ArubaOS 8.10.0.1 Release Notes

a Hewlett Packard
Enterprise company

Copyright Information

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components 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, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.

Contents

Chapter 1
Revision History

The following table lists the revision numbers and the corresponding changes that were made in this release:

Table 1: *Revision History*

Revision	Change Description
Revision 05	Added limitation on **Airtime Fairness Mode**.
Revision 04	Updated the **Important** section in the **Release Overview** chapter.
Revision 03	Updated the **Limitations** section in the **Known Issues** chapter.
Revision 02	Added the **Important** section in the **Release Overview** chapter.
Revision 01	Initial release.

Chapter 2
Release Overview

This ArubaOS release notes includes the following topics:

- New Features and Enhancements
- Supported Platforms
- Regulatory Updates
- Resolved Issues
- Known Issues and Limitations
- Upgrade Procedure

Important

- As mandated by the Wi-Fi Alliance, ArubaOS 8.10.0.x requires Hash-to-Element (H2E) for 6 Ghz WPA3-SAE connections. H2E is supported only on Windows 11, Linux wpa_supplicant version 2.10 and later versions. Hence, users must upgrade their Windows and Linux software for successful 6 Ghz WPA3-SAE connections.
- The factory-default image of APs introduced in ArubaOS 8.9.0.0 or later versions use **aruba-conductor** as the host name instead of **aruba-master** to identify a target managed device or stand-alone controller during DNS discovery. However, the factory-default image of APs that were introduced prior to ArubaOS 8.9.0.0 still use **aruba-master** during DNS discovery. The usage of **aruba-conductor** is to align with the Inclusive Language Initiative.

Related Documents

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

- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- *Aruba Mobility Conductor Licensing Guide*
- *Aruba Virtual Appliance Installation Guide*
- *Aruba AP Software Quick Start Guide*

Supported Browsers

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

Web Browser	Operating System
Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) or later	▪ Windows 10 or later ▪ macOS
Firefox 107.0.1 or later	▪ Windows 10 or later ▪ macOS
Apple Safari 15.4 (17613.17.1.13) or later	▪ macOS
Google Chrome 108.0.5359.71 or later	▪ Windows 10 or later ▪ macOS

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.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

Chapter 3
What's New

There are no new features, enhancements or behavioral changes introduced in this release.

This chapter describes the platforms supported in this release.

Mobility Conductor Platforms

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

Table 3: *Supported Mobility Conductor Platforms*

Mobility Conductor Family	Mobility Conductor Model
Hardware Mobility Conductor	MCR-HW-1K, MCR-HW-5K, MCR-HW-10K
Virtual Mobility Conductor	MCR-VA-50, MCR-VA-500, MCR-VA-1K, MCR-VA-5K, MCR-VA-10K

Mobility Controller Platforms

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

Table 4: *Supported Mobility Controller Platforms*

Mobility Controller Family	Mobility Controller Model
7000 Series Mobility Controllers	7005, 7008, 7010, 7024, 7030
7200 Series Mobility Controllers	7205, 7210, 7220, 7240, 7240XM, 7280
9000 Series Mobility Controllers	9004, 9012
9200 Series Mobility Controllers	9240
MC-VA-xxx Virtual Mobility Controllers	MC-VA-10, MC-VA-50, MC-VA-250, MC-VA-1K

AP Platforms

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

Table 5: *Supported AP Platforms*

AP Family	AP Model
200 Series	AP-204, AP-205
203H Series	AP-203H
203R Series	AP-203R, AP-203RP

Table 5: *Supported AP Platforms*

AP Family	AP Model
205H Series	AP-205H
207 Series	AP-207
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303 Series	AP-303, AP-303P
303H Series	AP-303H, AP-303HR
310 Series	AP-314, AP-315
318 Series	AP-318
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377
370EX Series	AP-375EX, AP-377EX, AP-375ATEX
AP-387	AP-387
500 Series	AP-504, AP-505
500H Series	AP-503H, AP-503HR, AP-505H, AP-505HR
510 Series	AP-514, AP-515, AP-518
518 Series	AP-518
530 Series	AP-534, AP-535
550 Series	AP-555
560 Series	AP-565, AP-567
570 Series	AP-574, AP-575, AP-577
580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX

Table 5: *Supported AP Platforms*

AP Family	AP Model
630 Series	AP-635
650 Series	AP-655

Chapter 5
End-of-Support

This chapter provides information on the Aruba products that are not supported for a particular release.

The following AP models will no longer be supported beginning with the next major release, ArubaOS 8.11.0.0 and higher:

- 200 Series
- 203H Series
- 203R Series
- 205H Series
- 207 Series
- 210 Series
- 220 Series
- 228 Series
- 270 Series
- 320 Series
- 330 Series
- 340 Series
- AP-387

Chapter 6
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 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 https://asp.arubanetworks.com/.

The following DRT file version is part of this release:

- DRT-1.0_84001

Chapter 7
Resolved Issues

ArubaOS now supports an updated Ethernet PHY transceiver in Aruba 650 Series and Aruba 580 Series access points.

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

Limitations

Following are the limitations observed in this release.

IP Default-Gateway Management Address

Aruba recommends to not configure the IP default-gateway management address for 7010, 7024, 7205, and 7280 controllers running ArubaOS 8.10.0.0.

650 Series and 630 Series Access Points

The 650 Series and 630 Series access points have the following limitations:

- No Wi-Fi uplink on the 6 GHz radio channel
- No spectrum analysis on any radio
- No Zero-Wait DFS
- No Hotspot and Air Slice support on the 6 GHz radio
- No 802.11mc responder and initiator functionality on any radio
- Only 4 VAPs on the 6 GHz radio instead of 16
- Maximum of 512 associated clients on any radio instead of 1024

6 GHz Channel Information in Regulatory Domain Profile

ArubaOS does not display the 6 GHz channel information in the existing regulatory domain profile of Wi-Fi 6E APs by default.

To include 6 GHz channel information, ensure that you change the country code to a different country code, apply the change, and then revert it to the original country code. Another option is to create a new regulatory domain profile that includes the 6 GHz channel information by default, or copy the existing regulatory domain profile into a new regulatory domain profile to save the configuration.

The following example configures a regulatory domain profile and specifies a valid 6 GHz band.

```
host) [mynode](config) #ap regulatory-domain-profile reg-635
host) [mynode] (Regulatory Domain profile "reg-635") #country-code US
host) [mynode] (Regulatory Domain profile "reg-635") #valid-6ghz-channel 165
```

No Support for 6 GHz Radio Band and WPA3-PSK-H2E in Wi-Fi Uplink

The Wi-Fi Uplink feature does not support 6 GHz radio band and WPA3-PSK-H2E encryption type for Wi-Fi 6E APs (630 Series and 650 Series access points).

Air Slice

Air Slice is partially enabled on 500 Series access points and 510 Series access points. However, WMM boost will be functional even if Air Slice high-priority queuing is disabled.

Airtime Fairness Mode

Airtime Fairness Mode is not supported in 802.11ax access points.

Known Issues

Following are the known issues observed in this release.

Table 6: *Known Issues in ArubaOS 8.10.0.1*

New Bug ID	Description	Reported Version
AOS-218844 AOS-222351 AOS-227400 AOS-231009	Mobility Conductor picks only 43% of the APs for cluster CRU. This issue is observed in Mobility Conductor running ArubaOS 8.8.0.0 or later versions.	ArubaOS 8.8.0.0
AOS-227404	After a reboot of the Mobility Conductor Virtual Appliance, the route cache entries for IPsec tunnel display the MAC address as 0. This issue is observed in L3 connected Mobility Conductor Virtual Appliances running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-227804	The AirMatch mode-aware feature takes all the APs, including dual-band and tri-band APs, into consideration, but post computation it considers only the dual-band APs and excludes the tri-band APs. This issue is observed in a managed device running ArubaOS 8.10.0.0	ArubaOS 8.10.0.0
AOS-228058	ArubaOS WebUI does not allow users to configure MTU size as 2500 for IPsec tunnels. This issue is observed in Mobility Conductors running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-228065	The **Dashboard** > **Overview** page of the WebUi display 0 for VLAN. This issue is observed in Mobility Conductors running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-228149	When the number of wired devices tagged to the managed device is more than 100, the wired devices are not flagged after activating the cluster. This issue is observed in a managed device running ArubaOS 8.10.0.0 in a cluster setup.	ArubaOS 8.10.0.0
AOS-228284	IPv6 reassembly failure is observed when packet size is greater than the tunnel MTU. This issue is observed in Mobility Conductors running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-228764	A few AP-655 access points running ArubaOS 8.10.0.0 crash and reboot unexpectedly. The log files list the reason for the event as **PC is at cnss_wait_for_cold_boot_cal_done+0xe0/0x124**.	ArubaOS 8.10.0.0
AOS-229094	A few wired servers are incorrectly marked with more than one flag in the output of the show---command. This issue occurs when ADP table does not get updated with the details of the VLAN. This issue is observed in managed devices running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0

Table 6: *Known Issues in ArubaOS 8.10.0.1*

New Bug ID	Description	Reported Version
AOS-229559	A wrong policy may be enforced when a combination of DPI application-based rules and WebCC-based policies are used. This issue is observed in a managed device running ArubaOS 8.7.0.0.	ArubaOS 8.7.0.0
AOS-229758	Clients are unable to obtain the IP address or forward traffic. This issue occurs when WPA2-PSK-AES and WPA-PSK-TKIP opmodes are used in decrypt-tunnel mode. This issue is observed in APs running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-231206	The **wpa3_sae process** crashes or is stuck in **PROCESS_NOT_RESPONDING_CRITICAL** state. This issue occurs due to timer corruption. However, this issue does not affect the connectivity of already connected clients. This issue is observed in managed devicesrunning ArubaOS 8.6.0.17 or later versions.	ArubaOS 8.6.0.17
AOS-231454	The show commands display an error message, **auth module busy**. This issue occurs when large number of netdestination configurations are added. This issue observed in Mobility Controllers running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-231490	Dynamic packet capture fails to generate the pcap file. This issue occurs when WPA3-SAE encryption is used. This issue is observed in AP-505 and AP-515 access points running ArubaOS 8.7.1.9 or later versions.	ArubaOS 8.7.1.9
AOS-231769	The downlink MU-MIMO transmission with negative gains are observed for Samsung S21 devices in 160 MHz channel. This issue is observed in APs running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-231849	Mesh Portal APs do not change channels even after AirMatch changes the channels. This issue is observed in APs that have only mesh vaps configured. This issue is observed in APs running ArubaOS 8.6.0.16 or later versions. **Workaround:** Configure a **wlan virtual-ap profile <name>** to resolve the issue.	ArubaOS 8.6.0.16
AOS-232049	AirGroup traffic fails to reach the **MDNS** process on Mobility Conductors running ArubaOS 8.10.0.0 in a Mobility Conductor-Managed Device topology. This issue occurs when the AirGroup traffic hits the **any any any permit** datapath ACL that appears before the OpenFlow ACL.	ArubaOS 8.10.0.0
AOS-232181	Some APs do not form GRE tunnels with the Mobility Conductor Virtual Appliances on ESXi hypervisor and the MTU size falls back to 1578 bytes. This issue occurs when the MTU size of the jumbo tunnels is set to 9000 bytes. This issue is observed in APs running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-232331	The AP multicast aggregation tunnel packets on managed devices do not reach the **MDNS** process on Mobility Conductors running ArubaOS 8.10.0.0. This issue occurs when the reboot of **STM** process on the **managed devices** changes the AP multicast aggregation tunnel ID, and the change is not detected by OpenFlow.	ArubaOS 8.10.0.0

Table 6: *Known Issues in ArubaOS 8.10.0.1*

New Bug ID	Description	Reported Version
AOS-232463	The **Remote Clients** table under **Dashboard** > **Overview** > **Clients** page in the WebUI displays incorrect value of client age under the **Age** column. This issue is observed in managed devices running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-232503	A few APs do not accept action messages and this results in random channel and power assignments. This issue occurs when the opmode is changed from Dual-band to Dual-5G. This issue is observed in APs running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-232606	The WebCC classification fails in centralized mode in a native IPv6 deployment. This issue is observed in Mobility Conductors and managed devices running ArubaOS 8.9.0.1 or later versions in a Mobility Conductor-Managed Device topology.	ArubaOS 8.10.0.0
AOS-232614	The multicast aggregation message, **stm_send_split_tunnel_status_to_mdns** is not sent to the **OFA** process. This issue occurs due to incorrect endianness. This issue is observed in 9000 Series controllers running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-232623	Multiple APs are incorrectly marked as forwarder on the same VLAN. This issue is observed in APs running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-232699	A mesh portal is converted into AAM mode and the radios in mesh points are disabled. This issue occurs when the AirMatch mode-aware feature is enabled. This issue is observed in APs running ArubaOS 8.10.0.0	ArubaOS 8.10.0.0
AOS-232757	A BLE southbound API connection is terminated when the characteristic discovery is interrupted. This issue is observed in a managed device running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-233010	The 2.4 GHz radio of an AP does not turn off in accordance with the AirMatch mode-aware decision. The log on the Mobility Controller shows that the AP is in AAM mode but the log on the managed device shows that the AP has not moved into AAM mode. This issue is observed in APs running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0
AOS-233098	Controller-generated traffic is always forwarded through the management port instead of the data port. This issue occurs when the IP default-gateway management address is configured in controllers. This issue is observed in 7010, 7024, 7205, and 7280 controllers running ArubaOS 8.10.0.0. **Workaround:** Aruba recommends to not configure the IP default-gateway management address for 7010, 7024, 7205, and 7280 controllers running ArubaOS 8.10.0.0.	ArubaOS 8.10.0.0

Chapter 9
Upgrade Procedure

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 Conductor, managed device, or stand-alone controller.

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device?
  - Are all managed devices running the same version of ArubaOS?
  - What services are used on your managed device (employee wireless, guest access, Remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load ArubaOS images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Aruba Mobility Conductor Licensing Guide*.
- With the introduction of the Long Supported Release (LSR) and Short Supported Release (SSR) terminology in ArubaOS 8.10.0.0, a Mobility Conductor running an LSR release supports managed devices running the same release and the three preceding releases. This is considered as N-3 support. This allows a customer to run the latest LSR, the previous SSRs and the previous LSR simultaneously. A Mobility Conductor running an SSR release supports managed devices running the same release and the two preceding releases. This would be considered N-2 support and is the same behavior as the pre-ArubaOS 8.10.0.0 MultiVersion support.

- Only for the ArubaOS 8.10.0.0 LSR release, ArubaOS 8.6.0.0 is treated as an LSR despite being beyond N-3. As such a Mobility Conductor running ArubaOS 8.10.0.0 supports managed devices running ArubaOS 8.10.0.0, ArubaOS 8.9.0.0, ArubaOS 8.8.0.0, ArubaOS 8.7.0.0 and ArubaOS 8.6.0.0.

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 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 the minimum flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 23 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 23 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 23 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 CLI.

In the WebUI

From the Mobility Conductor, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups.

In the CLI

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

Low Free Flash Memory

Sometimes, after extended use, the flash memory might get used up for logs and other files. The ArubaOS image has increased in size and this may cause issues while upgrading to newer ArubaOS images without cleaning up the flash memory.

Prerequisites

Before you proceed with the freeing up the flash memory:

- Ensure to always backup the configuration and flash memory. Issue the **backup configuration** and **backup flash** commands to backup the configuration and flash.
- Copy the **flashbackup.tar.gz** and **configbackup.tar.gz** files out of the controller. Then delete the **flashbackup.tar.gz** and **configbackup.tar.gz** files from the flash memory of the controller.
- Use only one partition for the upgrade activity and keep the other partition unchanged.

If you use the WebUI to perform an upgrade, a banner on the **Maintenance** page provides the following reminder to have sufficient free flash memory before initiating an upgrade.

For a healthy and stable system it requires free space of 360 MB for AOS v8.3 and 8.5, 570 MB for AOS 8.6 and 8.7 and 450 MB for AOS 8.8 and higher version in the /flash directory. Please make sure minimum required memory is available in /flash before upgrading to newer version.

Freeing up Flash Memory

The following steps describe how to free up the flash memory before upgrading:

1. Check if the available memory in **/flash** is greater than the limits listed in Table 7 for all supported controller models:

   Table 7: *Flash Memory Requirements*

Upgrading from	Upgrading to	Minimum Required Free Flash Memory Before Initiating an Upgrade
8.3.x	8.10.x	360 MB
8.5.x	8.10.x	360 MB
8.6.x	8.10.x	570 MB
8.7.x	8.10.x	570 MB
8.8.x	8.10.x	450 MB
8.9.x	8.10.x	450 MB
8.10.x	8.10.x	450 MB

   To check the available free flash memory, issue the **show storage** command. Following is the sample output from a controller with low free flash memory:

```
(host) [mynode] #show storage
Filesystem              Size    Available       Use     %       Mounted on
/dev/usb/flash3         1.4G    1014.2M         386.7M  72%     /flash
```

2. If the available free flash memory is less than the limits listed in Table 7, issue the following commands to free up more memory.
   - **tar crash**
   - **tar clean crash**
   - **tar clean logs**
   - **tar clean traces**

3. Issue the **show storage** command again to check if the available space in **/flash** is more than the minimum space required for ArubaOS upgrade as listed in Table 7
4. **If you are unable to free up sufficient flash memory, contact Technical Support. Do not reboot the controller.**
5. If sufficient flash memory is available, proceed with the standard ArubaOS upgrade. See Upgrading ArubaOS.
6. If a reboot was performed, you may see some of the following errors. Follow the directions below:
   - Upgrade using standard procedure. You may see some of the following errors:

     Error upgrading image: Ancillary unpack failed with tar error (tar: Short header).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Ancillary unpack failed with tar error (tar: Invalid tar magic).

     Please clean up the /flash and try upgrade again.

     Error upgrading image: Need atleast XXX MB space in /flash for image upgrade, please clean up the /flash and try upgrade again.

     Failed updating: [upgradeImageNew.c] extractAncTar (dev: /dev/usb/flash1 imgLoc: /flash/config/ArubaOS_70xx_8.8.0.0-mm-dev_78066
   - If any of the above errors occur, issue the **show image version** command to check for the default boot partition. The partition which was upgraded should become the default partition. Following is the sample output of the **show image version** command:

```
(host) [mynode] #show image version
---------------------------------
Partition               : 0:0 (/dev/usb/flash1) **Default boot**
Software Version        : ArubaOS 8.9.0.0 (Digitally Signed SHA1/SHA256 -
Production Build)
Build number            : 81046
Label                   : 81046
Built on                : Thu Aug 5 22:54:49 PDT 2021
---------------------------------
Partition               : 0:1 (/dev/usb/flash2)
Software Version        : ArubaOS 8.7.0.0-2.3.1.0 (Digitally Signed SHA1/SHA256 -
Developer/Internal Build)
Build number            : 0000
Label                   : arpitg@sdwan-2.3_arpitg-3-ENG.0000
Built on                : Tue Aug 10 15:02:15 IST 2021
```

   - If the default boot partition is not the same as the one where you performed the upgrade, change the default boot partition. Issue the **boot system partition <part_number>** command to change the default boot partition. Enter **0** or **1** for **part_number** representing partition 0:0 or partition 0:1, respectively.
   - Reload the controller. If any of the errors listed in step 4 were observed, the following errors might occur while booting ArubaOS 8.9.0.0.

```
Sample error:
[03:17:17]:Installing ancillary FS                    [ OK ]
Performing integrity check on ancillary partition 1   [ FAIL : Validating new
ancillary partition 1...Image Integrity check failed for file
/flash/img1/mswitch/sap/arm32.ari. Digest Mismatch]
Extracting Webui files..tar: Short read
chown: /mswitch/webui/*: No such file or directory
chmod: /mswitch/webui/wms/wms.cgi: No such file or directory
```

   - After the controller reboots, the login prompt displays the following banner:

```
**********************************************************************
```

```
* WARNING:  An additional image upgrade is required to complete the *
* installation of the AP and WebUI files. Please upgrade the boot   *
* partition again and reload the controller.                        *
*********************************************************************
```

- Repeat steps 1 through 5. If sufficient free flash memory is available, proceed with the standard ArubaOS upgrade procedure. See Upgrading ArubaOS.
- If sufficient free flash memory is not available, issue the **dir** and **dir flash** commands to identify large files occupying the flash memory.

- Exercise caution while deleting files. Contact Technical Support if you are not sure which large files in the **/flash** directory could be safely deleted to free up the required space.

  Issue the **delete filename <filename>** command to delete large files to free more flash memory.
- Check if sufficient flash memory is free as listed in Table 7.
- Proceed with the standard ArubaOS upgrade procedure in the same partition. See Upgrading ArubaOS.

Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Log files
- Flash backup

Backing up and Restoring Flash Memory

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

In the WebUI

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

1. In the Mobility Conductor 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 Conductor or managed device. For details, see Memory Requirements on page 20.

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 is displayed ccurs when you upgrade using the WebUI and navigate to the **Configuration** tab after the managed device reboots. This message disappears after clearing the Web browser cache.

In the WebUI

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

1. Download the ArubaOS image from the customer support site.
2. Upload the ArubaOS 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.

NOTE

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

4. Log in to the ArubaOS WebUI from the Mobility Conductor.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

NOTE

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

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

In the CLI

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

1. Download the ArubaOS image from the customer support site.
2. Open an SSH session to your Mobility Conductor.
3. Execute the **ping** command to verify the network connection between the Mobility Conductor 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 partition. 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 Conductor.

```
(host)#reload
```

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

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

Verifying the ArubaOS Upgrade

Verify the ArubaOS upgrade in the WebUI or CLI.

In the WebUI

The following steps describe how to verify that the Mobility Conductor is functioning as expected:

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. 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 23 for information on creating a backup.

In the CLI

The following steps describe how to verify that the Mobility Conductor 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 version** command to verify the ArubaOS image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. 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 23 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 23.
2. Verify that the control plane security is disabled.

3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.

4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade ArubaOS version.

When you specify a boot partition or copy an image file to a system partition, Mobility Conductor 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 the pre-upgrade flash backup from the file stored on the Mobility Conductor or managed device. Do not restore the ArubaOS flash backup file.
- Do not import the WMS database.
- If the RF plan is unchanged, do not import it. 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 Conductor or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.

   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.

   b. From **Select destination file** drop-down list, select **Flash file system**, and 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**, and click **Reboot**.

The Mobility Conductor or managed device reboots after the countdown period.

4. When the boot process is complete, verify that the Mobility Conductor or managed device is using the correct ArubaOS version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the ArubaOS version:

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

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

or

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

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

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

3. Execute the **show image version** command to view the partition on which your pre-upgrade ArubaOS version is stored.

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

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

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

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

5. Reboot the Mobility Conductor or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

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