ArubaOS 8.3.0.2

aruba
a Hewlett Packard
Enterprise company

Release Notes

Open Source Code

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

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 06	■ Removed **Migration Guide** from the documents listed under **Related Documents** section as the Migration Tool is no longer supported. ■ Removed the **Migrating from ArubaOS 6.x to ArubaOS 8.x** section from **Upgrade Procedure** chapter as the Migration Tool is no longer supported.
Revision 05	Revised bug 181143 and 193777.
Revision 04	Added workaround for bug 175550.
Revision 03	Added bug 168645.
Revision 02	Removed description for the bug 180650 from the known issues section.
Revision 01	Initial release.

This ArubaOS release notes includes the following topics:

Throughout this document, branch controller and local controller are termed as managed device.

For the list of terms, refer Glossary.

Related Documents

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

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

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

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

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

AP-Wireless

Mute AP Radio

Starting from this release, the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands include the **am-tx-mute** parameter. Enable the **am-tx-mute** parameter to prevent an AP that operates in the AM or spectrum mode from creating spurious transmissions during AP boot. By default, the **am-tx-mute** is disabled.

Enable the **am-tx-mute** parameter in the **rf dot11a-radio-profile** or **rf dot11g-radio-profile** command only for APs that operate in the AM or spectrum mode.

To enable the am-tx-mute parameter:

```
(host) (config) #rf dot11a-radio-profile default
(host) (config) (rf dot11a-radio-profile "default")#am-tx-mute
```

Management Users

Implementing Management User Audits

The administrator can track the following details:

- Location of the last successful login
- Date and time stamp of the last successful login
- Number of successful attempts over a period of time
- Number of unsuccessful attempts since the last successful login

Implementing Password Validation

When a PSK based management user changes the password, a check is added to ensure that there is at least a difference of 8 characters between the new password and the old password.

Configuring Concurrent Sessions

A check is added to limit the number of concurrent sessions that an administrator account can maintain. If the admin user tries to create a new session after the maximum concurrent user sessions limit is reached, then the system displays an error message and does not allow the user to login although the login credentials entered are valid.

This option can be configured only using the CLI.

Maintaining Standard Mandatory Notice and Consent Banner

Starting from this release, a configuration option is added to enable retaining the Login Banner on the WebUI login page until the user clicks the **I Accept** button. Only after which the login prompt is displayed.

Zeroizing TPM Keys

Starting from this release, you can zeroize a cryptographic module, this involves erasing sensitive parameters such as electronically stored data, cryptographic keys, and critical security parameters from a controller or an AP to prevent disclosure of information if the equipment is permanently and irreversibly decommissioned.

VIA Client Audit

Starting from this release, when a user authenticates and accesses the VIA client, a notification with details about the last successful logon date and time stamp is provided.

This chapter describes the hardware platforms supported in ArubaOS 8.3.0.2.

Mobility Controller Platforms

The following table displays the controller platforms that are supported in ArubaOS 8.3.0.2.

Table 3: *Supported Controller Platforms in ArubaOS 8.3.0.2*

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

AP Platforms

The following table displays the AP platforms that are supported in ArubaOS 8.3.0.2.

Table 4: *Supported AP Platforms in ArubaOS 8.3.0.2*

AP Family	AP Model
100 Series	AP-104, AP-105
103 Series	AP-103
103H Series	AP-103H
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135
170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1

Table 4: *Supported AP Platforms in ArubaOS 8.3.0.2*

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

Table 4: *Supported AP Platforms in ArubaOS 8.3.0.2*

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

Virtual Platforms

The following list displays the Mobility Master Hardware Appliance and Mobility Master Virtual Appliance platforms that are supported in ArubaOS 8.3.0.2.

- MM-HW-1K
- MM-HW-5K
- MM-HW-10K
- MM-VA-50
- MM-VA-500
- MM-VA-1K
- MM-VA-5K
- MM-VA-10K

The following list displays the Mobility Controller Virtual Appliance platforms that are supported in ArubaOS 8.3.0.2.

- MC-VA-10
- MC-VA-50
- MC-VA-250
- MC-VA-1K

Chapter 4
Regulatory Updates

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_65937

This chapter describes the issues resolved in this release.

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169256 175610 176992 182160	**Symptom:** Managed devices were unable to learn some ARP response it received from the APs. The fix ensures that the ARP responses are not dropped. **Scenario:** This issue occurred because session synchronization for some high value sessions from Active UAC to Standby UAC caused session table corruption, which led to the drop in ARP responses. This issue was observed in managed devices running ArubaOS 8.1.0.2 in a cluster setup.	Controller - Datapath	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.3.0.2
170249 172066 175830 175931 176688 179004 181990 182574 182752	**Symptom:** A client was unable to connect to an AP that reported 100% CPU utilization. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 100 Series access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	100 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.2
171230	**Symptom:** A client experienced intermittent packet loss. This issue is resolved by limiting the number of retries attempted when a client is unresponsive. **Scenario:** This issue occurred when a client did not send a deauthentication or disassociation request to an AP and became unresponsive. The AP attempted to communicate with the unresponsive clients and created an RTS and BAR storm in the network. Hence, other clients in the network experienced intermittent packet loss. This issue was observed in AP-205, AP-215, and AP-225 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-205, AP-215, and AP-225 access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.2

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174320 173924 174100 175992 176293 177665 178689 179464	**Symptom:** An AP did not support fast recovery. This issue is resolved by adding support for fast recovery on AP-303H, AP-305, AP-315, AP-325, and AP-335 access points. **Scenario:** This issue was observed in AP-303H, AP-305, AP-315, AP-325, and AP-335 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-303H, AP-305, AP-315, AP-325, and AP-335 access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.2
175140	**Symptom:** AP-325 access points were not coming up on the managed device. This issue was resolved by fixing IP reassembly code. **Scenario:** This issue occurred because of an issue in the reassembly code of the managed devices. This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.0.0.0 or later versions.	Controller - Datapath	AP-325 access points	ArubaOS 8.2.0.2	ArubaOS 8.3.0.2
176185	**Symptom:** An AirGroup profile did not take effect on a managed device when it was configured in centralized mode. This issue is resolved by increasing the limit of disallowed VLANs or disallowed roles to 128. **Scenario:** This issue occurred when AirGroup was enabled with more than 32 disallowed VLANs or disallowed roles. This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.	AirGroup	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.2
177045 180877	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when radio in the AP tried to reset PHY and the driver was stuck. This issue was observed in AP-203H and AP-207 access points running ArubaOS 8.3.0.0 or later versions.	AP-Platform	AP-203H and AP-207 access points	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177162	**Symptom:** The position of an ACL that was configured on the default **user-role** was changed unexpectedly. The fix ensures that a managed device retains the ACLs in the correct positions. **Scenario:** This issue occurred when a managed device was reloaded and at startup, the ACLs were loaded in the wrong sequence. This issue was observed in managed devices running ArubaOS 8.3.0.0.	Configuration	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2
177299 180021	**Symptom:** A Remote AP did not connect when an OCSP server was not reachable. This issue is resolved by allowing the Remote AP to connect when the OCSP server is not reachable and the **ocsp_default** environment variable is set to accept. **Scenario:** This issue occurred when the **ocsp_default** environment variable was set to accept and the OCSP server was not reachable. This issue was observed in Remote AP running ArubaOS 8.2.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.2
177891	**Symptom:** The **Authentication** process in a managed device crashed unexpectedly and a client was disconnected. This issue is resolved by ensuring that the role name is valid and not empty. **Scenario:** This issue occurred when a CPPM role download was configured but the role name was invalid or empty. This issue was observed in 7220 controllers running ArubaOS 8.2.0.2 or later versions.	Base OS Security	7220 controllers	ArubaOS 8.2.0.2	ArubaOS 8.3.0.2
178032	**Symptom:** A client dropped the connection to an AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when active-scan was enabled in an AP. However, after 1.5 seconds, a client did not transmit or receive any packet on non-home channel, did not send beacons, or disconnected from the AP and roamed to another AP. The AP did not report neighbors in active scanning channels (channel 1 through 9 and 5 GHz non-DFS channels). This issue was observed in access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2
178114 180746	**Symptom:** A Remote AP failed to come up. The fix ensures that the Remote AP works as expected. **Scenario:** This issue occurred when the MTU was not adjusted automatically. This issue was observed in AP-305 access points running ArubaOS 8.0.1.0 or later versions.	AP Datapath	AP-305 access points	ArubaOS 8.0.1.0	ArubaOS 8.3.0.2

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178523 184618 185593	**Symptom:** LACP was unable to work on ports 0/0/24 and 0/0/25. The fix ensures that the correct maximum number of ports per managed device is returned to the Mobility Master. **Scenario:** This issue occurred because an incorrect number of maximum ports supported per managed device was returned to the Mobility Master. This issue was observed in 7024 managed devices running ArubaOS 8.2.0.0 or later versions.	Port-Channel	7024 controller	ArubaOS 8.2.0.0	ArubaOS 8.3.0.2
178116 178234	**Symptom:** Error messages related to ofc-flow-manager was displayed in the logs although the OpenFlow controller was disabled. This issue is resolved by converting these error messages which are non-functional issues into warning messages. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	SDN-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2
178324	**Symptom:** The 5 GHz channel of an outdoor AP switched to channel 46 which was excluded in the regulatory-domain-profile. This issue is resolved by sending only the outdoor channel EIRP list for an outdoor AP. **Scenario:** This issue occurred when an outdoor AP randomly picked up a channel designated for use by an indoor AP from the exhaustive EIRP list. This issue was observed in outdoor access points running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.2
178419 180044 181059	**Symptom:** The mDNS radius requests were sent with the NAS-IP address in reverse order to the ClearPass Policy Manager. 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 managed devices running ArubaOS 8.3.0.0 or later versions.	AirGroup	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2
178498	**Symptom:** An AirGroup user could use Apple TVs on different AP groups. The fix ensures that the AirGroup users show all available information for the user. **Scenario:** This issue occurred when AirGroup was enabled in centralized mode with auto association. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions in a cluster setup .	AirGroup	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.2

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178462 179319 180173 180667 181235	**Symptom:** The **show memory debug** command did not include the **memory available** column. This issue is resolved by adding a new field, **MemAvailable** to display the available memory. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.2
179056 180149 180214 180324	**Symptom:** The status of the AP is displayed as DOWN in the WebUI but displayed as UP when you execute the command, **show ap database long** in the CLI. The fix ensures that the status is displayed correctly in the WebUI and CLI. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.2
179837 182068	**Symptom:** The usage time was incorrectly displayed in **Dashboard > Usage** page. There was a time difference when compared to the controller's clock that was set through NTP. The fix ensures that the correct usage time is displayed. **Scenario:** This issue occurred because the DST was not considered when calculating the usage time. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2
179867	**Symptom:** An AP switched to APM mode unexpectedly. This issue is resolved by checking the AP certificate information if the new bandwidth has channels available during bandwidth upgrade. If a channel is not available for the new bandwidth, a debug message is logged with the reason for the unsuccessful bandwidth upgrade. **Scenario:** This issue occurred during bandwidth upgrade when AirMatch changed the min-channel-bandwidth in the 5 GHz radio-profile of an AP to a value that did not match the AP certificate information for the country code. This issue was observed in access points running ArubaOS 8.2.1.0 or later versions.	AirMatch	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.2
180398	**Symptom:** A cluster upgrade did not go beyond the first node in a cluster. This issue is resolved by updating the correct model name of the device during upgrade. **Scenario:** This issue occurred when a wrong model name was applied to a device during upgrade. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.2

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
180400	**Symptom:** The derived VLAN of a client was changed to a different VLAN. This issue is resolved by not synchronizing the registration information of the client. Hence, MAC authentication occurs for the first time after a client disconnects and reconnects. The VLAN is cached for reuse during the next iteration. **Scenario:** This issue occurred when a client disconnected and reconnected back to the S-UAC after a cluster failover. This issue was observed in a cluster topology with managed device running ArubaOS 8.2.1.0 or later versions.	Cluster-Manager	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.2
181440 182153	**Symptom:** A Mobility Master on Hyper V took longer than usual to boot. The fix ensures that the Mobility Master boots as expected. **Scenario:** This issue occurred when the **rngd** process was not running. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2
182248 182524	**Symptom:** Although the cluster node was up, the cluster upgrade failed with the **Cannot upgrade cluster as cluster node is down** error message. The fix ensures that the cluster upgrade completes successfully. **Scenario:** This issue occurred when a Mobility Master was upgraded and reloaded and a managed device reconnected back to the Mobility Master. The ArubaOS version on the Mobility Master and the managed device was different and the managed device ignored the active master IP address information that was sent by the Mobility Master. This issue was observed in a topology with active and standby Mobility Masters when both active and standby Mobility Masters were upgraded to ArubaOS 8.2.1.1 while the managed devices were running ArubaOS 8.2.1.0 as cluster members.	Configuration	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.2
182590	**Symptom:** An error message, **Error reading transceiver ID Prom on 0/0/0** was displayed when the Small Form-factor Pluggable transceiver (SFP module) was connected to the controller. The fix ensures that the SFP modules are supported. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.3.0.0.	Controller-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.2

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182981	**Symptom:** XML data was displayed when the show license aggregate command was executed from API. The fix ensures that the JSON output is displayed instead of the XML data. **Scenario:** This issue occurred when the command was run over the API on the Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.3.0.1.	Configuration	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.3.0.2
183929	**Symptom:** The Edge browser did not redirect a user to the correct page after the user successfully completing Captive Portal authentication. This issue is resolved by redirecting the user to the correct page after a successful Captive Portal authentication. **Scenario:** This issue occurred when the redirect URI was not stored while storing the original URL. After successfully completing Captive Portal authentication, the user was redirected back the original URL instead of the URL with the redirect URI. This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.2
181143	**Symptom:** The same product key was generated when the Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was cloned. This issue is resolved by generating the product key based on the UUID of the system. **NOTE:** If a cloned Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance that runs any version lower than ArubaOS 8.2.2.0 was upgraded to ArubaOS 8.2.2.0 and higher, ArubaOS 8.3.0.2 and higher, or ArubaOS 8.4.0.0 and higher, in the respective releases, the serial number and passphrase were changed and all licenses associated with the older serial number were invalidated. Migrate or regenerate the existing licenses for the new serial number after the upgrade. Contact Aruba Technical Support before the upgrade. **Scenario:** This issue occurred when an OVA-based Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was deployed, an OVF template was exported, and the exported OVF template was deployed. This issue was observed in Mobility Controller Virtual Appliance or Mobility Master Virtual Appliance running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.2

Table 5: *Resolved Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182049	**Symptom:** A client lost connectivity with an AP. The fix ensures that the position of the validuser ACL deny rule is not changed and the client does not lose connectivity. **Scenario:** This issue occurred when the position of a validuser ACL deny rule was changed. This issue was observed in managed devices running ArubaOS 8.2.1.1.	Configuration	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.2

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

Known Issues

Following are the known issues observed in this release.

Table 6: *Known Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version
155936 182485 180912	**Symptom:** A managed device does not respond to the PPP LCP echo request messages from a PPPoE server. Hence, the PPPoE link is not usable. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.1. **Workaround:** None.	PPPoE	All platforms	ArubaOS 8.2.0.1
168180	**Symptom:** The **profmgr** process in a managed device crashes when a single instance default profile is modified in the 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
168636	**Symptom:** A client is unable to connect to a controller from Aruba Central using SSH. **Scenario:** This issue is observed in 7005 controllers 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

Table 6: *Known Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version
172217	**Symptom:** Write memory does not show configurations committed. **Scenario:** This issue occurs when a user configures ACLs, VLANs, and interface configuration and issues the **write memory** command. This issue is observed in managed devices running ArubaOS 8.2.0.1. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.0.1
172857 178662	**Symptom:** The **BOCMGR** process in a Mobility Master crashes unexpectedly. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.3.0.0
175138	**Symptom:** The **Configurations > Services > Guest provisioning** page appears blank and non-editable. **Scenario:** This issue occurs when user enters **&** character in the email fields and submits the changes. This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions. **Workaround:** None.	Guest Provisioning	All platforms	ArubaOS 8.2.0.2
175550	**Symptom:** User cannot disable the security logging for the **aaa** process using the **logging security process aaa subcat aaa level debugging** command. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions. **Workaround:** Each time a managed device reboots, execute the following command in the CLI: ■ **Logging security subcat aaa level debugging** **Write memory** ■ **No logging security subcat aaa** **Write memory**	Configuration	All platforms	ArubaOS 8.2.0.2
175717 178608	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Master Initiated Reboot (Intent:cause:register 59:86:50:2)**. **Scenario:** This issue is occurs when a managed device is deleted and re-added in the hierarchy. This issue is observed in managed devices running ArubaOS 8.2.0.2. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.0.2

Table 6: *Known Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version
176330 177428	**Symptom:** The **Diagnostics > Technical Support > Copy Files** page of the WebUI displays a success message although the TFTP file transfer fails. **Scenario:** This issue occurs when a user attempts to copy a file using TFTP. This issue is observed in Mobility Master running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.0.0
176952	**Symptom:** The **/flash/upload** directory is available to unauthenticated users. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.0. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.0.0
177204	**Symptom:** The following streaming API and the CLI command on a managed device returns a value of 0 for Minimum RTT: ■ The **stats_ip_probe_uplink** streaming API ■ The **show ip health-check verbose** CLI command **Scenario:** This issue occurs in managed devices with **Uplink Health-check** configuration enabled. This issue is observed in 7000 Series and 7200 Series controllers running ArubaOS 8.0.1.0. **Workaround:** None.	Controller-Datapath	7000 Series and 7200 Series controllers	ArubaOS 8.0.1.0
177509	**Symptom:** User is unable to ping the servers behind the VVA from a managed device. **Scenario:** This issue occurs when the managed device obtains configuration after a reload. This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
177618	**Symptom:** The **sapd** process crashes in an AP. **Scenario:** This issue occurs when two APs have the same AP name. This issue is observed in access points running ArubaOS 8.2.0.2. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.2.0.2
177800	**Symptom:** Aruba Central agent debugging logs contain the hash value for the certificate sign challenge. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Logging	All platforms	ArubaOS 8.0.1.0

Table 6: *Known Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version
178760 179949 179950	**Symptom:** Instant APs connecting to a managed device is obtaining reversed IP address. **Scenario:** This issue occurs when a MAC address of an Instant AP is configured with a remote-ip address in whitelist-db. This issue is observed in Mobility Controller Virtual Appliance running ArubaOS 8.3.0.0. **Workaround:** None.	CPsec	All platforms	ArubaOS 8.3.0.0
178783	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0
179267	**Symptom:** The WebUI shows the **Invalid MAC address** error when adding a MAC address in the **Managed Network > Configuration > Access Points > Whitelist** page. **Scenario:** This issue occurs when a MAC address does not include the : (colon) character. This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.3.0.0
179485	**Symptom:** A Mobility Master reboots unexpectedly. The log file lists the reason for the event as **profmgr** process crash. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.2.1.0. **Workaround:** None.	L2 Forwarding	All platforms	ArubaOS 8.2.1.0
179942	**Symptom:** A client is not able to send or receive traffic to or from an AP. **Scenario:** This issue occurs when the station management process in an AP PAPI message to the AAC instead of the UAC. This issue is observed in Mobility Master running ArubaOS 8.2.1.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.2.1.0
180489	**Symptom:** CLI-based upgrade of a stand-alone controller fails with the **Timed out, Try again** error message. **Scenario:** This issue occurs in a slow network connection when the **copy scp** command fails to download the ArubaOS image after 15 minutes. This issue is observed in managed devices running ArubaOS 8.2.1.0. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.1.0

Table 6: *Known Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version
181221	**Symptom:** Clients are unable to connect to the managed device. **Scenario:** This issue occurs when enforce DHCP is enabled and route IP table buffer overflows. This issue is observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0
181355	**Symptom:** The mDNS process crashes on a managed device. **Scenario:** This issue occurs because the hash table used to store MAC address is corrupt due to a race condition. This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.3.0.0
181615	**Symptom:** Controllers lose licenses if the controller was unplugged within 3 hours of adding the license and there were no configuration changes made on the controller. **Scenario:** This issue occurs because the database backup is not triggered when the write memory command is executed. This issue is not limited to any specific platform or ArubaOS version. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.3.0.0
181729	**Symptom:** The **show running-config** command does not list an ACL while the **show configuration effective** command lists the same ACL. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.2.1.1
181773	**Symptom:** Managed devices reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0
182352	**Symptom:** An AP does not take the EIRP settings from the radio profile and broadcasts with High EIRP. **Scenario:** This issue is observed in access points running ArubaOS 8.2.1.1. **Workaround:** None.	AirMatch	All platforms	ArubaOS 8.2.1.1

Table 6: *Known Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version
182486	**Symptom:** A client is not able to access the internet. **Scenario:** This issue occurs when the PPPoE interface includes the **ip nat outside** configuration. This issue is observed in managed devices running ArubaOS 8.2.1.0. **Workaround:** None.	VLAN	All platforms	ArubaOS 8.2.1.0
182612 182372	**Symptom:** Client are unable to resolve ARP requests. **Scenario:** This issue occurs because the AP memory utilization rate is high, leading to drop in client traffic. This issue is observed in access points running ArubaOS 8.3.0.0. **Workaround:** None.	AP Datapath	All platforms	ArubaOS 8.3.0.0
183034	**Symptom:** Clients get disconnected after roaming although auto connect is enabled. **Scenario:** This issue is observed in access points running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.2.1.1
183134	**Symptom:** The **profmgr** process crashes on a Controller multiple times. **Scenario:** This issue occurs when SSID is defined on one node and Virtual APs or the AP groups are defined on lower nodes. This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.3.0.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.3.0.0

Table 6: *Known Issues in ArubaOS 8.3.0.2*

Bug ID	Description	Component	Platform	Reported Version
183246	**Symptom:** Managed devices could get converted to master node automatically when a power outage occurs while a configuration change is received from the Mobility Master. **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
184786	**Symptom:** APs are not broadcasting on Virtual APs and on start up, display D flag after managed devices are rebooted in a cluster. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions in a cluster setup. **Workaround:** Ensure the VLAN name binding on **virtual-ap** profile is same as the name of named VLAN.	AP-Platform	All platforms	ArubaOS 8.2.0.2
193777	**Symptom:** The **authentication** process crashes when the managed device is upgraded from ArubaOS 8.2.1.1 to ArubaOS 8.3.0.2. **Scenario:** When the system configuration contains netdestination aliases and they are included in ACLs as an ACE entry, the aliases are expanded as hit entries. This issue is observed when the number of hit entries exceed the maximum limit of 8K (maximum of 8192), post which the new hit entries are not accepted and the system is vulnerable to **authentication** process crash. This issue is observed in managed devices running ArubaOS 8.3.0.1 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.3.0.1

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

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

Topics in this chapter include:

Important Points to Remember

To upgrade your Mobility Master or managed device:

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

- If possible, use FTP to load ArubaOS images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, *Aruba Mobility Master Licensing Guide*.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Deleted the following files to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 31 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 31 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 31 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or the CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

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

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

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

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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 30.

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

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

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

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

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

1. Log in to the vSphere client.

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

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

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

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

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

In the WebUI

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

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

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

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

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

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

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

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

In the CLI

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

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

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

or

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

or

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

4. Execute the **show image version** command to check if the ArubaOS image is loaded on the flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

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

5. Execute the **copy** command to load the new image to the non-boot partition.

```
(host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

6. Execute the **show image version** command to verify that the new image is loaded.
   ```
   (host)# show image version
   ```
7. Reboot the Mobility Master.
   ```
   (host)# reload
   ```

Verifying the ArubaOS Upgrade

Verify the upgrade using the WebUI or CLI.

In the WebUI

Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the WebUI to verify if all the managed devices are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 31 for information on creating a backup.

In the CLI

Execute the **show version** command to verify the ArubaOS image version. The following steps describe how to verify that the Mobility Master is functioning as expected:

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 31 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 31.
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.