ArubaOS 8.8.0.1 Release Notes

aruba

a Hewlett Packard
Enterprise company

Copyright Information

Open Source Code

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

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

Contents

Contents 3

Revision History 4

Release Overview 5

Related Documents 5

Supported Browsers 5

Terminology Change 5

Contacting Support 6

New Features and Enhancements in ArubaOS 8.8.0.1 7

Supported Platforms in ArubaOS 8.8.0.1 8

Mobility Master Platforms 8

Mobility Controller Platforms 8

AP Platforms 8

Regulatory Updates in ArubaOS 8.8.0.1 10

Resolved Issues in ArubaOS 8.8.0.1 11

Known Issues in ArubaOS 8.8.0.1 15

Limitations 15

Known Issues 15

Upgrade Procedure 21

Important Points to Remember 21

Memory Requirements 22

Backing up Critical Data 23

Upgrading ArubaOS 25

Verifying the ArubaOS Upgrade 26

Downgrading ArubaOS 28

Before Calling Technical Support 30

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 AP-503H access points are added to the list of **Supported Platforms**.
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

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

Chapter 3

New Features and Enhancements in ArubaOS 8.8.0.1

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

Chapter 4
Supported Platforms in ArubaOS 8.8.0.1

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 8.8.0.1*

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 8.8.0.1*

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 8.8.0.1*

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

Table 5: *Supported AP Platforms in ArubaOS 8.8.0.1*

AP Family	AP Model
207 Series	AP-207
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303 Series	AP-303, AP-303P
303H Series	AP-303H, AP-303HR
310 Series	AP-314, AP-315
318 Series	AP-318
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377
370EX Series	AP-375EX, AP-377EX, AP-375ATEX
AP-387	AP-387
500 Series	AP-504, AP-505
500H Series	AP-503H, AP-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 8.8.0.1

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_80292

Chapter 6
Resolved Issues in ArubaOS 8.8.0.1

This chapter describes the resolved issues in this release.

Table 6: *Resolved Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-183519	—	Some APs were incorrectly marked as down in datazone controllers. The fix ensures that the controllers display the correct status of APs. This issue was observed in stand-alone controllers running ArubaOS 8.3.0.4 or later versions.	ArubaOS 8.3.0.4
AOS-208740 AOS-213754	—	The **profmgr** process crashed on a few Mobility Masters running ArubaOS 8.5.0.11 or later versions. The fix ensures that the Mobility Masters work as expected.	ArubaOS 8.5.0.11
AOS-208846	—	Clients connected to bridge mode SSIDs were unable to receive IP addresses and pass traffic. The fix ensures that clients are able to receive IP addresses. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-209127 AOS-211115	—	Internal server timeout was observed during an authentication request. The fix ensures successful authentication. This issue was observed in stand-alone controllers with master-redundancy setup using VRRP environment, where the stand-alone controllers were running ArubaOS 8.6.0.4 or later versions.	ArubaOS 8.6.0.4
AOS-211545 AOS-217654	—	Some APs running ArubaOS 8.5.0.10 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt.** The fix ensures that the APs work as expected.	ArubaOS 8.5.0.10
AOS-211622 AOS-211728	—	Some stand-alone controllers running ArubaOS 8.3.0.14 or later versions crashed and rebooted unexpectedly. The log files listed the reason for the event as, **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:0:2c)**. The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.3.0.14

Table 6: *Resolved Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212904	—	Users were unable to access the L3 redundant controller using CLI and the error message, **Permission path (/) is Invalid for user (ads.jvicentini)** was displayed. The fix ensures that the users are able to access the L3 redundant controller using CLI. This issue was observed in standby Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-213041 AOS-215501	—	A managed device did not classify WebCC and DPI traffic. The fix ensures that the managed device classifies WebCC and DPI traffic. This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-213784	—	A server received multiple **GSM radio lookup failed, error(error_htbl_key_not_found)** notifications for all BSSIDs. This issue is resolved by moving the GSM lookup failure logs to user-debug category. This issue was observed in a Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-214391 AOS-217130 AOS-217832	—	Some APs were unable to come up on a managed device. This issue occurred when UDP 8209 traffic was sent without establishing IPsec tunnels. . The fix ensures that the APs are able to come up on a managed device. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-214416	—	Some stand-alone controllers running ArubaOS 8.6.0.6 or later versions displayed the error message, **An internal system error has occurred at file main.c function rx_handler line 1517 error sxdr_read_str_safe szFunctionName failed.** The fix ensures that the stand-alone controllers work as expected.	ArubaOS 8.6.0.6
AOS-214434	—	Some APs were unable to come up on a managed device. This issue occurred when UDP 8209 traffic was sent without establishing IPsec tunnels. The fix ensures that the APs are able to come up on a managed device. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-215495	—	Some APs displayed the error message, **ARM Channel 40 Physical_Error_Rate 0 MAC_Error_Rate 84 Frame_Retry_Rate 0 arm_error_rate_threshold 70 arm_error_rate_wait_time 90**. The fix ensures that the APs work as expected. This issue was observed in AP-535 access points running ArubaOS 8.5.0.5 or later versions.	ArubaOS 8.5.0.5
AOS-216525	—	9012 controllers running ArubaOS 8.6.0.0 or later versions experienced traffic drop when the client and server were on different VLANs. The fix ensures that the 9012 controllers work as expected.	ArubaOS 8.6.0.4

Table 6: *Resolved Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-217382	—	VRRP flapping was observed in a few Mobility Masters. This issue occurred when the VRRP master could not send periodic advertisements. The fix ensures that the Mobility Masters work as expected. This issue was observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-217539 AOS-219010 AOS-219952 AOS-220918 AOS-221298	—	The **auth** process crashed on managed devices running ArubaOS 8.6.0.6 or later versions. The fix ensures that the managed devices work as expected.	ArubaOS 8.6.0.6
AOS-217678 AOS-218131	—	Some APs did not honor the user alias route src-nat ACL and tunneled the traffic to managed devices. The issue occurred when a netdestination alias is configured in the ACL. The fix ensures that the APs work as expected. This issue is observed in APs running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-217694 AOS-218525	—	Some APs running ArubaOS 8.7.1.1 or later versions crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel Panic: Take care of the TARGET ASSERT first**. The fix ensures that the APs work as expected.	ArubaOS 8.7.1.1
AOS-217703	—	Some managed devices took a long time to boot up after an upgrade. The fix ensures that the managed devices do not take a long time to boot up. This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-218117 AOS-219179	—	The **show ntp servers** and **show ntp status** commands displayed the error message, **Address family for hostname not supported**. However, the WebUI displayed the NTP servers. The fix ensures that the commands do not display the error message. This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	ArubaOS 8.6.0.7
AOS-218167	—	Users were unable to delete static OSPF aggregate routes. The fix ensures that the users are able to delete static OSPF aggregate routes. This issue was observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-218208	—	Some clients were unable to connect to APs. The log file listed the reason for the event as, **AP is resource constrained**. The fix ensures seamless connectivity. This issue was observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8

Table 6: *Resolved Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218277 AOS-214428	—	The **auth** process crashed on managed devices running ArubaOS 8.5.0.11 or later versions. Hence, the Remote APs rebooted and VIA users faced connectivity issues. The fix ensures that the managed devices work as expected.	ArubaOS 8.5.0.11
AOS-219008	—	Some UI endpoints like API page, spectrum displayed information even before authentication. This issue was observed when the API request came over port 443. The fix ensures that the managed devices work as expected.	ArubaOS 8.8.0.0

Chapter 7
Known Issues in ArubaOS 8.8.0.1

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

Limitations

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.

Custom Certificate

When ArubaOS is downgraded from 8.8.0.0 to 8.7.0.0, APs retains the custom certificate that was synchronized in ArubaOS 8.8.0.0. In ArubaOS 8.8.0.0, an AP downloads the custom certificate from a managed device and saves it in its flash memory if a bridge mode SSID is configured. If the managed device is downgraded to ArubaOS 8.7.0.0, the AP is also downgraded. The AP that is running ArubaOS 8.7.0.0 checks if any custom certificate is saved in its flash memory. If the AP finds a custom certificate saved in its flash memory, it uses the custom certificate. If the AP does not find a custom certificate saved in its flash memory, it generates a new default certificate. If you do not want to use the custom certificate, issue the following command to erase the flash sector:

```
apfcutil -i RAP
```

The AP reboots and generates new default certificate.

Known Issues

Following are the known issues observed in this release.

Table 7: *Known Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
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 8.8.0.1*

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-208102 AOS-214040	—	APs running ArubaOS 8.7.0.0 or later versions crash unexpectedly. The log files list the reason for the event as **Process /aruba/bin/sapd has too many open files (771)**.	ArubaOS 8.7.0.0
AOS-209093 AOS-210452	—	Some managed devices running ArubaOS 8.7.0.0 or later versions generate multiple AMON receiver errors.	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-210198	—	The **Dashboard > Security > Detected Radio** page of the WebUI displays incorrect number of **Clients**. This issue is observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	ArubaOS 8.6.0.5
AOS-210416 AOS-210480	—	The **show ap client trail-info** command display incorrect **VLAN(s)** values. This issue is observed in Mobility Masters running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-211720	—	The **STM** process crashes on managed devices running ArubaOS 8.5.0.5 or later versions and hence, APs failover to another cluster.	ArubaOS 8.5.0.5
AOS-212605 AOS-218721	—	Some APs running ArubaOS 8.6.0.9 or later versions crashes unexpectedly. The log files list the reason for the event as **wlc_key_get_info+0x4/0x60 [wl_v6]**.	ArubaOS 8.7.1.1

Table 7: *Known Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-212861 AOS-215350 AOS-215522 AOS-216305	—	Some AP-535 and AP-555 access points running ArubaOS 8.6.0.6 or later versions crash and reboot unexpectedly. The log file lists the reason for the reboot as **kernel panic: Take care of the TARGET ASSERT first.**	ArubaOS 8.6.0.6
AOS-213011 AOS-219946	—	Packet loss is observed for clients during a cluster failover. This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions.	ArubaOS 8.5.0.10
AOS-214963	—	Some APs running ArubaOS 8.5.0.11 or later versions detect false radar.	ArubaOS 8.5.0.11
AOS-214977	—	Memory leak is observed in **arci-cli-helper** process. This issue occurs while running an API script. This issue is observed in APs running ArubaOS 8.5.0.8 or later versions.	ArubaOS 8.5.0.8
AOS-215498	—	Some AP-535 access points running ArubaOS 8.5.0.11 or later versions detect false radar.	ArubaOS 8.5.0.11
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 UCC session idle timeout.	ArubaOS 8.6.0.6
AOS-216512	—	The DHCP client / station related AMON message sends the mask, server IP address, and client IP address in a reverse order to the AirWave server. This issue is observed in Mobility Masters running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
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-216764	—	Users are not redirected to the captive portal page. This issue is observed in managed devices running ArubaOS 8.7.1.0 or later versions in a cluster setup.	ArubaOS 8.7.1.0
AOS-216766	—	Some APs generate sapd coredump. This issue is observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-216874 AOS-219841	—	The virtual MAC address of the VLAN gets deleted from the bridge table and hence, results in network outage. This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11

Table 7: *Known Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-216972	—	Some managed devices running ArubaOS 8.6.0.7 or later versions forward data frames that are larger than the configured IPsec tunnel MTU value.	ArubaOS 8.6.0.7
AOS-217104 AOS-219159	—	ESI redirect fails and traffic gets forwarded to the default gateway. This issue is observed in managed devices running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-217106	—	The **no valid** parameter of the **ap regulatory-domain-profile** command does not work while creating a new regulatory profile. This issue is observed in controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** Configure and save an ap regulatory-domain-profile and then issue the no valid commands.	ArubaOS 8.6.0.7
AOS-217807	—	Remote APs take a long time to come up on a managed device. This issue occurs due to a delay in whitelist-db synchronization between theMobility Master and managed devices and when external authentication is enabled for Remote APs. This issue is observed in managed devices running ArubaOS 8.6.0.5 or later versions in a cluster setup.	ArubaOS 8.6.0.5
AOS-218012	—	The **Maintenance** tab of the WebUI displays a list of clusters that are not configured for that particular node. This issue is observed in Mobility Masters running ArubaOS 8.5.0.9 or later versions.	ArubaOS 8.5.0.9
AOS-218075 AOS-219316	—	Some managed devices running ArubaOS 8.5.0.11 or later versions log multiple error message, **Trying to obtain mac address**. .	ArubaOS 8.5.0.11
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-218231 AOS-216177	—	Wireless users are unable to find a few wired clients. This issue is observed in controllers 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-218404 AOS-212330	—	Some APs are unable to ping a few clients. This issue is observed in APs running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-218518 AOS-218880	—	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 reason Datapath timeout (SOS Assert).**	ArubaOS 8.7.1.0

Table 7: *Known Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-218621	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **AP Reboot reason: BadAddr:6c0094119461 PC:wlc_ampdu_recv_addba_resp+0x240/0x838 [wl_v6] Warm-reset**.	ArubaOS 8.7.1.1
AOS-218622	—	Some APs running ArubaOS 8.6.0.6 or later versions crashes unexpectedly. The log files list the reason for the event as **PC:aruba_wlc_ratesel_getcurrate+0x24/0xd0 [wl_v6] Warm-reset**.	ArubaOS 8.7.1.1
AOS-218822	—	High flash memory utilization is observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	ArubaOS 8.5.0.10
AOS-219034	—	Clients connecting to HT-enabled SSIDs connect as non-HT clients. This issue is observed in APs running ArubaOS 8.6.0.6 or later versions.	ArubaOS 8.6.0.6
AOS-219098 AOS-219914	—	Some devices are unable to connect to the network. This issue is observed in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219178	—	Clients connecting to the anchor controller are unable to receive IP addresses. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions.	ArubaOS 8.3.0.7
AOS-219214	—	The validuser acl list gets reordered in stand-alone controllers running ArubaOS 8.6.0.8 or later versions.	ArubaOS 8.6.0.8
AOS-219328	—	SNMP configurations fail and the error message, **Error: User (itam_net) should be created before adding to the trap host** is displayed. This issue occurs when the SNMP server v3 trap host which has the engine-id same as the engine-id of the controller is removed and added again. This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions.	ArubaOS 8.5.0.11
AOS-219365	—	Some APs running ArubaOS 8.7.0.0 or later versions reboot sporadically. This issue occurs when smart antenna feature is enabled.	ArubaOS 8.7.1.1
AOS-219379	—	Some Mobility Controllers are unable to connect to Mobility Controller Virtual Appliance. The log files list the reason for the event as **<WARN> |fpapps| handleMasterIpMsg: Ignoring duplicate Uplink update from CFGM: ip x.x.x.x sec_master_ip 0.0.0.0 role 3;.** This issue is observed in Mobility Controllers running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219383	—	The **Configuration > License > License Usage** tab does not display the license relates details. This issue is observed in stand-alone controllers running ArubaOS 8.5.0.12 or later versions.	ArubaOS 8.5.0.12

Table 7: *Known Issues in ArubaOS 8.8.0.1*

New Bug ID	Old Bug ID	Description	Reported Version
AOS-219384	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **PC is at wlc_nar_dotxstatus+0x450**.	ArubaOS 8.7.1.1
AOS-219390	—	The **datapath** process crashes on stand-alone controllers running ArubaOS 8.7.1.1 or later versions. The log files list the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. This issue occurs when the op mode of the SSID profile was changed from WPA3-AES-CCM-128 to WPA3-CNSA.	ArubaOS 8.7.1.1
AOS-219594	—	The **Logon-Webcc** process crashes on Mobility Masters running ArubaOS 8.7.1.2 or later versions	ArubaOS 8.7.1.2
AOS-219627 AOS-218851	—	Clients are unable to connect to 2.4GHz SSID of some APs. This issue occurs when the MAC address of the Radio 1 is incorrect. This issue is observed in APs running ArubaOS 8.7.1.1 or later versions.	ArubaOS 8.7.1.1
AOS-219725	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **PC is at wlc_nar_detach+0x8c**.	ArubaOS 8.7.1.1
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-219978 AOS-220568	—	iPhone 12 Pro users experience poor upstream network performance. This issue occurs when APs operate in tunnel mode. This issue is observed in APs running ArubaOS 8.6.0.9 or later versions in tunnel mode. **Workaround:** Disable AMSDU configuration in the **Configuration > Services > Firewall > Global Settings** page.	ArubaOS 8.7.1.2
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
AOS-220183	—	The user table does not list the PUTN users and the error message, **Dropping bridge miss rcvd for dormant PUTN user** is displayed. This issue is observed in managed devices running ArubaOS 8.7.1.0 or later versions.	ArubaOS 8.7.1.0
AOS-220293	—	Some APs running ArubaOS 8.7.1.1 or later versions crashes unexpectedly. The log files list the reason for the event as **aruba_wlc_ratesel_getmaxrate+0x34**.	ArubaOS 8.7.1.1
AOS-220996	—	The **switch_daemon** process crashes on Mobility Masters 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.

CAUTION

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 23 to copy the **crash.tar** file to an external server. Execute the **tar clean crash** command to delete the file from the managed device.
    - **Flash backups:** Use the procedures described in Backing up Critical Data on page 23 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
    - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 23 to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

CAUTION

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.

CAUTION

Ensure that there is enough free memory and flash space on your Mobility Conductor or managed device. For details, see Memory Requirements on page 22.

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.

NOTE

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

4. Log in to the ArubaOS WebUI from the Mobility Conductor.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.

   a. Select the **Local File** option from the **Upgrade using** drop-down list.

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

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

NOTE

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

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

In the CLI

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

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

2. Open an SSH session to your Mobility Conductor.

3. Execute the **ping** command to verify the network connection between the Mobility Conductor and the SCP server, FTP server, or TFTP server.

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

or

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

or

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

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

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Conductor.

```
(host)#reload
```

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

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

Verifying the ArubaOS Upgrade

Verify the ArubaOS upgrade in the WebUI or CLI.

In the WebUI

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

1. Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version.
2. Verify if all the managed devices are up after the reboot.
3. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
4. Verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 23 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show version** command to verify the ArubaOS image version.
3. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
4. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
5. Test a different type of client in different locations, for each access method used.
6. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 23 for information on creating a backup.

Downgrading ArubaOS

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

Pre-requisites

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

1. Back up your Mobility Conductor or managed device. For details, see Backing up Critical Data on page 23.
2. Verify that the control plane security is disabled.
3. Set the Mobility Conductor or managed device to boot with the previously saved configuration file.
4. Set the Mobility Conductor or managed device to boot from the partition that contains the pre-upgrade ArubaOS version.

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

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

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the ArubaOS version:

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

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

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

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

CAUTION

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
```

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 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.