# ArubaOS 8.6.0.2

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

# Revision History

The following table provides the revision history of this document.

**Table 1:** *Revision History*

| Revision | Change Description |
|---|---|
| Revision 04 | Removed the Migrating from ArubaOS 6.x to ArubaOS 8.x section from Upgrade Procedure as the Migration Tool is no longer supported. |
| Revision 03 | AOS-191317 has been added as a Known Issue. |
| Revision 02 | AOS-196629 has been added as a Known Issue. |
| 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 a list of terms, refer Glossary.

## 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

# 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)<br>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/<br>Email: aruba-sirt@hpe.com |

## New Features and Enhancements in ArubaOS 8.6.0.2

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

## Supported Platforms in ArubaOS 8.6.0.2

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 8.6.0.2*

| 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 8.6.0.2*

| 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 |
| MC-VA-xxx Virtual Mobility Controllers | 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 8.6.0.2*

| AP Family | AP Model |
|---|---|
| 100 Series | AP-104, AP-105 |
| 103 Series | AP-103 |
| 110 Series | AP-114, AP-115 |
| 130 Series | AP-134, AP-135 |
| 170 Series | AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1 |
| 200 Series | AP-204, AP-205 |
| 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 |

**Table 5:** *Supported AP Platforms in ArubaOS 8.6.0.2*

| AP Family | AP Model |
|---|---|
| 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 |
| AP-387 | AP-387 |
| 500 Series | AP-504, AP-505 |
| 510 Series | AP-514, AP-515 |
| 530 Series | AP-534, AP-535 |
| 550 Series | AP-555 |
| RAP 3 Series | RAP-3WN, RAP-3WNP |
| RAP 100 Series | RAP-108, RAP-109 |
| RAP 155 Series | RAP-155, RAP-155P |

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 support.arubanetworks.com.

## Regulatory Updates in ArubaOS 8.6.0.2

The following DRT file version is part of this release:

- DRT-1.0_73702

## Resolved Issues in ArubaOS 8.6.0.2

This chapter describes the issues resolved in this release.

**Table 6:** *Resolved Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-143169<br>AOS-196721 | 174366 | When the **tar crash** command was executed the second time, the **crash.tar** file was unavailable in the AP crash folder. The fix ensures that the **crash.tar** file is available in the AP crash folder. This issue was observed in 7220controllers running ArubaOS 8.3.0.10, or later versions. | ArubaOS 8.3.0.0 |
| AOS-148529<br>AOS-191978 | 181872 | A few clients connected to managed devices were unable to access the Internet. This issue occurred when the client traffic received incorrect Source NAT when IP Nat Inside feature was enabled on interface VLAN that was configured with PBR. This issue was observed in managed devices running ArubaOS 8.4.0.4 or later versions. | ArubaOS 8.4.0.4 |
| AOS-190154<br>AOS-190628<br>AOS-192465<br>AOS-195358 | — | The status of a few APs was incorrectly displayed as **Down** in the **Dashboard > Infrastructure > Access Devices** page of the WebUI and the status of the AP was **Up** in the CLI. The fix ensures that the WebUI displays the correct status of the APs. This issue was observed in Mobility Masters running ArubaOS 8.5.0.1 or later versions. | ArubaOS 8.5.0.1 |
| AOS-190836 | — | The **show interface gigabitethernet 0/0/0 transceiver** command displayed an error message **Error reading Transceiver ID Prom on 0/0/0**. The fix ensures that the command works as expected. This issue was observed in Mobility Masters running ArubaOS 8.5.0.1 or later versions. | ArubaOS 8.5.0.1 |
| AOS-192746<br>AOS-193755<br>AOS-196642 | — | Multiple APs were marked as **Down** during the upgrade of DHCPv6 server. This issue occurred when a DHCPv6 server was migrated from physical to virtual machines, and the IPv6 address of the DHCPv6 server was changed during the migration. The fix ensures that the APs work as expected. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions in a Mobility Master-Managed Device topology. | ArubaOS 8.3.0.8 |

**Table 6:** *Resolved Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-193559 | — | The **crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>** command did not accept IP addresses of the peer gateway that ended with 0 or 255 in a Mobility Master. As a result, the output of the **peer-ip <ipaddr>** command displayed the **Peer address cannot be a subnet or broadcast address** error message. The fix ensures that the Mobility Master allows peer IP addresses that ends with 0 or 255 except the following IP addresses: 255.255.255.255, 0.0.0.0 and 127.0.0.1 This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. | ArubaOS 8.4.0.0 |
| AOS-194519<br>AOS-196024 | — | A few 802.11r clients were unable to connect to APs during 802.1X authentication that led to packet drops in client traffic. This issue occurred when the APs were connected to Mobility Master Virtual Appliances. The fix ensures that the clients are able to connect to the APs seamlessly. This issue was observed in APs running ArubaOS 8.4.0.0 or later versions. | ArubaOS 8.5.0.0 |
| AOS-194591 | — | Managed devices were unable to form cluster nodes. The fix ensures that the managed devices are able to form cluster nodes. This issue was observed in 7240XMcontrollers running ArubaOS 8.5.0.2 or later versions in a cluster setup. | ArubaOS 8.5.0.2 |
| AOS-195266<br>AOS-197259<br>AOS-196392 | — | A managed device rebooted unexpectedly due to **dpagent** module crash. The log files listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause: register 54:86:50:2)**. This issue occurred when the dpagent module tried to free memory that was not properly allocated. The fix ensures that the managed device works as expected. This issue was observed in 7240XMcontrollers running ArubaOS 8.5.0.3 or later versions. | ArubaOS 8.5.0.3 |
| AOS-195271 | — | The **mon_serv_fwv** process crashed unexpectedly. The log file listed the reason for the event as **PROCESS_NOT_RESPONDING_CRITICAL**. The issue occurred when the mDNS process was restarted in the Mobility Master. This issue was observed in Mobility Master - Managed Device deployment running ArubaOS 8.5.0.3 or later versions in a centralized mode. | ArubaOS 8.5.0.3 |
| AOS-195813<br>AOS-197209 | — | Some android devices constantly rebooted when connected to the network. This issue occured when 802.11k was enabled using the default profile. This issue was observed in Mobility Masters running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-196231 | — | AirGroup clients trying to access Airplay services were unable to discover the AirGroup servers. This issue occurred when the Auto Associate feature was enabled. The fix ensures that the clients are able to discover the AirGroup servers. This issue was observed in Mobility Masters running ArubaOS 8.5.0.3 or later versions. | ArubaOS 8.5.0.3 |

**Table 6:** *Resolved Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-196315 | — | The status of the managed devices constantly flapped after upgrading the Mobility Master.This issue occurred when multiversion support was not enabled on 7280controllers. This issue is resolved by enabling multiversion support for 7280controllers. This issue was observed in 7280controllers running ArubaOS 8.5.0.3 or later versions. | ArubaOS 8.5.0.3 |
| AOS-196594 | — | A few 802.1X clients were deauthenticated and lost connectivity to an AP. This issue occurred when the PMK ID sent by the clients was not renewed. The fix ensures that the clients are able to connect to the AP. This issue was observed in APs running ArubaOS 8.4.0.0 or later versions. | ArubaOS 8.5.0.3 |
| AOS-196634<br>AOS-197154 | — | Android devices crashed and rebooted when connected to the network. This issue was observed in Mobility Masters running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-196937 | — | A stand-alone controller sent network advertisement using destination Layer 2 MAC address. The fix ensures that the stand-alone controller sends the network advertisement to the MAC address available in Source Link-Layer Address option. This issue was observed in 7240XMcontrollers running ArubaOS 8.2.0.0 or later versions. | ArubaOS 8.2.0.0 |

# Known Issues and Limitations in ArubaOS 8.6.0.2

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

## Limitations

Following are the limitations observed in this release.

### AP-555 Mesh Portal Limitation

AP-555 access points operating as a mesh portal reboot automatically when **split-5ghz-mode** is enabled.

### Incorrect Sub-Parameter Names in Masteripv6 Command

The following sub-parameter names under **ipsec-custom-cert** and **ipsec-custom-cert** parameters of **masteripv6** command are incorrect:

- **interface-c**
- **vlan-c**
- **fqdn-c**
- **interface-f**
- **vlan-f**
- **fqdn-f**

### IoT

The **telemetry** profile gets added in a managed device when **ap-grp** is configured in the profile. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions.

### No IPv6 Support for Mini-Setup Provisioning Mode

The provisioning of managed devices using IPv6 address is currently not supported in a mini-setup mode.

### No Support for FQDN over IPv6 Network

FQDN support for IPv6 address is currently not available in full setup provisioning mode for managed devices.

### No ZTP Support for IPv6 in Activate Server

ZTP for IPv6 using an Activate server is currently not supported.

## Known Issues

Following are the known issues observed in this release.

**Table 7:** *Known Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-151022<br>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 |
| AOS-155037 | 190571 | A Remote AP fails to come up. This issue occurs in a Remote AP with EST key type **X9.62/SECG curve**. This issue is observed in AP-303H access points running ArubaOS 8.3.0.3 or later versions. | ArubaOS 8.3.0.3 |
| AOS-156085<br>AOS-157704 | 192119<br>194393 | A few managed devices are unable to get the controller-IP address during boot up, after an upgrade. This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. | ArubaOS 8.1.0.0 |
| AOS-156424<br>AOS-156777<br>AOS-185158<br>AOS-193880 | 192581<br>193081 | Invalid SSIDs are displayed in the **Dashboard > WLAN** page in the WebUI. This issue occurs because few APs are broadcasting invalid SSIDs. This issue was observed in managed devices running ArubaOS 8.2.2.0 or later versions. | ArubaOS 8.2.2.0 |
| AOS-182073<br>AOS-183743 | — | An AP crashes and reboots unexpectedly. The log files lists the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**.This issue is observed in AP-315 access points running ArubaOS 8.3.0.5 or later versions. | ArubaOS 8.3.0.5 |
| AOS-182847 | — | A few users are unable to copy the **WPA Passphrase** field and **High-throughput** profile to a new SSID profile in the **Configuration > System > Profiles > Wireless LAN > SSID > <SSID_Profile>** option of the WebUI. This issue occurs when a new SSID profile is created from an existing SSID profile in the WebUI. This issue is observed in managed devices running ArubaOS 8.4.0.0 in a Mobility Master-Managed Device topology. | ArubaOS 8.4.0.0 |
| AOS-184977<br>AOS-188242<br>AOS-188378 | — | The output of the commands **show version, show clock, and show image version** do not display any information and the default gateway details are missing in a managed device. This issue occurs when the **/tmp** directory runs out of memory. This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions. | ArubaOS 8.4.0.0 |

**Table 7:** *Known Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-185538 | — | High number of EAP-TLS timeouts are observed in a managed device. This issue occurs because multiple IP addresses are assigned to each client. This issue is observed in managed devices running ArubaOS 8.3.0.8 or later versions. | ArubaOS 8.3.0.8 |
| AOS-188527<br>AOS-193897 | — | The IP address of the NAT configured managed device is visible in the HTTP header of the web server. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions. | ArubaOS 8.3.0.0 |
| AOS-190071<br>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 setup when the VLAN of user role is in trunk mode. This issue is observed in 7005 controllers running ArubaOS 8.4.0.0 or later versions.<br>**Workaround:**<br>■ Remove web category from the ACL rules and apply **any any any permit** policy.<br>■ Disable WebCC on the user role.<br>■ Change the VLAN of user role from trunk mode to access mode. | ArubaOS 8.4.0.0 |
| AOS-190230<br>AOS-194670 | — | A few Remote APs fail to come up on a managed device after an AP reboot, and are getting the same inner IP that has already been assigned to other Remote APs. This issue occurs because most of the Remote AP whitelist database entries are removed from the Mobility Master. This issue is observed in APs running ArubaOS 8.4.0.0 or later versions.<br>**Workaround:** Purge the Remote AP whitelist database entries on Mobility Master and managed device and add them again. However, this will reboot the Remote APs and can cause network disruption. | ArubaOS 8.4.0.0 |
| AOS-190380<br>AOS-196361 | — | A few users are unable to connect to VIA server from the guest account. This issue occurs because PBR is not applied to data packets from UDP port 4500 . As a result, the client traffic is not forwarded correctly. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. | ArubaOS 8.0.0.0 |
| AOS-191317<br>AOS-194342 | — | A few High Efficiency 802.11ax Intel clients are unable to pass traffic. This issue occurs when the clients are configured with OFDMA and Medium Power Save mode, which results in delay or packet drop to other clients. This issue is observed in 510 Series access points running ArubaOS 8.5.0.6 or later versions.<br>**Workaround:**<br>■ Issue the **wlan he-ssid-profile** command to disable MU-OFDMA in HE-SSID profile .<br>■ Move the client in wireless adaptor in Maximum Performance mode. | ArubaOS 8.6.0.0 |
| AOS-191394 | — | APs crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. This issue is observed in 500 Series access points running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-191612 | — | The MAC address of users connected using VIA is not sent to ClearPass Policy Manager for authentication. This issue is observed when IKE V2 with EAP-FTC is used for VIA authentication. This issue is observed in Mobility Masters running ArubaOS 8.5.0.1 or later versions. | ArubaOS 8.5.0.1 |

**Table 7:** *Known Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-192568<br>AOS-192736 | — | A few clients are unable to connect to APs even though High-Efficiency was disabled on all the SSID profiles of the APs. This issue is observed in AP-515 access points running ArubaOS 8.5.0.0 or later versions. | ArubaOS 8.5.0.1 |
| AOS-193383 | — | APs crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Take care of the TARGET ASSERT first**. This issue is observed in 500 Series access points running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-193775<br>AOS-194581 | — | A mismatch of AP count and client count is observed between the Mobility Master and the managed device. This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. | ArubaOS 8.5.0.2 |
| AOS-193976 | — | APs reboot unexpectedly. The log file lists the reason for the event as **Critical process /aruba/bin/sapd [pid XXXX] DIED, process marked as RESTART.** This issue occurs when the AP fails over to HA standby. This issue is observed in access points running ArubaOS 8.1.0.0 or later versions. | ArubaOS 8.5.0.1 |
| AOS-194052 | — | A few clients are unable to obtain IP addresses. This issue occurs when High Efficiency is enabled on the WPA2-PSK SSID profile of the APs. This issue is observed in Mobility Controller Virtual Appliances running ArubaOS 8.5.0.0 or later versions.<br>**Workaround:** Disable High Efficiency on the WPA2-PSK SSID profile of the APs. | ArubaOS 8.5.0.0 |
| AOS-194146 | — | A managed device does not display any warning message when the cluster profile name contains more than 32 characters. This issue is observed in managed devices running ArubaOS 8.5.0.2 or later versions in a cluster setup. | ArubaOS 8.5.0.2 |
| AOS-194201 | — | The value of Tx data bytes transmitted for 5 GHz radio is lesser than the actual transmitted value. This issue is observed in AP-205 access points running ArubaOS 8.3.0.0 or later versions. | ArubaOS 8.3.0.0 |
| AOS-194325<br>AOS-194579 | — | The **datapath** process in a managed device crashes multiple times. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions in a Mobility Master-Managed Device topology. | ArubaOS 8.3.0.0 |
| AOS-194370 | — | High Memory utilization is observed in the **cluster manager** process of managed devices. This issue is observed in managed devices running ArubaOS 8.4.0.2 or later versions in a cluster setup. | ArubaOS 8.4.0.2 |
| AOS-194518 | — | APs keep retrying a frame although they receive Block Acknowledgment (BA) packets from clients. This issue is observed in 500 Series access points running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-194706 | — | A managed device crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions in a Mobility Master-Managed Device topology. | ArubaOS 8.5.0.2 |

**Table 7:** *Known Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-194727 | — | An AP sends RTS requests continuously to one client only and this results in delay or packet drop to other clients. This issue is observed in 340 Series access points running ArubaOS 8.3.0.7 or later versions. | ArubaOS 8.3.0.7 |
| AOS-194911 | — | Incorrect flag output is displayed for APs configured with 802.1X authentication when the **show ap database** command is executed. This issue is observed in APs running ArubaOS 8.5.0.2 or later versions. | ArubaOS 8.5.0.2 |
| AOS-194964 | — | A few users are unable to clone the configuration from an existing group to a new group in a Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.4.0.1 or later versions.<br>**Workaround:** Change the operating mode of the AP from am-mode to ap-mode. | ArubaOS 8.5.0.2 |
| AOS-195000 | — | A few APs crash unexpectedly. The log files list the reason for the event as **Kernel panic: softlockup - hung tasks**. This issue is observed in AP-515 access points running ArubaOS 8.5.0.1 or later versions. | ArubaOS 8.5.0.1 |
| AOS-195036 | — | The **authentication** process in a managed device crashes unexpectedly. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions. | ArubaOS 8.3.0.6 |
| AOS-195162 | — | The WebUI is unresponsive and the licenses are not visible in the **Mobility Master > Configuration > Licenses** page in the WebUI. This issue occurs when 29 non-default pools are configured and enabled. This issue is observed in Mobility Masters running ArubaOS 8.5.0.1 or later versions. | ArubaOS 8.5.0.1 |
| AOS-195177 | — | Managed devices frequently generate internal system error logs. This issue occurs when the **sapd** process reads a non-existent interface. This issue is observed in 7220 controllers running ArubaOS 8.3.0.7 or later versions. | ArubaOS 8.3.0.7 |
| AOS-195228 | — | The device status is always displayed as inactive when SNMP walk is performed. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.2 or later versions. | ArubaOS 8.5.0.2 |
| AOS-195265 | — | A managed device crashes and reboots unexpectedly. The log files list the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. This issue occurs due to ACL corruption. This issue is observed in managed devices running ArubaOS 8.5.0.0 or later versions. | ArubaOS 8.5.0.3 |
| AOS-195400 | — | An AP crashes unexpectedly. This issue occurs when creating or deleting a WLAN SSID profile. This issue is observed in 550 Series access points running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-195434 | — | An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is observed in APs running ArubaOS 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology. | ArubaOS 8.5.0.2 |

**Table 7:** *Known Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-195444 | — | Managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:60)**. This issue occurs due to high CPU utilization. This issue is observed in managed devices running ArubaOS 8.5.0.1 or later versions. | ArubaOS 8.5.0.1 |
| AOS-195589<br>AOS-196087 | — | The **Profmgr** process crashes unexpectedly in a Mobility Master. This issue occurs if the VLAN commands entered exceed 256 characters. This issue is observed in Mobility Master running ArubaOS 8.3.0.4 or later versions in a cluster-setup. | ArubaOS 8.3.0.4 |
| AOS-195677<br>AOS-196311 | — | The **airmatch_recv** process crashes unexpectedly in a Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions in a Mobility Master - Managed Device topology. | ArubaOS 8.3.0.7 |
| AOS-195947 | — | APs crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Take care of the TARGET ASSERT first**. This issue occurs due to kernel buffer. This issue is observed in tri-radio enabled AP-555 access points running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-196057 | — | A few APs stop responding to the data frames from the STAs and stop forwarding the ping request packets. This issue is observed in 500 Series access points running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-196101<br>AOS-197335 | — | Access points crash and reboot unexpectedly. The log file lists the reason for the event as **external watchdog reset**. This issue is observed in AP-203H access points running ArubaOS 8.3.0.10 or later versions. | ArubaOS 8.3.0.10 |
| AOS-196215 | — | Some clients are unable to manage multiple clusters using a single Mobility Master. This issue occurs when the Mobility Master assumes that the clusters are on the same VLAN and cannot reuse the same VRRP ID in the cluster profile. This issue is observed in Mobility Master running ArubaOS 8.5.0.3 or later versions.<br>**Workaround:** Use different VRRP IDs for clusters that are on the same VLAN. | ArubaOS 8.5.0.3 |
| AOS-196455 | — | Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. This issue is observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.<br>**Workaround:** The following are recommended:<br>In the CLI, create an AP regulatory-domain- profile without any channel configuration, save the changes and later add or delete channels as desired.<br>In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes and later add or delete channels as desired. | ArubaOS 8.5.0.4 |
| AOS-196457 | — | High radio noise floor is observed on APs. This issue is observed on AP-515 access points running ArubaOS 8.5.0.2 or later versions. | ArubaOS 8.5.0.2 |

**Table 7:** *Known Issues in ArubaOS 8.6.0.2*

| New Bug ID | Old Bug ID | Description | Reported Version |
|---|---|---|---|
| AOS-196560<br>AOS-197671 | — | APs crash and reboot unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue is observed in 500 Series access points running ArubaOS 8.6.0.0 or later versions. | ArubaOS 8.6.0.0 |
| AOS-196629 | — | After a legacy master controller is successfully upgraded to ArubaOS 8.6.0.2, and the **show switches** command is executed, the value of the **Configuration State** parameter is displayed as **LAST SNAPSHOT** for some managed devices. This issue is observed in 9004 and 7280 managed devices running ArubaOS 8.4.0.0 and ArubaOS 8.5.0.0, or later versions.<br>**Workaround:** Upgrade the managed devices to ArubaOS 8.4.0.6 or ArubaOS 8.5.0.5, or later versions. | ArubaOS 8.6.0.2 |
| AOS-196683 | — | Access points come up without standby APs. This issue occurs in a cluster when AP channel scanning detects an invalid AP and skips scanning the remaining APs. This issue is observed in managed devices running ArubaOS 8.5.0.3 or later versions. | ArubaOS 8.5.0.3 |
| AOS-196805 | — | The command **show ap debug client-stats** displays lower rates for management frames. This issue is observed in access points running ArubaOS 8.3.0.6 or later versions. | ArubaOS 8.3.0.6 |
| AOS-196878<br>AOS-197216 | — | The Datapath module crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.** This issue is observed in Managed devices running ArubaOS 8.5.0.2 or later versions. | ArubaOS 8.5.0.2 |
| AOS-196887<br>AOS-196959 | — | WPA3-SAE-AES Opmode enabled clients are unable to connect to the AP and the AP sends **Deauthentication Reason Code: 49 Invalid pairwise masterkey identifier (PMKI) [24-25]** deauthentication code. This issue is observed in access points running ArubaOS 8.5.0.5 or later versions in a cluster setup. | ArubaOS 8.5.0.5 |
| AOS-196896<br>AOS-197050 | — | APs crash and reboot unexpectedly. This issue occurs when the stm process crash when more than 256 clients connected to a Remote AP or Campus AP on bridge mode gets deleted at the same time. This issue is observed in AP-325 access points running ArubaOS 8.5.0.3 or later versions. | ArubaOS 8.5.0.3 |
| AOS-196970 | — | A few APs stop responding to data frames and cannot decode Block Acknowledgment (BA) packets from the STAs causing packet drop. This issue is observed in 500 Series access points running ArubaOS 8.5.0.0 or later versions. | ArubaOS 8.5.0.0 |
| AOS-197160 | — | Managed devices crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2.** This issue occurs due to corrupt ACL entries. This issue is observed in managed devices running ArubaOS 8.3.0.8 in a cluster-setup. | ArubaOS 8.3.0.8 |

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, or stand-alone controller.

Topics in this chapter include:



## Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device?
  - 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 Master Licensing Guide*.
- Multiversion is supported only if the Mobility Master is running two code versions higher than the code versions running on the managed devices. For example multiversion is supported if a Mobility Master is running ArubaOS 8.5.0.0 and the managed devices are running ArubaOS 8.3.0.0 and will not be supported if the managed devices are running ArubaOS 8.2.0.0 or ArubaOS 8.4.0.0.

# 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 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 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 25 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 25 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 25 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 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 memory using the WebUI or CLI.

#### In the WebUI

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

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

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 24.

NOTE

When you navigate to the **Configuration** tab in the WebUI, the managed device might display the **Error getting information: command is not supported on this platform** message. This message 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 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** 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 Master 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 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 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 Master.
   ```
   (host)#reload
   ```
8. Execute the **show version** command to verify that the upgrade is complete.
   ```
   (host)#show version
   ```

## Verifying the ArubaOS Upgrade

Verify the ArubaOS upgrade in the WebUI or CLI.

### In the WebUI

The following steps describe how to verify that the Mobility Master 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 25 for information on creating a backup.

### In the CLI

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 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 25 for information on creating a backup.

# Downgrading ArubaOS

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

## Pre-requisites

Before you reboot the 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 25.
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 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 the pre-upgrade flash backup from the file stored on the Mobility Master 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 Master 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 Master or managed device reboots after the countdown period.
4. When the boot process is complete, verify that the Mobility Master 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 Master 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 Master 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
   ```

CAUTION

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 Master or managed device.

```
(host) # reload
```

6. When the boot process is complete, verify that the Mobility Master 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.