This issue occurred when shut is performed on the standby-UAC, and the sta/user/mac user/ip user entries were activated on the standby-UAC because it lost connectivity with the active UAC. This issue was observed in a cluster setup in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** The workaround is as follows: ■ Decrease the user idle timer to 30 secs in the cluster setup. ■ Once shut is performed, wait for at least a minute before performing no shut. This helps stabilizing the cluster environment.	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0
142081	**Symptom:** Controller path IPv6 packets were not captured for both TCP and UDP sessions. This issue is resolved by setting the appropriate options and its offset to type of protocol. **Scenario:** When the **show packet-capture contolpath-pcap** command was executed, the IPv6 packets were not filtered in the controlpath-pcap output. This issue was observed in Mobility Master and managed devices running ArubaOS 8.0.	IPsec	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0
142097	**Symptom:** User session terminates and the user is automatically logged out The fix ensures that the user session is not terminated when in **Dashboard**. **Scenario:** This issue is observed when the user is on any page of **Dashboard** and when the WebUI remains idle for longer than the set Idle Timeout value. This issue is observed in Mobility Master running ArubaOS 8.0.0.0.	WebUI	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0
148557	**Symptom:** Clients observed a sudden increase in the number of DHCPv6 or Multicast messages from the access points. This issue is resolved by making changes to the **SAPD** process. **Scenario:** This issue occurred when DHCP daemon for IPv6 sent DHCPv6 solicit messages when an AP received IPv4 addresses continuously. This issue was observed in managed devices running ArubaOS 6.4.4.9.	AP-Platform	All platforms	ArubaOS 6.4.4.9	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
148638	**Symptom:** Users were unable to remove **vpn-dialer default-dialer** from configuration group. This issue is resolved by making changes made to the validation logic that avoids mismatch between dialer parameter and token name. **Scenario:** This issue occurred when the dialer name was not copied to the correct parameter in the validation logic. As a result, there was a mismatch of token name and dialer parameter. This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0
151084 162101	**Symptom:** The **Dashboard** option in UI did not display the number of APs that were down. This issue is resolved by displaying status of the AP, when it is down, under the following options: **Dashboard > Access Points > Access Points** **Configuration > Access Points > Campus APs** **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	UI Configuration	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
151188 155048 156819 160570 162510	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **FW ASSERT at _tx_send_setup_ppdu_ params**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred in 300 Series, 310 Series, 320 Series, and 330 Series access points running ArubaOS 8.1.0.0 or later versions.	AP-Wireless	300 Series, 310 Series, 320 Series, and 330 Series access points	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
152576	**Symptom:** Trusted CA and public certificate entries were not visible on the standby managed device when configured from the **/mm** node of the Mobility Master WebUI. The fix ensures that the trusted CA and public certificate entries are visible on the standby managed device. **Scenario:** This issue was observed in standby managed devices running ArubaOS 8.0.1.0 or later versions.	Certificate Manager	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.2.0.0
156094	**Symptom:** Users received duplicate copies of broadcast and multicast packets. Improvements in handling the multicast packets for per-user tunnel node users fixed the issue. **Scenario:** This issue was observed in per-user tunnel node users in a cluster running ArubaOS 8.1.0.0.	Tunnel-Node-Manager	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
157287 167263 167432	**Symptom:** Poor voice or video call quality was experienced with devices connected to an access point. The fix ensures that the AP does not drop Rx data aggregates. **Scenario:** This issue occurred as AP was dropping Rx data aggregates during the call. This issue was observed in AP-303H access points running ArubaOS 8.1.0.0.	AP-Wireless	AP-303H access points	AP-303H 8.1.0.0	ArubaOS 8.2.0.0
157613	**Symptom:** The **Dashboard > WAN** page of the Mobility Master WebUI displayed the WAN uplink status incorrectly. The fix ensures that the WAN uplink status is displayed correctly on the **Dashboard**. **Scenario:** This issue was observed in a branch office setup running ArubaOS 8.1.0.0 or later versions.	UI-Monitoring	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
158446	**Symptom:** In a cluster setup, multicast video stream stopped after AP Anchor Controller (AAC) was modified during an active AP rebalance. The fix ensures that multicast is supported during an active AP rebalance. **Scenario:**This issue was observed in managed devices which were a part of a cluster running ArubaOS 8.1.0.0.	Multicast	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
158591	**Symptom:** Datapath process crashed on a Mobility Master upon increasing the flash size. The fix ensures that the system does not crash when the flash size is increased. **Scenario:** This issue occurred only when the flash size was increased on the Mobility Master Virtual Appliance or a Mobility Controller Virtual Appliance running ArubaOS 8.1.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
158600	**Symptom:** The WebUI allowed a user to choose the current VLAN-ID as the dynamic RADIUS modifier. The fix ensures that a user cannot select the current VLAN-ID as the dynamic RADIUS modifier. **Scenario:** This issue was observed in managed devices running ArubaOS 6.5.3.0.	WebUI	All platforms	ArubaOS 6.5.3.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
158911	**Symptom:** The **show license-usage ap** command on standalone license client (Mobility Controller Virtual Appliance250 (US)) did not display the country to which it belonged. The fix ensures that the country is displayed for standalone license client (Mobility Controller Virtual Appliance250 (US)) **Scenario:** This Issue was observed only in Mobility Controller Virtual Appliance-250 (US) and not in Mobility Controller Virtual Appliance-50 (US).	Configuration	Mobility Controller Virtual Appliance-250 (USA)	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
158950	**Symptom:** License manager crashed on standby managed device. The fix ensures that the license manager works as expected. **Scenario:** This issue was observed when license pool-profile on active Mobility Master was added or deleted and then, a failover to a backup managed device occurred. This issue was observed in a Mobility Master or a Mobility Master Hardware Appliance running ArubaOS 8.1.0.0.	Licensing	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
158974 167108 167336 167367	**Symptom:** An AP crashed and rebooted during a GRE tunnel tear down. The fix ensures that the AP does not crash while tearing down a GRE tunnel and works as expected. **Scenario:** This issue occured when an AP deleted the GRE tunnel after losing connectivity to its managed device. This issue was observed in AP-315 and AP-325 access points running ArubaOS 8.1.0.0 or later versions.	AP-Platform	AP-315 and AP-325 access points	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
159207 162707 165115	**Symptom:** Some clients were unable to obtain an IP address. The fix ensures that the clients obtain IP address appropriately. **Scenario:** This issue occurred because the controller dropped the DHCP ACK message from some clients. This issue was observed in managed devices running ArubaOS 8.0.1.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.2.0.0
159604	**Symptom:** Heartbeat failures were observed between an Aruba switch and a managed device when the user traffic rate was high. The fix ensures that the switch's heartbeat packets get distributed across the CPU cores. **Scenario:** This issue occurred because the heartbeat packets from the switch were not distributed across the managed device's CPU cores. This issue was observed in a managed device running ArubaOS 8.1.0.0 or later versions.	Tunnel-Node Manager	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
159770	**Symptom:** The **isakmpd** process crashed when MOBIKE protocol was used. The fix ensures that the hash table is generated correctly when MOBIKE updates the SA address. **Scenario:** This issue occurred because IKE was trying to access freed up memory. This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0
160125	**Symptom:** The **mDNS** process crashed. This issue is resolved by introducing a minimum length check to ensure that a packet which does not have any data is not processed. **Scenario:** The Mobility Master crashed when a packet sent to the MDNS port contained only the IP address and UDP header but did not contain any MDNS data. This issue was observed in a Mobility Master running ArubaOS 8.1.0.0.	AirGroup	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
160152	**Symptom:** Wireless clients could not establish multiple IPsec/VPN tunnels through the Mobility Controller Virtual Appliance that served as a NAT device. The fix ensures that the wireless clients are able to establish multiple IPsec/VPN tunnels through the Mobility Controller Virtual Appliance. **Scenario:** This issue occurred in the following scenario: ■ When source NAT was applied to the VPN traffic passing through a Mobility Controller Virtual Appliance. ■ When multiple VPN sessions were triggered on the Mobility Controller Virtual Appliance. This issue was observed in Mobility Controller Virtual Appliance running ArubaOS 8.0.0.0 or later versions.	IPsec	Mobility Controller Virtual Appliance	ArubaOS 8.0.0.0	ArubaOS 8.2.0.0
160353	**Symptom:** The output of the **show database synchronize** command displayed the error, **1705 synchronization have failed** when executed on a Mobility Controller Virtual Appliance. The fix ensures that the CLI output does not display mis-leading error messages. **Scenario:** This issue occurred because the database tried to synchronize a file that did not exist. This issue was observed on Mobility Controller Virtual Appliance running ArubaOS 8.0.1.0 or later versions.	Database	Mobility Controller Virtual Appliance	ArubaOS 8.0.1.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
160574	**Symptom:** The **WMS** process crashed in a Mobility Master. The fix ensures that the **WMS** process does not crash. **Scenario:** This issue occurred while processing a **Monitoring** query. This issue was observed in Mobility Masters running ArubaOS 8.1.0.0 or later versions.	Monitoring	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
160940	**Symptom:** In a stand-alone controller or a managed device, the per-user tunneled node users could not receive multicast stream. **Scenario:** This issue occurred when Cluster was disabled and when IGMP or MLD was enabled on a stand-alone controller or a managed device running ArubaOS 8.1.0.1.	Tunnel-Node Manager	All platforms	ArubaOS 8.1.0.1	ArubaOS 8.2.0.0
161014	**Symptom:** An error was displayed when an IP address in the reserved range was configured for establishing a Site-to-Site tunnel. This issue is resolved by removing the restriction in kernel versions 2.6.32, 2.6.34, and 3.6.18. **NOTE:** From ArubaOS 8.2.0.0, addresses beyond Global Unicast (2000::/3), Unique Local Unicast (fc00::/7), and Link Local Unicast (fe80::/10) are accepted. The restriction is removed only for the IPv6 Site-to-Site IPsec tunnel. **Scenario:** This issue occurred when users configured an IPv6 address (under interface VLAN) that was in reserved range as per IETF. The restriction in the kernel blocked the users from creating a Site-to-Site IPsec tunnel with reserved address ranges. This issue was not limited to any specific hardware platform or ArubaOS version.	IPv6	All Platforms	ArubaOS 8.1.0.0 FIPS	ArubaOS 8.2.0.0
161024	**Symptom:** The WebUI listed an unknown **Mobility Master**. The fix ensures the WebUI lists a valid **Mobility Master** when adding a new peer. **Scenario:** This issue occurred when SAs were not deleted while adding a new peer. This issue was observed in a Mobility Master running ArubaOS 8.1.0.0.	IPsec	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
161270	**Symptom:** Few APs were running in 80 MHz channels even when 80 MHz-support was disabled in the arm-profile. **Scenario:** This issue occurred when the arm-profile used was cloned from another profile. This issue was observed in 7010 standalone controllersrunning ArubaOS 8.1.0.0.	Configuration	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
161424	**Symptom:** Route ACL policies that use netdestination were lost after a reload of the Mobility Master. The fix ensures that the route ACL policies are intact after a reload. **Scenario:** This issue occurred due to an incorrect ordering sequence of the **route-acl** and **netdestination** commands that were sent to the authentication module. This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
161631	**Symptom:** A remote access point did not work with 4G-LTE USB MODEM. This issue is resolved by supporting the configuration of a second APN during USB initialization. **Scenario:** This issue occurred when a second APN was configured but not used in a Remote AP. This issue was observed in Remote APs running ArubaOS 8.1.0.0 or later versions.	Remote AP	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
161644	**Symptom:** Client traffic stopped because the AP sent a malformed reassociation response message. The fix ensures that the AP sends a valid reassociation response message. **Scenario:** This issue occurred after a client performed an 802.11r Fast BSS transition roam when Cluster was disabled on the Mobility Master.This issue was observed in AP platforms running ArubaOS version 8.0.0.0 or later versions.	Station Management	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
161839	**Symptom:** An error, **Error Determining image version** was displayed while upgrading a managed device from ArubaOS 8.1.0.0 to ArubaOS 8.1.0.1 using a TFTP server. The fix ensures that the image upgrade from a TFTP server is successful. **Scenario:** This issue occurred if the TFTP server ran on Windows systems whose default transfer mode is ASCII. This issue was observed only when upgrading a managed device from ArubaOS 8.1.0.0.	Controller-Platform	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
162038 166923	**Symptom:** The output of the **show ap debug system-status** command displayed incorrect speed and duplex information but, the **show ap debug port status** command displayed the correct information. The fix ensures that the **show ap debug system-status** command displays the correct speed and duplex information when the link is up or unknown when the link is down. **Scenario:** This issue was observed in access points running ArubaOS 8.1.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
162606	**Symptom:** An error, **Error Determining image version** was displayed while trying to modify the CPsec whitelist in the WebUI. The fix ensures that the CPsec whitelist modification is successful. **Scenario:** This issue occurred when the CPsec auto cert provisioning was turned off and the whitelisted AP showed an unapproved factory certificate in the CLI. This issue was observed in Controllers running ArubaOS 8.1.0.0 or later versions.	UI-Configuration	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
162888	**Symptom:** When one or more helper addresses were configured with three IPv6 addresses in a VLAN interface, it either failed to set the link address or set a wrong link address in the Relay-forward packets. The fix ensures that the source address selects the appropriate IPv6 address and sets it to the link-address in the Relay-forward packets. **Scenario:** This issue was observed when three IPv6 addresses were configured for a VLAN interface using the **ipv6 helper-address <DHCPServer / RelayAgent address>** command. This issue was observed in controllers and managed devices running ArubaOS 8.2.0.0.	DHCP	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.0
162956	**Symptoms:** The uplink client configured with prefix delegation failed to receive the IP address from the DHCP server because the IPv6 packets with incorrect prefix length was processed. The fix ensures that the server drops the packets that have prefix length greater than 64 and adds a syslog message. **Scenario:** This issue occured when DHCPv6 server was configured for IP address allocation. This issue was observed in Mobility Master running ArubaOS 8.1.0.0 or later versions.	DHCP	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
162996	**Symptoms:** The output of the **show memory debug verbose** command revealed a high memory utilization by the **ARM** process. This issue is resolved by fixing a memory leak in the **Monitoring** process. **Scenario:** This issue occurred when ARM was enabled on the Mobility Master. This issue was observed in Mobility Master running ArubaOS 8.1.0.0 or later versions.	ARM	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
163173	**Symptoms:** Multiple clients were not authenticated. The log file listed the reason for the events as **RADIUS-VSA: Error while parsing Vendor-Specific attribute with multiple sub-attributes in Access-Accept packet**. This issue is resolved by enhancing the **authentication** process to support multiple sub-attributes in a single RADIUS VSA. **Scenario:** This issue occurred in the **authentication** process during client authentication. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	RADIUS	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
163342	**Symptom:** LMS preemption partially failed when the Backup-LMS was part of a Cluster Controller. The fix ensures that the LMS preemption is successful. **Scenario:** This issue occurred when **ap-load-balance** was enabled on the Cluster. This issue was observed in ArubaOS 8.1.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
164108	**Symptom:** The configured MTU value of an AP was not reflected in standby managed device. This fix ensures that the configured MTU is reflected in standby managed device. **Scenario:** This issue occured when SAP MTU was configured in the AP system-profile. This issue was observed in a cluster setup running ArubaOS 8.1.0.1.	AP-Platform	All platforms	ArubaOS 8.1.0.1	ArubaOS 8.2.0.0
164257	**Symptom:** WAN configuration was missing from the Mobility Master WebUI though it was visible from the CLI. Improvements to the process handling WebUI queries fixed the issue. **Scenario:** This issue occurred when there was a case mismatch between the defined profile name and the WebUI referenced profile name. This issue was observed in a Mobility Master running ArubaOS 8.1.0.1 or later versions.	Configuration	All platforms	ArubaOS 8.1.0.1	ArubaOS 8.2.0.0

Table 6: *Resolved Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
164385	**Symptom:** When deploying a Mobility Master OVA file under Vcenter 6.5, the system displayed the error, **The provided manifest file is invalid: Invalid OVF manifest entry**. This issue is resolved by upgrading the OVA tool which includes the manifest of the OVF as required by Vcenter 6.5. **Scenario:** This issue occurred because the manifest of the OVF required by Vcenter 6.5 was not supported by the Mobility Master OVA file. This issue was observed in Mobility Master running ArubaOS 8.1.0.1.	Controller-Platform	All platforms	ArubaOS 8.1.0.1	ArubaOS 8.2.0.0
165135	**Symptom:** A user could not add VLAN ID and IPv6 address for source interface in RADIUS server through the WebUI. The fix ensures that a user can add VLAN ID and IPv6 address through the WebUI. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.0
166228 168270	**Symptom:** A user was unable to connect to a Wi-Fi network because a managed device was unresponsive. The fix ensures that users are able to connect to the Wi-Fi network. **Scenario:** This issue occurred when the mDNS CPU load was full. This issue was seen when a specific type of Google cast query was sent to a managed device. This issue was observed in 7240XM managed devices running ArubaOS 8.1.0.0.	AirGroup	7240XM managed devices	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
167098 167373 169128 169709	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first**. The fix ensures that the race condition causing the access points to crash is resolved. **Scenario:** This issue occurred because of a race condition. This issue was observed in AP-303H and AP-365 access points running ArubaOS 8.1.0.0 or later versions.	AP-Wireless	AP-303H and AP-365 access points	ArubaOS 8.1.0.0	ArubaOS 8.2.0.0
167679	**Symptom:** A Mobility Master tried to reach the wrong IP address of an Airwave server. This issue is resolved by correcting the endianess of the IP address. **Scenario:** This issue occurred because of wrong endianess. This issue was observed in Mobility Master running ArubaOS 8.1.0.2.	SNMP	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.2.0.0

This chapter describes the issues identified in this release.

Limitations When Filling Fields

The following limitations are observed when filling WebUI fields:

Special Characters

Avoid the following special characters in all name fields of any configuration:

- Less than (<)
- Greater than (>)
- One single quote (')
- One double quote (")

It is acceptable if the value of a string parameter is enclosed with opening and closing quote – single or double. Follow this process for all configurations which take string as an argument including but not limited to any profile names, AP names, location strings, ACL names, role names etc.

Mixed Cases for Key Names

The CLI is case insensitive. The user can enter the keynames in any case and they are stored in the case in which the user specified it (with a exceptions like ACL names, role names, and so on) and the references are matched in the case insensitive way. However, if a user wants to configure or use both WebUI and CLI for configuration, add the references in the same case as the original configuration. For example, if "ssid profile" is defined as "EmployeeSSID" and you want to use that in a Virtual AP, the ssid-profile under the Virtual AP should match the same case "EmployeeSSID". Even though the CLI accepts "employeeSSID" or "employeessid", it might not be displayed properly in the WebUI. Hence, maintain the case for the configuration similar across different objects or commands in the configuration.

Limitations When Creating Netdestination Entries

The following limitations are observed when creating netdestination entries:

- A single netdestination definition can have a maximum of 256 netdestination entries. On the whole, there can be a maximum of 1024 netdestination entries on the Controller or Managed Device.
- When a session or route ACL is configured, the product of the netdestination entries between two netdestination definitions (Source alias and Destination alias) cannot exceed 8192 netdestination entries.

AP and User Scalability Limitation

To support 6K APs and 64K users on MC-VA-10, increase the number of CPUs to 14.

Cluster Rolling Upgrade Limitation

Cluster Rolling Upgrade is not supported on mesh nodes. Therefore, a cluster upgrade cannot be performed for mesh deployments.

UCC Visibility for FaceTime Calls

The UCC heuristics is based on client signaling and port numbers.

- For clients running FaceTime version prior to version 10, the signaling occurs peer-to-peer and UDP port 16402 is used.
- For clients running FaceTime version 10 or later, the signaling occurs peer-to-server and UDP ports 16393 and 16394 are used. OpenFlow is not installed and the UCC heuristics are not visible on the Mobility Master.
- If one client runs FaceTime version prior to version 10 and another client runs FaceTime version 10 or later, UDP port 16402 is used for backward compatibility. OpenFlow is installed and UCC heuristics is visible.

Table 7: *Known Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version
140678	**Symptom:** The SNMP CLI commands are not case sensitive. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.0.1.0. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.0.1.0
143244	**Symptom:** Zone statistics are not segregated in the CLI output for the command, **show ap debug radio-stats ap-name <ap-name> radio <radio name> advanced**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0.0.0
142463	**Symptom:** Clients are disconnected and reconnected randomly. **Scenario:** This issue is observed when the radio on the Data Zone Mobility Master is enabled or disabled resulting in resetting of the Basic Service Set (BSS). This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0.0.0

Table 7: *Known Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version
149041	**Symptom:** AP comes up with an ID flag when CPsec is enabled. **Scenario:** This issue is observed when an AP is connected to a managed device through two VLANs, where VLAN 1 is the IP address of the managed device and the AP is connected directly to VLAN 2 on the same managed device. This issue is observed when CPsec is enabled. **Workaround:** Remove the IPv6 address from the VLAN 2.	AP-Platform	All platforms	ArubaOS 8.0.1.0
149222	**Symptom:** When a user configures a managed device from the **/mm/mynode** node hierarchy of the CLI, the Mobility Master does not display the devices in the WebUI. Only the devices configured from the **/mm** node hierarchy are displayed in the WebUI. **Scenario:** This issue is observed in the WebUI of a Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	IPsec	Mobility Master	ArubaOS 8.0.0.0
151906	**Symptom:** Application classification does not work on managed devices if unique application ID or name is not used. **Scenario:** This issue occurs when custom application scripts are added, deleted, and re-added with the same custom application ID or name. This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** If you are upgrading from ArubaOS 8.0.0.0 with custom applications configured, delete the customer applications and re-add them after upgrading to ArubaOS 8.0.1.0 or later vetsions. If you are adding, deleting, and re-adding custom applications in ArubaOS 8.0.1.0 or later versions, do not reuse the custom application ID or name. Instead, use different unique (previously unused) application ID or name.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
151952	**Symptom:** When the 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
152360	**Symptom:** The **Dashboard > Traffic Analysis > WLAN** page in the WebUI shows repetitive WLANs. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None	WebUI	All platforms	ArubaOS 8.0.1.0
153243	**Symptom:** HPE switches request licenses on Mobility Master. **Scenario:** This issue is observed in PUTN feature enabled HPE switches. **Workaround:** HPE switches do not consume any license on Mobility Master.	Tunnel-node-manager	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version
154893	**Symptom:** The **Postgres** process in a managed device 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 from the Managed Devices are not pushed from the Mobility Master to the standby Mobility Master. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.1.0.0. **Workaround:** Load the certificates on Mobility Master as well as the Managed device.	Base OS Security	All platforms	ArubaOS 8.1.0.0
161327	**Symptom:** The 802.1X EAP-TLS provisioning parameters are not available in the WebUI. **Scenario:** This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.2.0.0. **Workaround:** Use the command-line interface to configure the EAP-TLS provisioning parameters.	WebUI	All platforms	ArubaOS 8.2.0.0
162272	**Symptom:** A Mobility Master Virtual Appliance is in stuck state. **Scenario:** This issue occurs during a serial console redirect in a Mobility Master Virtual Appliance running ArubaOS 8.2.0.0. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.0.0
163452	**Symptom:** The kernel in an Mobility Master Virtual Appliance is unresponsive. **Scenario:** This issue occurs when the Mobility Master Virtual Appliance triggers sysrq. This issue is observed in a Mobility Master Virtual Appliance running ArubaOS 8.2.0.0. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.0.0
164916	**Symptom:** A managed device does not display an error when executing the **show license-pool-profile-root** command. **Scenario:** This issue occurs when the managed device is a license client. This issue is observed in a managed device running ArubaOS 8.2.0.0. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.2.0.0

Table 7: *Known Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version
167575	**Symptom:** A ClearPass Policy Manager server shows the **Radius <COA profile name> fails for client <mac-addr>** error message. **Scenario:** This issue occurs when a ClearPass Policy Manager server or RADIUS server initiates a Disconnect-Request to a managed device. The managed device disconnects the client but sends a negative acknowledgement to the ClearPass Policy Manager server or RADIUS server. This issue is observed in managed devices running ArubaOS 8.2.0.0. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.2.0.0
168146	**Symptom:** A Mobility Master Hardware Appliance does not download the activate whitelist from a managed device. **Scenario:** This issue is observed in a Mobility Master Hardware Appliance running ArubaOS 8.1.0.2. **Workaround:** None.	Branch Controller	Mobility Master Hardware Appliance	ArubaOS 8.1.0.2
168501	**Symptom:** APs crash unexpectedly when using Suite-B algorithm to enroll certificates using EST. **Scenario:** This issue occurs when the AP platforms do not support enrollment of Suite-B certificates like ECDSA-256 and ECDSA-384 using EST. This issue is observed in AP-135, AP-325, and AP-334 access points running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Certificate Manager	AP-135, AP-325, and AP-334 access points	ArubaOS 8.2.0.0
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
169012	**Symptom:** Multizone is not enabled on an AP. **Scenario:** This issue occurs when RFP is enabled after assigning multizone profile to an AP group. This issue is observed in a cluster running ArubaOS 8.2.0.0. **Workaround:** None.	AP Datapath	All platforms	ArubaOS 8.2.0.0

Table 7: *Known Issues in ArubaOS 8.2.0.0*

Bug ID	Description	Component	Platform	Reported Version
169216	**Symptom:** The packet outflow stops in a Mobility Master Virtual Appliance unexpectedly. **Scenario:** This issue occurs when a Mobility Master Virtual Appliance is deployed on Hyper-V and the line rate is 100%. This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.2.0.0. **Workaround:** None.	Controller-Datapath	Mobility Master Virtual Appliance	ArubaOS 8.2.0.0
169416	**Symptom:** A client disconnects from an AP and does not reconnect. The status of the AP status is displayed as **Unprovisioned, no such group** in the data zone. **Scenario:** This issue occurs when multizone is assigned to an AP group. This issue is observed in a cluster running ArubaOS 8.2.0.0. **Workaround:** None.	AP Datapath	All platforms	ArubaOS 8.2.0.0
169526	**Symptom:** Database synchronization fails between a primary and standby Mobility Master. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.2.0.0.	Database	All platforms	ArubaOS 8.2.0.0
169661	**Symptom:** An IPsec tunnel is not established when the value of the **src-net** parameter is set to **ANY**. **Scenario:** This issue is observed in managed device running ArubaOS 8.2.0.0. **Workaround:** Set the value of the **src-net** parameter to either the IP address or VLAN, and then reset it to **ANY**.	IPsec	All platforms	ArubaOS 8.2.0.0

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

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

Topics in this chapter include:

Migrating Licenses from ArubaOS 8.0.x to ArubaOS 8.2.x

If you are migrating from ArubaOS 8.0.x to ArubaOS 8.2.x, migrate the MC-VA licenses if the country type is restricted (US, JP, IL, EG).

Manually delete and add all MC-VA licenses after upgrading to the new ArubaOS version.

- Upgrade from ArubaOS 8.0.1.x or later releases.
  - No change if MC-VA license is not used.
  - If country type is one of restricted country type (US, JP, IL, EG), there is no country lock behavior.
  - Aruba recommends to upgrade to ArubaOS 8.1.0.0 for the country lock feature.
- New order in ArubaOS 8.0.1.0
  - After My Networking Portal (MNP) is updated based on the new country lock, use the part numbers that are part of ArubaOS part 8.1.0.0.
  - Use only MC-VA-XX-RW from MNP.
  - In ArubaOS 8.0.1 MC-VA-XX-US, MC-VA-XX-JP, MC-VA-XX-IL, MC-VA-XX-EG country licenses cannot be used after MNP update.
- Transfer to ArubaOS 8.0.1.x

- Applicable in case of RMA of ArubaOS 8.0.1.x.
- Transfer of license from MNP is supported only for RW license type.

- Upgrade from ArubaOS 8.0.1.x to ArubaOS 8.1.x
  - If you have configured one of the restricted country type (US, JP, IL, EG):
    - The existing licenses are considered as RW licenses. APs will be in unlicensed state for the restricted country types (US, JP, IL, EG).
    - Delete the existing MC-VA license.
    - Obtain a new license from MNP according to the country based on the order.
    - Apply the new license on standalone controller or Mobility Master to get country lock MC-VA.
    - Licenses other than MC-VA are not impacted.
  - If you have configured any country apart from the restricted country type (US, JP, IL, EG):
    - Existing licenses are considered as RW licenses.
    - APs will advertise the channels based on country if previous license are present.
    - No impact for non-restricted country types.

Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device have?
  - 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, refer *Aruba Mobility Master Licensing Guide*.

Memory Requirements

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

- Do not proceed with upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with 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 space, free some used memory. Copy any log files, crash data, or flash backups from your managed device, to any desired location. Delete the following files from the managed device to free some memory before upgrading:
  - **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 43 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 43 to back up the flash directory to a file named **flash.tar.gz**, and then 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 43 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 card. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

Deleting a CLI

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
- Flashbackup

Backing up and Restoring Compact Flash Memory

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

In the WebUI

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

1. In the Mobility Master node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the flash file system 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 system 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 backup 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 system 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 he 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.
```

Upgrade ArubaOS using the WebUI or CLI

The following sections provide the procedures for upgrading your WLAN network to the latest ArubaOS version using the WebUI or CLI.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 42.

NOTE

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

Before you upgrade Mobility Master from ArubaOS 8.0.0.0 to ArubaOS 8.2.0.0, take a note of the following points:

- ArubaOS 8.2.0.0 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 8.2.0.0 to avoid upgrade failure. To remove a network adapter from ArubaOS 8.0.0.0 Mobility Master Virtual Appliance:

NOTE

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

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

- Before upgrading to ArubaOS 8.2.0.0 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 8.2.1.0, 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 a local file.

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

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded at the factory. The Mobility Master or the 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 does not take effect until reboot. If you choose to reboot after upgrade, Mobility Master or the managed device reboots automatically.

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

In the CLI

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

1. Download ArubaOS image from the customer support site.
2. Open an SSH session on 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
```

8. Execute the **show version** command to verify that the upgrade is complete.

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

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 number. 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 device 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 43 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 the APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory, to an external server or mass storage facility. See Backing up Critical Data on page 43 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.

Before You Begin

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 43.
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.