ArubaOS 8.2.0.1

a Hewlett Packard
Enterprise company

Release Notes

Copyright Information

Open Source Code

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

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

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 03	■ 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 02	Added bug 168645.
Revision 01	Initial release.

Chapter 1 Release Overview

This ArubaOS release notes includes the following topics:

NOTE

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

Chapter 2
New Features and Enhancements

There are no features or enhancements introduced in this release.

Supported Hardware Platforms

This chapter describes the hardware platforms supported in this release.

Mobility Controller Platforms

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

Table 3: *Supported Mobility Controller Platforms in ArubaOS 8.2.0.1*

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 4: *Supported AP Platforms in ArubaOS 8.2.0.1*

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 4: *Supported AP Platforms in ArubaOS 8.2.0.1*

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_61955

Chapter 5
Resolved Issues

This chapter describes the issues resolved in this release.

Table 5: *Resolved Issues in ArubaOS 8.2.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167575	**Symptom:** A ClearPass Policy Manager server displayed the **Radius <COA profile name> fails for client <mac-addr> error message**. The fix ensures that the error message is not displayed in the ClearPass Policy Manager server. **Scenario:** This issue occurred when a ClearPass Policy Manager server or RADIUS server initiated a Disconnect-Request to a managed device. The managed device disconnected the client but sent a negative acknowledgment to the ClearPass Policy Manager server or RADIUS server. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1
168031	**Symptom:** A crash log from a managed device indicated incomplete core dumps. The fix ensures that the generated crash log contains the complete dump information. **Scenario:** This issue occurred when a managed device crashed and generated the logs. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1
168146	**Symptom:** A Mobility Master Hardware Appliance failed to download the activate whitelist from a managed device. The fix ensures that the Mobility Master Hardware Appliance successfully downloads the whitelist from a managed device. **Scenario:** This issue was observed in a Mobility Master Hardware Appliance running ArubaOS 8.1.0.2 or later versions.	Branch Controller	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.2.0.1
168507	**Symptom:** APs that were configured as Air Monitor or in Spectrum mode became inactive in secondary AP Anchor Controller. **Scenario:** This issue occurred when the cluster was enabled and if the APs were assigned a secondary AP Anchor Controller. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Station Management	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1

Table 5: *Resolved Issues in ArubaOS 8.2.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168530 164543 168773 168823	**Symptom:** Clients were unable to connect to the SSID. The fix ensures that the clients get authenticated appropriately. **Scenario:** This issue occurred when the APs failed to respond to 802.11 authentication requests. This issue was observed in AP-303H, 300 Series, 310 Series, 320 Series, 330 Series and 360 Series access points running ArubaOS 8.1.0.0 or later versions.	AP-Wireless	AP-303H, 300 Series, 310 Series, 320 Series, 330 Series and 360 Series access points	ArubaOS 8.1.0.0	ArubaOS 8.2.0.1
169010	**Symptom:** An AP failed to respond and rebooted. The log file listed the reason for the event as **Unhandled fault: external abort on non-linefetch (0x1008) at 0xe6000000**. The fix ensures that the AP runs as expected. **Scenario:** This issue was observed in 300 Series access points running ArubaOS 8.2.0.0.	AP-Platforms	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1
169327	**Symptom:** The Mobility Master displayed an error - **An internal system error has occurred at file server_group.c function cfg_server_group_item_int line 384 error Error: unknown server**. The fix ensures that the re-positioned server configurations are pushed to the managed device. **Scenario:** This issue occurred when the server configurations in the server group were re-positioned, but the new positions were not pushed to the managed device. This issue was observed in managed devices running ArubaOS 8.1.0.3 or later versions.	Base OS Security	All platforms	ArubaOS 8.1.0.3	ArubaOS 8.2.0.1
169568 169246 169314 169523 170181 170446	**Symptom:** A managed device stopped responding and rebooted. The log file for the event listed the reason as **kernel panic: Intent:cause:register 12:86:e0:2**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.0.1

Table 5: *Resolved Issues in ArubaOS 8.2.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169581 169880	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **kernel panic: Fatal exception in interrupt**. Improvements to the wireless driver of the AP resolved the issue. **Scenario:** This issue occurred due to a corruption in the memory of the AP. This issue was observed in AP-303H, 300 Series, 310 Series, 320 Series, 330 Series and 360 Series access points running ArubaOS 8.2.0.0.	Mesh	AP-303H, 300 Series,310 Series, 320 Series, 330 Series and 360 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1
170171	**Symptom:** A web server module that handles captive portal requests crashed intermittently on a managed device. The fix ensures that the web server module does not crash. **Scenario:** This issue occurred due to a high volume of Captive Portal requests to the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Captive Portal	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1
170217 170241	**Symptom:** Clients were unable to connect to an SSID when 802.11r was enabled on the managed device. The fix ensures that the clients successfully connect to the SSID without service interruption. **Scenario:** This issue occurred when the clients attempted a full 802.1x authentication after an 802.11r roam. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1

Table 5: *Resolved Issues in ArubaOS 8.2.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170346	**Symptom:** Some clients were unable to connect to an AP because the whitelist database of Campus AP was missing in the managed device. The fix ensures that the clients connect to the APs without service interruption. **Scenario:** This issue occurred due to irrelevant log messages in the log files. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Database	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1
170457	**Symptom:** A managed device dropped the vlan probe requests causing the cluster to remain in L3 connected state. **Scenario:** This issue occurred if **bcmc - optimization** was enabled on the vlan interface after reloading the managed devices in a cluster. This issue was observed in cluster setup running ArubaOS 8.2.0.0.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1
170803	**Symptom:** A managed device stopped responding and rebooted. The log file for the event listed the reason as **Nanny rebooted the machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when a management server was configured on the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.0.1

Chapter 6
Known Issues and Limitations

This chapter describes the issues identified in this release.

Table 6: *Known Issues in ArubaOS 8.2.0.1*

Bug ID	Description	Component	Platform	Reported Version
159921	**Symptom:** The **Dashboard > WAN** page of the Mobility Master WebUI displays the WAN uplink status incorrectly. **Scenario:** This issue is observed in a Branch office setup running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	UI-Monitoring	All platforms	ArubaOS 8.1.0.0
160389	**Symptom:** The **Dashboard > WAN> <node>** page of the Mobility Master WebUI displays only 5 uplinks. **Scenario:** This issue is observed in a Branch office setup running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	UI-Monitoring	All platforms	ArubaOS 8.1.0.0
160551	**Symptom:** An AP keeps declaring a stale IP as the master, and fails to come up even after purging the stale master IP from the AP boot environment variables. **Scenario:** This issue occurs because the AP restores all the cleared variables due to a backup restore feature. This issue is observed in APs running ArubaOS 8.1.0.0 or later versions. **Workaround:** Execute the **bootenv_backup.sh** script to clear the saved record.	AP-Platform	All platforms	ArubaOS 8.1.0.0
162605	**Symptom:** A wireless client appears to be active on to two different APs at the same time because one of the APs fails to age out the client entry from its user table. **Scenario:** This issue occurs when the wireless client roams from one AP to another AP that terminates on a different managed device. This issue is observed in 200 Series access points running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	AP-Wireless	200 Series access points	ArubaOS 8.1.0.1
164607 169102 169316	**Symptom:** An AP reboots unexpectedly. The log file for the event lists the reason as **"Reboot caused by kernel panic: L2 single-bit error detected"**. **Scenario:** This issue is observed in 300 Series access points running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	AP-Wireless	300 Series access points	ArubaOS 8.1.0.3

Table 6: *Known Issues in ArubaOS 8.2.0.1*

Bug ID	Description	Component	Platform	Reported Version
168060	**Symptom:** The **Authentication** module in a managed device crashes multiple times. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.2 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.1.0.2
168180	**Symptom:** The **profmgr** process crashes when the single instance default profile is modified by the administrator in disaster recovery mode. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0.1.0
168238	**Symptom:** The configuration push is interrupted when there is a connectivity issue between the Mobility Master and the managed device, which results in bad configuration. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0.1.0
168636	**Symptom:** Clients are unable to SSH to a controller from the APC. **Scenario:** This issue is observed in 7005 platforms running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Aruba Central	7005 controllers	ArubaOS 8.0.1.0
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
169112 170103	**Symptom:** An invalid error, **Failed to sync /flash/upload/custom/** is logged every 10 seconds in a Mobility Master. **Scenario:** This issue occurs when a captive portal profile is deleted from the Mobility Master. This issue is observed in Mobility Master running ArubaOS 8.1.0.1 or later versions. **Workaround:** None.	Captive Portal	All platforms	ArubaOS 8.1.0.1

Table 6: *Known Issues in ArubaOS 8.2.0.1*

Bug ID	Description	Component	Platform	Reported Version
170056	**Symptom:** Image upgrade using a local file fails on a managed device when upgrading from the Mobility Master WebUI. **Scenario:** The issue occurs when Safari or Google Chrome web browsers are used. This issue is observed in Mobility Master running ArubaOS 8.2.0.0 or later versions. **Workaround:** Use the Firefox web browser.	WebUI	All platforms	ArubaOS 8.2.0.0
170258	**Symptom:** Error logs display **Unexpected nanny runtime error at __get_core, 825, core file not found** in a managed device. **Scenario:** This issue occurs when the database runs out of memory at the time of core collection. This issue is observed in managed devices running ArubaOS 8.2.0.0. **Workaround:** Reload the managed device.	Controller-Platform	All platforms	ArubaOS 8.2.0.0
170695	**Symptom:** Auto Sign on with L2 authentication fails on a managed device. **Scenario:** This issue occurs when clients with SSO profile attempt 802.1x authentication. This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.2.0.0

Upgrade Procedure

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

CAUTION

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

Topics in this chapter include:

- Migrating Licenses from ArubaOS 8.0.x to ArubaOS 8.2.x
- Important Points to Remember on page 20
- Memory Requirements on page 21
- Backing up Critical Data on page 22
- Upgrade ArubaOS using the WebUI or CLI on page 23
- Downgrading ArubaOS on page 26
- Before Calling Technical Support on page 28

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).

NOTE

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 22 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 22 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 22 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

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 21.

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.

NOTE

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.

NOTE

> 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 22 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 22 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 22.
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:

NOTE

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.