ArubaOS 8.7.1.6 Release Notes

a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2021 Hewlett Packard Enterprise Development LP.

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

Chapter 1
Revision History

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

Table 1: *Revision History*

Revision	Change Description
Revision 02	The bug, **AOS-125897** was added as a known issue.
Revision 01	Initial release.

Chapter 2
Release Overview

This ArubaOS release notes includes the following topics:

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

For a list of terms, refer Glossary.

Related Documents

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

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

Supported Browsers

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

- 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 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 on Windows 7, Windows 8, Windows 10, and macOS

Terminology Change

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

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

Contacting Support

Table 2: *Contact Information*

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

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

CLI

show stm perf-history command

Starting from ArubaOS 8.7.1.6, the **show stm perf-history** command displays the number of association requests received by the controller for the past 24 hours.

```
(host) #show stm perf-history
Association Rate History
------------------------
Day  Hour  Min  Total  Peak rate/s  Peak time
---  ----  ---  -----  -----------  ---------
10   14    45   5725   40.0         14:47:34
10   14    50   9850   40.0         14:50:26
10   14    55   10040  40.0         14:55:05
10   15    0    9860   40.0         15:01:30
10   15    5    9900   40.0         15:05:18
10   15    10   9900   40.0         15:10:33
10   15    15   9900   40.0         15:15:16
10   15    20   10075  40.0         15:20:05
```

The output displays the association rate history for every five minute of the past 24 hours.

Chapter 4
Supported Platforms in ArubaOS 8.7.1.6

This chapter describes the platforms supported in this release.

Mobility Master Platforms

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

Table 3: *Supported Mobility Master Platforms in ArubaOS 8.7.1.6*

Mobility Master Family	Mobility Master Model
Hardware Mobility Master	MM-HW-1K, MM-HW-5K, MM-HW-10K
Virtual Mobility Master	MM-VA-50, MM-VA-500, MM-VA-1K, MM-VA-5K, MM-VA-10K

Mobility Controller Platforms

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

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.7.1.6*

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

AP Platforms

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

Table 5: *Supported AP Platforms in ArubaOS 8.7.1.6*

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

Table 5: *Supported AP Platforms in ArubaOS 8.7.1.6*

AP Family	AP Model
203R Series	AP-203R, AP-203RP
205H Series	AP-205H
207 Series	AP-207
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303 Series	AP-303, AP-303P
303H Series	AP-303H, AP-303HR
310 Series	AP-314, AP-315
318 Series	AP-318
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377
370EX Series	AP-375EX, AP-377EX
AP-387	AP-387
500 Series	AP-504, AP-505
500H Series	AP-503H, AP-505H
510 Series	AP-514, AP-515, AP-518
530 Series	AP-534, AP-535
550 Series	AP-555
560 Series	AP-565, AP-567
570 Series	AP-574, AP-575, AP-577

Chapter 5
Regulatory Updates in ArubaOS 8.7.1.6

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_81660

Chapter 6
Resolved Issues in ArubaOS 8.7.1.6

The following issues are resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-213507	—	Some managed devices crashed unexpectedly. The log files listed the reason for the event as, **Reboot Cause: Soft Watchdog reset**. Some users also experienced decreased network performance in high density deployments. The fix ensures that the managed devices work as expected. This issue was observed in 7210, 7220, 7240, and 7240XM controllers running ArubaOS 8.3.0.14 or later versions. **Duplicates:** AOS-210240, AOS-214964, AOS-215393, AOS-215421, AOS-215628, AOS-215765, AOS-215827, AOS-216087, AOS-216315, AOS-216420, AOS-216888, AOS-217041, AOS-218007, AOS-218021, AOS-218907, AOS-219588, AOS-219597, AOS-216315, AOS-216420, AOS-216888, AOS-220471, AOS-220981, AOS-221390, AOS-221642, AOS-222036, AOS-223402, AOS-224238, AOS-225375, AOS-226268, AOS-226517, AOS-223254, and AOS-224552	ArubaOS 8.5.0.10
AOS-225808 AOS-226249	—	The APs crashed unexpectedly after a cluster split. This issue occurred when there were seven or more managed devices in a dual stack deployment. This issue was observed in managed devices running ArubaOS 8.7.0.0 or later versions in a cluster setup.	ArubaOS 8.7.1.3
AOS-226324 AOS-225655	—	AirMatch stopped working on Mobility Masters running ArubaOS 8.7.1.1 or later versions. This issue occurred when the network had multiple 802.1ax APs. The fix ensures that the AirMatch feature works as expected.	ArubaOS 8.7.1.1
AOS-226410	—	Cluster heartbeats were dropped in 7280 controllers running ArubaOS 8.7.1.5 in a cluster setup. The fix ensures that the cluster heartbeats are not dropped.	ArubaOS 8.7.1.5
AOS-226516 AOS-226552	—	Some AP-505H mesh access points running ArubaOS 8.7.1.5 changed its wired MAC address every time after a reboot. The fix ensures that the APs do not change its MAC address every time after a reboot.	ArubaOS 8.7.1.5
AOS-226008	—	Cluster heartbeats were delayed and ping latency was also observed. This issue occurred due to continuous irregular traffic like ARP flooding. The fix ensures that the managed devices work as expected. This issue was observed in managed devices running ArubaOS 8.7.1.4 or later versions in a cluster setup.	ArubaOS 8.7.1.4

Table 6: *Resolved Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222895	—	The **STM** process was stuck on managed devices running ArubaOS 8.6.0.0 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.9

Chapter 7
Known Issues in ArubaOS 8.7.1.6

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

Limitation

Following are the limitations observed in this release:

Port-Channel Limitation in 7280 Controllers

On 7280 controllers with all the member ports of each port-channel configured from the same NAE (Network Acceleration Engine), if one of the member ports experiences link flap either due to a network event or a user driven action, the rest of the port-channels also observe the link flap for less than a second.

No Support for Unique Local Address over IPv6 Network

The IPv6 addresses for interface tunnels do not accept unique local addresses.

Known Issues

Following are the known issues observed in this release:

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-125897 AOS-187598 AOS-189036 AOS-192082 AOS-192723 AOS-192731 AOS-192734 AOS-195746 AOS-198423 AOS-204676	151952	When a managed device reboots, APs and clients boot without IP addresses and other fields. This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.	ArubaOS 8.0.1.0
AOS-151022 AOS-188417	185176	The output of the **show datapath uplink** command displays incorrect session count. This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions.	ArubaOS 8.1.0.0
AOS-151355	185602	A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.	ArubaOS 8.0.1.0

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-153742 AOS-194948	188871	A stand-alone controller crashes and reboots unexpectedly. The log files list the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 51:86:0:8)**. This issue is observed in 7010 controllers running ArubaOS 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.	ArubaOS 8.5.0.1
AOS-190071 AOS-190372	—	A few users are unable to access websites when WebCC is enabled on the user role. This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in 7005 controllers running ArubaOS 8.4.0.0. **Workaround:** Perform the following steps to resolve the issue: 1.Remove web category from the ACL rules and apply **any any any permit** policy. 2. Disable WebCC on the user role. 3. Change the VLAN of user role from trunk mode to access mode.	ArubaOS 8.4.0.0
AOS-190621	—	WebUI does not filter the names of the APs that contain the special characters, + and %. This issue is observed in managed devices and Mobility Masters running ArubaOS 8.2.0.0 or later versions.	ArubaOS 8.4.0.2
AOS-193231 AOS-200101 AOS-207456	—	The **Dashboard > Infrastructure > Access Devices** page of the WebUI displays an error message, **Error retrieving information**. This issue is observed in Mobility Masters running ArubaOS 8.5.0.3 or later versions.	ArubaOS 8.5.0.3
AOS-196042 AOS-217995 AOS-221263	—	The **show ucc dns-ip-learning** command displays **Unknown** for **Service Provider**. This issue is observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-199545 AOS-212851	—	Some APs report low noise floor after upgrading the cluster to ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-199884	—	Mobility Master logs the following error messages, **PAPI_Free: This buffer 0x4f6c48 may already be freed** and **PAPI_Free: Bad state index 0 state 0x1.** This issue is observed in Mobility Masters running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5
AOS-200515 AOS-219987	—	The **DDS** process crashes on managed devices running ArubaOS 8.3.0.10 or later versions.	ArubaOS 8.3.0.10

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-201166 AOS-207939 AOS-209042	—	A controller crashes and reboots unexpectedly when the **HTTPD** process is restarted. The log files list the reason for the event as **Reboot cause: Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c)**. This issue is observed in stand-alone controllers running ArubaOS 8.2.0.0 or later versions.	ArubaOS 8.5.0.2
AOS-201376	—	The measured power, **Meas. Pow** column in the **show ap debug ble-table** command does not get updated when the TX power of an AP is changed. This issue is observed in APs running ArubaOS 8.5.0.6 or later versions.	ArubaOS 8.5.0.6
AOS-201428	—	The **show log all** command does not display output in a chronological order. This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-202552 AOS-203990	—	The **Dashboard > Traffic Analysis > AppRF** page of the WebUI displays **Unknown** for WLANs, Roles, and Devices. This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	ArubaOS 8.3.0.0
AOS-203025 AOS-224678	—	A few mesh point APs are Down in the AP database. This issue occurs when CPsec is disabled. This issue is observed in managed devices running ArubaOS 8.5.0.6 or later versions in a cluster setup.	ArubaOS 8.5.0.6
AOS-203614 AOS-209261	—	The Mobility Master dashboard does not display the number of APs and clients present in the network. This issue is observed in Mobility Masters running ArubaOS 8.6.0.2 or later versions.	ArubaOS 8.6.0.2

AOS-205140	—	The AppRF ACLs using a voice role block WebRTC calls. This issue occurs when WebRTC audio and video ACLs are not part of the default **voip-applications-acl**. This issue is observed in Mobility Masters running ArubaOS 8.6.0.8 or later versions.
		Workaround: Add WebRTC audio and video ACLs to the user role using the following command:
		`ip access-list session webrtc`
		`any any app alg-webrtc-audio permit`
		`any any app alg-webrtc-video permit`
			ArubaOS 8.6.0.8

AOS-206541	—	The **Maintenance > Software Management** page does not display the list of all managed devices that are part of a cluster. This issue is observed in Mobility Masters running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-206752	—	The console log of 7205 controllers running ArubaOS 8.5.0.9 or later versions displays the **ofald| |sdn| ERRS ofconn_rx:476 <10.50.1.26:6633> socket read failed, err:Resource temporarily unavailable(11)** message.	ArubaOS 8.5.0.9

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-206795	—	A user is unable to rename a node from the Mobility Master node hierarchy. This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions. **Workaround:** Restart **profmgr** process to rename the node.	ArubaOS 8.3.0.7
AOS-206890	—	The **body** field in the **Configuration > Services > Guest Provisioning** page of the WebUI does not allow users to add multiple paragraphs for email messages. This issue is observed in Mobility Masters running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-206902 AOS-208241	—	AirGroup users are unable to connect to Sonos speakers. This issue is observed in managed devices running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-206929	—	The **show global-user-table** command does not provide an IPv6 based filtering option. This issue is observed in Mobility Masters running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-206930	—	Some Mobility Masters running ArubaOS 8.7.0.0 or later versions allow to configure the same IPv6 address twice. This issue occurs when the user enters the same IPv6 address in a different format.	ArubaOS 8.7.0.0
AOS-207006 AOS-215138	—	A few APs go down and UDP 8209 traffic is sent without UDP 4500 traffic. This issue is observed in managed devices running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-207245	—	Some managed devices running ArubaOS 8.5.0.8 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 53:86:0:802c).**	ArubaOS 8.5.0.8
AOS-207303	—	Users are unable to add a managed device to an existing cluster of managed devices configured with rap-public-ip address. This issue is observed in managed devices running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-207366	—	The **show advanced options** menu is not available in the **Configuration > Access Points > Campus APs** page of the WebUI. This issue occurs when more than one AP is selected. This issue is observed in Mobility Masters running ArubaOS 8.3.0.13.	ArubaOS 8.3.0.13
AOS-207692	—	Some managed devices running ArubaOS 8.6.0.4 or later versions log multiple authentication error messages.	ArubaOS 8.6.0.4

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-209273	—	The **Dashboard > Infrastructure** page of the WebUI does not display the data in graphical charts for mesh APs. This issue is observed in Mobility Masters running ArubaOS 8.7.0.0 or later versions	ArubaOS 8.7.0.0
AOS-209276	—	The **show datapath crypto counters** command displays the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. This issue is observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-209315	—	The IDS unauthorized device profile incorrectly sends deauthentication frames to APs. This issue occurs when **protect-misconfigured-ap** parameter is enabled in the **ids unauthorized-device-profile**. This issue is observed in APs running ArubaOS 8.6.0.9 or later versions	ArubaOS 8.6.0.9
AOS-209888 AOS-224884	—	The **Diagnostics > Tools > AAA Server Test** page of the WebUi displays the **Authentication** status as **0** instead of **Authentication Successful**. This issue is observed in managed devices running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-209977	—	An SNMP query with an incorrect string fails to record the offending IP address in the trap or log information. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-210273 AOS-217372	—	Some managed devices running ArubaOS 8.6.0.7 or later versions log the message, **<INFO> |dot1x-proc:1| Sending a request for Switch IP6** repeatedly even when there are no IPv6 configurations in the network.	ArubaOS 8.6.0.7
AOS-210482	—	Some managed devices running ArubaOS 8.3.0.6 or later versions display the error message, **Invalid set request** while configuring ESSID for a Beacon Report Request profile.	ArubaOS 8.3.0.6
AOS-210490	—	Some managed devices running ArubaOS 8.5.0.8 or later versions display the error message, **Error: Tunnel is part of a tunnel-group** while deleting an L2 GRE tunnel which is not a part of any tunnel group.	ArubaOS 8.5.0.8
AOS-211658	—	A few clients are unable to connect to AP-535 access points running ArubaOS 8.6.0.5 or later versions in a cluster setup. This issue occurs when WMM and HT configurations are enabled.	ArubaOS 8.6.0.5
AOS-211720	—	The **STM** process crashes on managed devices and hence, APs failover to another cluster. This issue is observed in managed devices running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-211863	—	Some APs do not come up on managed devices. This issue occurs when the forwarding mode is changed to bridge mode and when the name of the ACL reaches the maximum size of 64 bytes. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212038	—	The **show memory <process-name>** command does not display information related to the **dpagent** process. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-212255	—	Some APs are stuck in **Not in Progress** state during cluster live upgrade. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-212591	—	Some managed devices running ArubaOS 8.7.1.0 crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**.	ArubaOS 8.7.1.0
AOS-215461 AOS-220709	—	Database synchronization fails between standby and stand-alone controllers running ArubaOS 8.6.0.9 or later versions. The log files list the reason for the event as **Standby switch did not acknowledge the WMS database restore request**.	ArubaOS 8.6.0.9
AOS-215669	—	Some managed devices running ArubaOS 8.6.0.7 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**.	ArubaOS 8.6.0.7
AOS-215712	—	Mobility Masters running ArubaOS 8.7.0.0 or later versions forward all syslog messages with severity level marked as debug. This issue occurs when CEF format is enabled on the Mobility Master.	ArubaOS 8.7.0.0
AOS-215852	—	Mobility Masters running ArubaOS 8.6.0.6 or later versions log the error message, **ofa: 07765|ofproto|INFO|Aruba-SDN: 1 flow_mods 28 s ago (1 modifications).** This issue occurs when openflow is enabled and when 35 seconds is configured as the UCC session idle timeout.	ArubaOS 8.6.0.6
AOS-216133	—	Clients are unable to connect to APs on A-band channels. This issue is observed in APs running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-216145	—	Mobility Masters running ArubaOS 8.5.0.8 or later versions send continuous DNS requests to the managed devices. This issue occurs when a folder that is not available on the /mm node is trying to get synchronized on the managed devices. **Workaround:**	ArubaOS 8.5.0.8

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
		Perform the following steps to resolve the issue: 1.Issue the **show memory debug | include rsync** command to identify the name of the folder that is trying to get synchronized on the managed devices. 2. Ensure that the folder is not present in the /flash/upload/custom/ path of the Mobility Master and then issue the **no sync files <folder name>** command to stop synchronization.	
AOS-216536 AOS-220630	—	Some managed devices running ArubaOS 8.5.0.11 or later versions are unable to come up on the Mobility Master. This issue occurs when the managed devices get the branch IP address as the controller IP address in a VPNC deployment.	ArubaOS 8.5.0.11
AOS-216622	—	A few APs incorrectly display the restricted flag, **p = Restriction mode in POE-AF/AT** in the AP database even if the Ethernet port is disabled. This issue is observed in APs running ArubaOS 8.7.0.0 or later versions.	ArubaOS 8.7.0.0
AOS-217628 AOS-221178 AOS-226513 AOS-226575 AOS-226753	—	Some managed devices running ArubaOS 8.5.0.11 or later versions crash and reboot unexpectedly. The log files list the reason for the event as **Kernel Panic (Intent:cause:register 12:86:b0:2**.	ArubaOS 8.5.0.11
AOS-217653 AOS-224031	—	Some AP-535 access points running ArubaOS 8.7.1.4 or later versions do not respond to the fragmented ping requests from a few clients. This issue occurs when the APs operate in tunnel mode.	ArubaOS 8.7.1.4
AOS-217890	—	Some managed devices running ArubaOS 8.5.0.10 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Datapath timeout (SOS Assert)**.	ArubaOS 8.5.0.10
AOS-218162	—	The wired Ethernet port does not form GRE tunnel with the managed device. This issue is observed in managed devices running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-218254 AOS-218875	—	Some managed devices running ArubaOS 8.7.1.0 or later versions crashes unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:e0:2).**	ArubaOS 8.7.1.0
AOS-218519	—	A few mesh APs detect its own BSSIDs as phony BSSIDs. This issue is observed in APs running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218795	—	Downloadable user roles are not downloaded and hence, user roles are not assigned to the tunnel-node users. This issue is observed in managed devices running ArubaOS 8.7.1.2 or later versions.	ArubaOS 8.7.1.2
AOS-219112	—	A few UBT clients hop between VLANs. This issue is observed in managed devices running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219307 AOS-223234	—	Some managed devices running ArubaOS 8.5.0.12 or later versions crash unexpectedly. The log files list the reason for the event as, **Reboot cause: Kernel Panic (Intent:cause:register 12:86:f0:2)**.	ArubaOS 8.5.0.12
AOS-219376	—	Some users are unable to add VIA server details if the domain name exceeds 32 characters. This issue is observed in Mobility Masters running ArubaOS 8.7.1.2 or later versions.	ArubaOS 8.7.1.2
AOS-219383	—	The **Configuration > License > License Usage** tab does not display the license details. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.12 or later versions.	ArubaOS 8.5.0.12
AOS-219385	—	Some APs take a long time to come up on the backup data center after the primary data center failover. This issue is observed in APs running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-219619	—	Configurations inherited from the Mobility Master are incorrectly displayed as **local/mm** indicating that the configurations are locally enabled on the managed devices. This issue is observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-219739	—	The **profmgr** process crashes on the backup Mobility Masters running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-219803	—	The XML query done on a non-existing user results in an invalid response. This issue is observed in managed devices running ArubaOS 8.7.1.2 or later versions.	ArubaOS 8.7.1.2
AOS-219936	—	The stand-alone controller displays the error message, **Module Profile Manager is busy. Please try later** while configuring netdestination. This issue is observed in stand-alone controllers running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-220108	—	The **OFA** process crashes on Mobility Master Virtual Appliances running ArubaOS 8.6.0.6 or later versions. This issue occurs when the **show openflow debug ports** command is executed.	ArubaOS 8.6.0.6

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-220374	—	The authentication server load balancing does not work as expected. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-220515	—	Some managed devices running ArubaOS 8.0.0.0 or later versions display the error message, **|fpapps| filling up the default gateway configuration.**	ArubaOS 8.5.0.12
AOS-220704	—	Some APs are incorrectly displayed under different clusters. This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-220903	—	The **s** flag indicating LACP striping is not displayed in the output of the **show ap database long** command even if LLDP is enabled on two uplinks. This issue is observed in APs running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-220982	—	A few wireless clients are unable to pass traffic during a cluster failover. This issue is observed in managed devices running ArubaOS 8.5.0.13 or later versions.	ArubaOS 8.5.0.13
AOS-221307	—	Adding a new VLAN removes all the existing VLANs on the port channel. This issue occurs when the existing VLAN list exceeds 256 characters. This issue is observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-221666 AOS-222708	—	Some Remote APs running ArubaOS 8.6.0.9 or later versions crash and reboot unexpectedly. The log file lists the reason for the event as, **Kernel panic - not syncing**.	ArubaOS 8.6.0.9
AOS-221789 AOS-223052	—	The 802.1X authentication is initiated twice. This issue is observed in APs running ArubaOS 8.6.0.3 or later versions.	ArubaOS 8.6.0.9
AOS-221883 AOS-221884	—	Users are unable to add ACLs using the **firewall cp** command and an error message, **Error: Max CP firewall limit (97) reached** is displayed. This issue is observed in managed devices running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-222027 AOS-226135	—	Some managed devices generate kernel slab corruption logs. This issue is observed in managed devices running ArubaOS 8.7.1.3 or later versions in a cluster setup.	ArubaOS 8.7.1.3
AOS-222037	—	The cellular handoff assist feature does not work as expected on APs running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222267 AOS-212114 AOS-217474 AOS-219497 AOS-225306	—	A few managed devices go down intermittently. This issue occurs when the traffic between Mobility Master and managed devices is transmitted without IPsec encryption. This issue is observed in managed devices running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-222499	—	Clients that perform only four-way handshake are unable to update their VSA role derived after machine and user authentication. This issue is observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-222578	—	L2TP IP address leak is observed and the VLAN pool is exhausted. This issue is observed in managed devices running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-222589	—	Some AP-535 access points running ArubaOS 8.7.1.3 or later versions crash unexpectedly. The log files list the reason for the event as **kernel panic: Fatal exception in interrupt**. This issue occurs when the UCC RTPA configuration is enabled. **Duplicates:** AOS-222575, AOS-222576, AOS-223063, AOS-223138, and AOS-224724 **Workaround:** Disable the RTPA configuration using the **ucc rtpa-config no** command to resolve the issue.	ArubaOS 8.7.1.3
AOS-222754	—	The SNMP walk to managed devices fails when the SNMP requests have the IPv6 address of the controller. This issue occurs when the primary managed device has VRRP IPv6 address configured. This issue is observed in managed devices running ArubaOS 8.4.0.1 or later versions.	ArubaOS 8.4.0.1
AOS-222771	—	Some managed devices running ArubaOS 8.5.0.12 or later versions do not send SNMPv3 information to the AirWave server.	ArubaOS 8.5.0.12
AOS-222931	—	Some APs do not form active tunnels with the AAC. This issue is observed in managed devices running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-222936	—	A few clients are unable to connect to AP-565 mesh access points running ArubaOS 8.7.1.4 or later versions. The log files list the reason for this event as **UAC Down**. **Workaround:** ■ Configure the **reselection-mode** to **reselect-never** in the **ap mesh-radio-profile** command. ◦ (host)[mynode] #ap mesh-radio-profile default ◦ (host) [mynode] (Mesh Radio profile "default"] #reselection-mode reselect-never ■ Use 40 MHz channel bandwidth instead of 20 MHz bandwidth.	ArubaOS 8.7.1.4

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-222992	—	A large number of log files are generated and stored at /flash1/log/backup folder. This issue occurs due to a cluster failover between clients and APs. This issue is observed in 7220 and 7240XM controllers running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-223094 AOS-220190 AOS-223094 AOS-224240 AOS-224792	—	A few users are unable to login to the captive portal page that is hosted on ClearPass Policy Manager server. This issue occurs when the netdestination ID, which is added to the captive portal whitelist, is incorrectly changed to 0 after a reboot of the Mobility Master Virtual Appliance. This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.5.0.10 or later versions. **Workaround:** Create a new user role with the same set of ACL rules, and replace the existing user role.	ArubaOS 8.6.0.9
AOS-223273	—	The UBT users list is not available in the user table after a cluster failover. This issue is observed in Mobility Master running ArubaOS 8.7.1.4 or later versions in a cluster setup.	ArubaOS 8.7.1.4
AOS-223337	—	The clients added to the client match unsupported list are still considered for client match steers. This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-223577	—	The user table entries display only the IPv6 link local address. This issue is observed in stand-alone controllers running ArubaOS 8.2.0.0 or later versions.	ArubaOS 8.6.0.5
AOS-223656	—	Some Remote APs are unable to come up on managed devices after a reboot. This issue is observed in managed devices running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-223669	—	Some users are unable to complete captive portal authentication. This issue occurs when ipv6-user snmpwalk populates IPv4 user details. This issue is observed in managed devices running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.4
AOS-223740	—	The expired machine authentication cache entries are not removed. This issue is observed in stand-alone controllers running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3
AOS-223797	—	The **show ap remote auth-trace-buf** command does not display any output. This issue is observed in stand-alone controllers and managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-223839	—	The output of the **show ap active** command does not display any value for **Outer IP**. This issue is observed in Mobility Masters running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-223848	—	The **+** symbol in the **Configuration > Services > AirGroup > Service-Based Policy** page of the WebUI does not allow users to create an AirGroup profile. Users can create an AirGroup profile only by navigating to the **Configuration > System > Profiles > AirGroup** page of the WebUI. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.7.1.4
AOS-224019 AOS-226123	—	High controlpath memory utilization is observed and an error message, **Resource 'Controlpath Memory' has dropped below 85% threshold** is displayed. This issue is observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-224060 AOS-225534	—	The **STM** process crashes on Mobility Masters running ArubaOS 8.7.1.3 or later versions. This issue occurs when the **show ap details** command is executed.	ArubaOS 8.7.1.3
AOS-224110 AOS-224287	—	A few APs running ArubaOS 8.6.0.9 or later versions are stuck in the BLE upgrade loop after an upgrade.	ArubaOS 8.6.0.9
AOS-224186	—	The **show tech-support** command does not display any information about the kernel crash and displays the message, **No kernel crash information available**. This issue is observed in stand-alone controllers running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-224197	—	Some clients are unable to connect to managed devices running ArubaOS 8.7.1.3 or later versions in a cluster setup. This issue occurs after a cluster flap.	ArubaOS 8.7.1.3
AOS-224275 AOS-215206	—	The predefined v6-control policy does not allow DHCPv6 traffic. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.6.0.9
AOS-224326 AOS-226350	—	A few AP-514 access points running ArubaOS 8.7.1.5 or later versions crash unexpectedly. The log files list the reason for the event as **PC is at wlc_ratesel_set_link_bw+0x0**.	ArubaOS 8.7.1.5
AOS-224538	—	A few APs running ArubaOS 8.5.0.11 or later versions incorrectly fall back to the default AP group.	ArubaOS 8.5.0.11
AOS-224688	—	The HE enabled APs are incorrectly displayed as **HTT None** in AirWave. This issue is observed in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-224767 AOS-221486	—	A few clients are disconnected from the network. The log file lists the reason for the event as **Wlan driver excessive tx fail quick kickout**. This issue is observed in AP-535 and AP-555 access points running ArubaOS 8.6.0.0 or later versions.	ArubaOS 8.6.0.8

Table 7: *Known Issues in ArubaOS 8.7.1.6*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-224901	—	A few APs terminating in the backup LMS cluster do not move to the LMS cluster after a reboot. This issue is observed in managed devices running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-224961	—	The global user entries table is not updated when clients roam to a different AP. This issue occurs when 802.11r is enabled. This issue is observed in APs running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-225135	—	Clients connected to APs are unable to send or receive data packets from APs. This issue occurs when the ACL changes are not updated on APs. This issue is observed in APs running ArubaOS 8.6.0.9 or later versions.	ArubaOS 8.6.0.9
AOS-225268	—	Some Remote APs are assigned to incorrect nodes. This issue is observed in managed devices running ArubaOS 8.7.1.3 or later versions in a cluster setup.	ArubaOS 8.7.1.3
AOS-225709	—	The **STM** process crashes on managed devices running ArubaOS 8.7.1.4 or later versions.	ArubaOS 8.7.1.4
AOS-226343	—	L2TP users are randomly assigned to different VLAN pools. This issue occurs when the configured VLAN pool is exhausted. This issue is observed in controllers running ArubaOS 8.7.1.3 or later versions.	ArubaOS 8.7.1.3

Chapter 8
Upgrade Procedure

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

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

Important Points to Remember

To upgrade your managed device or Mobility Conductor:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device?
  - Are all managed devices running the same version of ArubaOS?
  - What services are used on your managed device (employee wireless, guest access, Remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load ArubaOS images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path, if required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, refer the *Aruba Mobility Conductor Licensing Guide*.
- Multiversion is supported in a topology where the managed devices are running the same version as the Mobility Conductor, or two versions lower. For example multiversion is supported if a Mobility Conductor is running ArubaOS 8.5.0.0 and the managed devices are running ArubaOS 8.5.0.0, ArubaOS 8.4.0.0, or ArubaOS 8.3.0.0.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless the minimum flash space inis 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 the managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 27 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 27 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 27 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

You can delete a file using the WebUI or CLI.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

Backing up and Restoring Flash Memory

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

In the WebUI

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

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

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

In the CLI

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

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

```
(host) #write memory
```

2. Execute the following command to back up the contents of the flash memory to the **flashbackup.tar.gz** file.

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

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

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


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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 27.

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

In the WebUI

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

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

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

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

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

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

In the CLI

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

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

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

or

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

or

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

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

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

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

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

or

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

or

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

or

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

6. Execute the **show image version** command to verify that the new image is loaded.

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

7. Reboot the Mobility Conductor.

```
(host)#reload
```

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

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

Verifying the ArubaOS Upgrade

Verify the ArubaOS upgrade in the WebUI or CLI.

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 27 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the ArubaOS image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 27 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 27.
2. Verify that the control plane security is disabled.
3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade ArubaOS version.

   When you specify a boot partition or copy an image file to a system partition, Mobility Conductor or managed device checks if the ArubaOS version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the ArubaOS version and configuration files.
5. After switching the boot partition, perform the following steps:

- Restore the pre-upgrade flash backup from the file stored on the Mobility Conductor or managed device. Do not restore the ArubaOS flash backup file.
- Do not import the WMS database.
- If the RF plan is unchanged, do not import it. If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded ArubaOS version.
- If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Conductor or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.

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

b. From **Select destination file** drop-down list, select **Flash file system**, and enter a file name (other than default.cfg).

c. Click **Copy**.

2. Determine the partition on which your pre-upgrade ArubaOS version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade ArubaOS version is not stored on your system partition, load it into the backup system partition by performing the following steps:

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

a. Enter the FTP or TFTP server address and image file name.

b. Select the backup system partition.

c. Enable **Reboot Controller after upgrade**.

d. Click **Upgrade**.

3. Navigate to the **Maintenance > Software Management > Reboot** page, select **Save configuration before reboot**, and click **Reboot**.

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

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

In the CLI

The following steps describe how to downgrade the ArubaOS version:

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

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

or

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

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

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

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

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

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

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

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

5. Reboot the Mobility Conductor or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call the Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with IP addresses and interface numbers.
- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information.