ArubaOS 8.5.0.13

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
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Contents

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

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
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.

Important Points Before Upgrading to ArubaOS 8.5.0.0

Starting from ArubaOS 8.5.0.0, the VMware hardware CPU should support SSE 4.2 or higher version. If enabled, Enhanced vMotion Compatibility (EVC) should present an appropriate CPU architecture which must support SSE4.2 or higher version. For deployments on versions prior to ArubaOS 8.5.0.0, SSE3 is the minimum supported version.

Additionally, the VMWARE CPU should also support Intel VT in all cases.

DPI Classification

DPI classification is not initialized after a controller is upgraded from ArubaOS 8.4.0.0, 8.4.0.1, or 8.4.0.2 to ArubaOS 8.5.0.0. The affected platforms are 7200 Series controllers.

An additional reboot of the affected platform is required to initialize DPI classification.

To check the status of DPI classification after upgrading an affected platform from ArubaOS 8.4.0.0, 8.4.0.1, or 8.4.0.2 to ArubaOS, 8.5.0.0, issue the **show firewall | include dpi** command. In the following example, DPI classification is disabled:

```
(host) #show firewall | include dpi
DPI Classification      Disabled [Cfg: enabled, PEF license: installed]
```

If DPI classification is enabled, further action is not needed. However, if DP classification is disabled, issue the **show datapath utilization** and check if the DPI classification CPUs are initialized. In the following example, the DPI classification CPUs are disabled:

```
(host) #show datapath utilization

Datapath CPU Allocation Summary
Slow Path (SP) : 1,  Slow Path Gateway (SPGW) : 1
Fast Path (FP) : 17,  Fast Path Gateway (FPGW) : 1
DPI : 0, Crypto (CRYP) : 0
Slow Path Spare (SPSPARE) : 0
```

If the DPI classification CPUs are not initialized, reboot the affected platform by:

- Issuing the **reload** command.

- Power cycling the controller.

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 Master 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 58 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.arubanetworks.com/
Airheads Social Forums and Knowledge Base	community.arubanetworks.com

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

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

CLI

show datapath frame debug command

Starting from ArubaOS 8.5.0.13, the output of the **show datapath frame debug** command has been modified to display **vlan bcmc drop frames** instead of **vlan bcmc check fails**.

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 8.5.0.13*

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 8.5.0.13*

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 8.5.0.13*

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, AP-303P
303H Series	AP-303H

Table 5: *Supported AP Platforms in ArubaOS 8.5.0.13*

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
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

Chapter 4
Regulatory Updates

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

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

The following DRT file version is part of this release:

- DRT-1.0_80036

Also, the following issues are resolved in this release.

We have migrated to a new defect tracking tool. All the bugs are listed with the new bug ID, which is prefixed by AOS.

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146920 AOS-210879	—	**Symptom:** Users were unable to delete an ACL policy configured with DSCP option. The fix ensures that users are able to delete the ACL policy. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.1 or later versions	Base OS Security	All platforms	ArubaOS 8.5.0.1
AOS-183519	—	**Symptom:** Some APs were incorrectly marked as down in datazone controllers. The fix ensures that the controllers display the correct status of APs. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.3.0.4 or later versions.	AP-Platform	All platforms	ArubaOS 8.3.0.4
AOS-187395 AOS-188564	—	**Symptom:** The AAA test to the external server failed in the **Diagnostics > Tools > AAA Server Test** page of the WebUI. The fix ensures that the AAA test to external server does not fail. **Scenario:** This issue occurred when the user entered the **"**, **%**, and **#** special characters in the **Password** field and clicked the **Test** option. As a result, the WebUI displayed the **Authentication** field as **failed** and **Processing time (ms)** field as **N/A**. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.4.0.2
AOS-188090 AOS-196004 AOS-199152	—	**Symptom:** The **Dashboard > Overview > Clients** page of the WebUI displayed incorrect client usage values intermittently. The fix ensures that the WebUI displays the correct values. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.4.0.0 or later versions.	Monitoring	All platforms	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188527 AOS-193897 AOS-202879	—	**Symptom:** The IP address of the NAT configured managed device was visible in the HTTP header of the web server. The fix ensures that the IP address is not visible in the HTTP header of the web server. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	Web Server	All platforms	ArubaOS 8.3.0.0
AOS-192738 AOS-197047	—	**Symptom:** The Mobility Master list in the WebUI incorrectly displayed the MAC address of the primary Mobility Master for the secondary Mobility Master. The fix ensures that the WebUI displays the correct MAC address. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.3.0.10 or later versions.	WebUI	All platforms	ArubaOS 8.3.0.10
AOS-195101	—	**Symptom:** Traffic between Master redundancy Mobility Masters dropped causing a few processes to be in **PROCESS_NOT_ RESPONDING** state. Hence, configurations were not synchronized between the peers. The fix ensures that the Mobility Masters work as expected. **Scenario:** This issue occurred when the **ipsec-mark-mgmt-frames** parameter was enabled in the **firewall wireless-bridge-aging** command. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.5.0.2
AOS-195526	—	**Symptom:** Clients were unable to get the DHCP address. The fix ensures that clients are able to obtain DHCP address. **Scenario:** This issue occurred because the ACE entries of the logon role ACL changed to **Deny all** when the PEFNG feature was disabled. This issue was observed in managed devices running ArubaOS 8.3.0.8 or later versions.	Base OS Security	All platforms	ArubaOS 8.3.0.8
AOS-202210 AOS-218532	—	**Symptom:** The **show iap table** and **show iap table long** commands did not display the list of Instant APs. The fix ensures that the commands display the list of Instant APs. **Scenario:** This issue was observed in controllers running ArubaOS 8.6.0.6 or later versions in a VPNC deployment.	Web Server	All platforms	ArubaOS 8.6.0.6

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-203115 AOS-217219	—	**Symptom:** The IAP-VPN tunnel went down and the error message, **Failed to create internal-iap IP user entry and user entry due to too many user entries 128** was displayed. The fix ensures that the stand-alone controllers work as expected. **Scenario:** This issue occurred when the user table had 128 entries. This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	IPsec	All platforms	ArubaOS 8.6.0.4
AOS-203926 AOS-217462 AOS-217578	—	**Symptom:** Voice traffic using NOE protocol was not getting tunneled in split tunnel forwarding mode. The fix ensures that the voice traffic using NOE protocol is tunneled. **Scenario:** This issue occurred when openflow was enabled. This issue was observed in managed devices running ArubaOS 8.6.0.3 or later versions.	AP Datapath	All platforms	ArubaOS 8.6.0.3
AOS-204158	—	**Symptom:** Users were unable to access the network. The fix ensures seamless connectivity. **Scenario:** This issue occurred after a reboot of the managed device during a cluster failover. This issue was observed in managed devices running ArubaOS 8.3.0.12 or later versions.	RADIUS	All platforms	ArubaOS 8.3.0.12
AOS-204334 AOS-205224 AOS-212129	—	**Symptom:** The **Upgrademgr** process was stuck and stopped responding after a reboot of the Mobility Master. The fix ensures that the Mobility Masters work as expected. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions.	Image Upgrade	All platforms	ArubaOS 8.5.0.0
AOS-206045	—	**Symptom:** Some managed devices initiated multiple RADIUS access requests simultaneously. The fix ensures that the managed devices do not initiate multiple RADIUS access requests simultaneously. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.4 or later versions.	RADIUS	All platforms	ArubaOS 8.5.0.4
AOS-206389 AOS-216860	—	**Symptom:** The **SAPD** process crashed on managed devices. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.6.0.5 or later versions.	AP-Platform	All platforms	ArubaOS 8.6.0.5

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-207664 AOS-213842 AOS-219671	—	**Symptom:** The login banner text was not displayed after upgrading the managed devices to ArubaOS 8.5.0.0 or later versions. The fix ensures that the login banner is displayed. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.5.0.0
AOS-207701 AOS-218006	—	**Symptom:** The RADIUS request packets did not contain the state attribute value and hence, clients faced connectivity issues. The fix ensures that the managed devices work as expected. **Scenario:** This issue occurred due to a race condition. This issue was observed in managed devices running ArubaOS 8.4.0.0 or later versions.	RADIUS	All platforms	ArubaOS 8.4.0.0
AOS-207775 AOS-215946	—	**Symptom:** The **auth** process crashed on managed devices. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.9 or later versions.	Base OS Security	All platforms	ArubaOS 8.5.0.9
AOS-208337 AOS-209348 AOS-212655 AOS-213442 AOS-219341	—	**Symptom:** The **airmatch_recv** process crashed on Mobility Master Virtual Appliances. The fix ensures that the Mobility Master Virtual Appliances work as expected. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.5.0.7 or later versions.	AirMatch	All platforms	ArubaOS 8.5.0.7
AOS-208625	—	**Symptom:** The RADIUS accounting packets did not have location and AP group related details. The fix ensures that location and AP group related details are available in the RADIUS accounting packets. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.7 or later versions.	RADIUS	All platforms	ArubaOS 8.5.0.7
AOS-208740 AOS-213754	—	**Symptom:** The **profmgr** process crashed on a few Mobility Masters. The fix ensures that the Mobility Masters work as expected. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.5.0.11 or later versions	AP-Platform	All platforms	ArubaOS 8.5.0.11

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-209086 AOS-216862	—	**Symptom:** The **Dot1X** process crashed on a few managed devices. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.0 or later versions.	Dot1X	All platforms	ArubaOS 8.5.0.0
AOS-209127	—	**Symptom:** Internal server timeout was observed during an authentication request. The fix ensures successful authentication. **Symptom:** 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.	Base OS Security	All platforms	ArubaOS 8.6.0.4
AOS-209165	—	**Symptom:** The **Configuration > AP Groups** page did not sort the list of AP groups based on when they were created, and hence the newly created AP groups were displayed at the bottom of the table. The fix ensures that the WebUI sorts the list of AP groups. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.3.0.0
AOS-209196 AOS-213746	—	**Symptom:** Some APs rebooted unexpectedly. The fix ensures that the APs work as expected. **Scenario:** The issue occurred when tunnel forwarding modes, dot11k, and WPA3 were enabled in APs. This issue was observed in AP-345 access points running ArubaOS 8.5.0.8 or later versions.	AP-Platform	AP-345 access points	ArubaOS 8.5.0.8
AOS-209402	—	**Symptom:** A few clients experienced dot1x timeout in split tunnel mode. The fix ensures that the clients do not experience a timeout. **Scenario:** This issue occurred when multiple wired clients were connected to an AP. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.3.0.0
AOS-209679 AOS-210115	—	**Symptom:** The **SAPD** process crashed on APs. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running ArubaOS 8.5.0.10 or later versions.	AP-Platform	All platforms	ArubaOS 8.5.0.10
AOS-210342	—	**Symptom:** The VRRP authentication password was not encrypted in the output of the **show running config** command. The fix ensures that the VRRP authentication password is encrypted. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.10 or later versions.	L2 Forwarding	All platforms	ArubaOS 8.5.0.10

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-211622 AOS-211728	—	**Symptom:** Some stand-alone controllers 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. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.3.0.14 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.3.0.14
AOS-212063 AOS-216153	—	**Symptom:** Licenses got installed with incorrect dates in some Mobility Masters. The fix ensures that the licenses are installed using correct dates. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	Licensing	All platforms	ArubaOS 8.5.0.10
AOS-212198	—	**Symptom:** Some Remote APs rebooted unexpectedly. The fix ensures that the Remote APs work as expected. **Scenario:** This issue occurred when time between the controller and the Remote AP was not in synchronization. This issue was observed in RAP-3WN Remote APs running ArubaOS 8.5.0.8 or later versions.	AP-Platform	RAP-3WN Remote APs	ArubaOS 8.5.0.8
AOS-212530 AOS-220288	—	**Symptom:** Some APs crashed and rebooted unexpectedly. The log files listed the reason for the event as, **reboot Intermittently-suspecting scb rrm cubby corruption.** The fix ensures that the APs work as expected. **Scenario:** This issue was observed in AP-515 access points running ArubaOS 8.5.0.10 or later versions.	AP-Wireless	AP-515 access points	ArubaOS 8.5.0.10
AOS-212568	—	**Symptom:** The **aaa/certmgr/cpsec** security category in the **Configuration > System > Logging > Logging Levels** page of the WebUI displays **None** even if values were configured. The fix ensures that the WebUI displays the correct values. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	Configuration	All platforms	ArubaOS 8.3.0.13

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-212904	—	**Symptom:** 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. **Scenario:** This issue was observed in standby Mobility Masters running ArubaOS 8.5.0.10 or later versions.	Base OS Security	All platforms	ArubaOS 8.5.0.10
AOS-212935	—	**Symptom:** Temporary ACL was applied to user roles even if the disaster-recovery mode was disabled. The fix ensures that the managed devices work as expected. **Scenario:** This issue occurred when configuration changes in disaster-recovery mode were not submitted using the **write memory** command. This issue was observed in managed devices running ArubaOS 8.3.0.6 or later versions.	Configuration	All platforms	ArubaOS 8.3.0.6
AOS-212980 AOS-217034 AOS-217127	—	**Symptom:** The **show datapath session dpi counters** table did not display any output. The fix ensures that the command works as expected. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.5.0.11 or later versions.	Controller Platform	All platforms	ArubaOS 8.5.0.11
AOS-213041 AOS-215501	—	**Symptom:** A managed device did not classify web-cc and DPI traffic. The fix ensures that the managed device classifies web-cc and DPI traffic. **Scenario:** This issue was observed in managed devices access points running ArubaOS 8.5.0.10 or later versions.	WebCC	All platforms	ArubaOS 8.5.0.10
AOS-213089	—	**Symptom:** Some managed devices crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:30:2).** The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions. **Duplicates:** AOS-213044, AOS-213295, AOS-214238, AOS-214431, AOS-214678, AOS-215123, and AOS-215572	Controller Platform	All platforms	ArubaOS 8.3.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-213115	—	**Symptom:** Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first.** The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running ArubaOS 8.5.0.10 or later versions.	AP-Wireless	All platforms	ArubaOS 8.5.0.10
AOS-213132 AOS-216300	—	**Symptom:** Users were unable to upload server certificates in PEM or DER format. The fix ensures that users are able to upload server certificates. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.6.0.6-FIPS.	Certificate Manager	All platforms	ArubaOS 8.6.0.6-FIPS
AOS-213305 AOS-213310 AOS-218723	—	**Symptom:** Some APs crashed and rebooted unexpectedly. The log file lists the reason for the event as **PC is at wlc_nar_ dotxstatus+0x88/0x7d8: AOS-200674 instrumentation kicks in (wlc_nar_validate_cubby).** The fix ensures that the APs work as expected. **Scenario:** This issue was observed in AP-515 access points running ArubaOS 8.7.0.0 or later versions	AP-Wireless	AP-515 access points	ArubaOS 8.7.0.0
AOS-213307	—	**Symptom:** L2 GRE ICMP keepalive response was sent outside the tunnel and hence, got dropped by the firewall. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.1 or later versions.	GRE	All platforms	ArubaOS 8.5.0.1
AOS-213784	—	**Symptom:** 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. **Scenario:** This issue was observed in a Mobility Masters running ArubaOS 8.6.0.5 or later versions.	AirGroup	All platforms	ArubaOS 8.6.0.5

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-213865	—	**Symptom:** The WebUI displayed the message, **one or more settings have been overridden at bottling** and displayed the older folder name after an override. The fix ensures that the WebUI does not displays the older folder name. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	Configuration	All platforms	ArubaOS 8.5.0.10
AOS-214243 AOS-215775	—	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:b0:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to a race condition. This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	Controller-Platform	All platforms	ArubaOS 8.6.0.7
AOS-214255	—	**Symptom:** Older 802.11b clients were unable to connect to a few APs. The fix ensures seamless connectivity. **Scenario:** This issue occurred when VAPs on 2.4 GHz radio were configured with different basic rates and when some of which did not include 802.11b CCK rates. This issue was observed in AP-203R, AP-203RP, AP-203H, and AP-207 access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-203R, AP-203RP, AP-203H, and AP-207 access points	ArubaOS 8.3.0.13
AOS-214391 AOS-217130 AOS-217832	—	**Symptom:** The STM process crashed on 7240XM controllers. The fix ensures that the controllers work as expected. **Scenario:** This issue was observed in 7240XM controllers running ArubaOS 8.4.0.0 or later versions.	Station Management	7240XM controllers	ArubaOS 8.4.0.0
AOS-214434	—	**Symptom:** Some APs were unable to come up on a managed device. The fix ensures that the APs are able to come up on a managed device. **Scenario:** This issue occurred when UDP 8209 traffic was sent without establishing IPsec tunnels. This issue was observed in managed devices running ArubaOS 8.5.0.8 or later versions.	AP Datapath	All platforms	ArubaOS 8.5.0.8

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-214714	—	**Symptom:** Some stand-alone controllers rebooted unexpectedly. The log file lists the reason for the event as, **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60).** The fix ensures that the stand-alone controllers work as expected. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.5.0.11 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.5.0.11
AOS-214835 AOS-218512 AOS-219282	—	**Symptom:** Some wireless clients connected to APs experienced slow network speed. Enhancements to the driver resolved the issue. **Scenario:** This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.3.0.0
AOS-215012 AOS-215567	—	**Symptom:** The AP debug counters, **Total Bootstraps** and **Reboots** were not reset after upgrading the managed devices to ArubaOS 8.5.0.11 or later versions. The fix ensures that the AP debug counters are reset. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	AP-Platform	All platforms	ArubaOS 8.5.0.11
AOS-215073	—	**Symptom:** Some APs went down and kept rebooting. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when many VAP configurations were sent from the **SAPD** to **AP-STM** process. This issue was observed in AP-515 access points running ArubaOS 8.5.0.8 or later versions.	AP-Platform	AP-515 access points	ArubaOS 8.5.0.8
AOS-215483 AOS-218551	—	**Symptom:** Users were unable to disable DPI. The fix ensures that users are able to enable and disable DPI. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.5.0.11 or later versions.	Controller-Platform	All platforms	ArubaOS 8.5.0.11
AOS-215495	—	**Symptom:** 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. **Scenario:** This issue was observed in AP-535 access points running ArubaOS 8.5.0.5 or later versions.	AP-Wireless	AP-535 access points	ArubaOS 8.5.0.5

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-215641 AOS-215642 AOS-217268 AOS-217362 AOS-217640	—	**Symptom:** The **ISAKMPD** process crashed on managed devices in a PSK-RAP setup. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.6.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.6.0.0
AOS-216204 AOS-219455	—	**Symptom:** Some APs crashed unexpectedly. The log file listed the reason for the event as, **Reboot caused by kernel panic: subsys-restart: Resetting the SoC - q6v5-wcss crashed**. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in AP-535 access points running ArubaOS 8.5.0.10 or later versions.	AP-Wireless	AP-535 access points	ArubaOS 8.5.0.10
AOS-216205	—	**Symptom:** Some APs crashed and rebooted unexpectedly. The log file listed the reason for the event as, **Reboot caused by kernel panic: CPU 0 stall**. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running ArubaOS 8.5.0.10 or later versions.	AP-Wireless	All platforms	ArubaOS 8.5.0.10
AOS-216281	—	**Symptom:** Some APs did not display any information related to crash. The fix ensures that the APs displays information related to crash and APs work as expected. **Scenario:** This issue occurred when the APs crashed twice. This issue was observed in APs running ArubaOS 8.6.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.6.0.0
AOS-216752 AOS-217439 AOS-217893	—	**Symptom:** The **impystart** process crashed on a Mobility Master Virtual Appliance. The fix ensures that the Mobility Master Virtual Appliance works as expected. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.5.0.4 or later versions.	IoT	All platforms	ArubaOS 8.5.0.4
AOS-217035	—	**Symptom:** A few APs were down and were unable to connect to the managed device. The fix ensures that the APs work as expected. **Scenario:** This issue occurred when UDP traffic was sent without establishing IPsec tunnels. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.3.0.0

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-217262	—	**Symptom:** Some APs displayed incorrect channel utilization. The fix ensures that the APs display correct values for channel utilization **Scenario:** This issue occurred when APs operated in 20 Mhz channel. This issue was observed in APs running ArubaOS 8.5.0.11 or later versions.	AP-Wireless	All platforms	ArubaOS 8.5.0.11
AOS-217382	—	**Symptom:** VRRP flapping was observed in a few Mobility Masters. The fix ensures that the Mobility Masters work as expected. **Scenario:** This issue occurred when the VRRP master could not send periodic advertisements. This issue was observed in Mobility Masters running ArubaOS 8.6.0.5 or later versions.	VRRP	All platforms	ArubaOS 8.6.0.5
AOS-217678 AOS-218131	—	**Symptom:** Some APs did not honour the user alias route src-nat ACL and tunneled the traffic to managed devices. The fix ensures that the APs work as expected. **Scenario:** The issue occurred when a netdestination alias is configured in the ACL. This issue is observed in APs running ArubaOS 8.6.0.7 or later versions.	RAP + BOAP	All platforms	ArubaOS 8.6.0.7
AOS-217703	—	**Symptom:** 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. **Scenario:** This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	Configuration	All platforms	ArubaOS 8.6.0.7
AOS-218075 AOS-219316	—	**Symptom:** Some managed devices logged multiple error message, **Trying to obtain mac address**. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	Captive Portal	All platforms	ArubaOS 8.5.0.11
AOS-218208	—	**Symptom:** 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. **Scenario:** This issue was observed in APs running ArubaOS 8.5.0.8 or later versions.	AP-Wireless	All platforms	ArubaOS 8.5.0.8

Table 6: *Resolved Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-218277 AOS-214428	—	**Symptom:** The **auth** process crashed on managed devices. Hence, the Remote APs rebooted and VIA users faced connectivity issues. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.5.0.11 or later versions.	Base OS Security	All platforms	ArubaOS 8.5.0.11
AOS-197323 AOS-212920	—	**Symptom:** The **Dashboard > Infrastructure** page of the WebUI did not display the static channel details assigned to an AP. The fix ensures that the WebUI displays the static channel details assigned to an AP. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.5.0.10 or later versions.	Station Management	All platforms	ArubaOS 8.5.0.10
AOS-208846	—	**Symptom:** 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. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.6.0.4 or later versions.	Base OS Security	All platforms	ArubaOS 8.6.0.4
AOS-217539 AOS-219010 AOS-219952	—	**Symptom:** The **auth** process crashed on managed devices. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.6.0.6 or later versions.	Dot1X	All platforms	ArubaOS 8.6.0.6
AOS-218117 AOS-219179	—	**Symptom:** 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. **Scenario:** This issue was observed in managed devices running ArubaOS 8.6.0.7 or later versions.	Controller-Platform	All platforms	ArubaOS 8.6.0.7
AOS-218167	—	**Symptom:** Users were unable to delete static OSPF aggregate routes. The fix ensures that the users are able to delete static OSPF aggregate routes **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions.	Routing	All platforms	ArubaOS 8.5.0.10

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

We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

Limitations

Following are the limitations observed in this release:

No Support for Zero Touch Provisioning and Multi-version for 9004 Controllers

Zero Touch Provisioning and multi-version for 9004 controllers are currently not supported.

It is recommended to have the Mobility Master and managed device running the same ArubaOS version.

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.

Known Issues

Following are the known issues observed in this release:

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-131325 AOS-146748	159222 179137	**Symptom:** An incorrect number of clients are displayed in the **Dashboard > Overview > Clients >Wireless Clients table > active-standby IP field** page of the WebUI **Scenario:** This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.1.0.0
AOS-145410 AOS-146962	177352 179430	**Symptom:** A managed device crashes and reboots with the error message, **Atleast 2000 MB free flash is recommended to keep system stable. Please clean up your flash file.** **Scenario:** This issue occurs when a managed device receives IP packets larger than one segment. This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.0.2
AOS-145566	177559	**Symptom:** A Mobility Master is unable to forward the traffic that is sourced from an IP interface in the gateway. **Scenario:** This issue occurs when netdestinations are used in the routing ACL rule. This issue is observed in Mobility Masters running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Policy-Based Routing	All platforms	ArubaOS 8.0.1.0
AOS-149413 AOS-196453	183040	**Symptom:** The **Dashboard > Overview > Remote Clients page** of the WebUI does not display any value for **OS** and **Connected to** fields. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
AOS-151022 AOS-188417	185176	**Symptom:** The output of the **show datapath uplink** command displays an incorrect session count. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-151355	185602	**Symptom:** A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Policy-Based Routing	All platforms	ArubaOS 8.0.1.0
AOS-153185	188148	**Symptom:** The **Dashboard > Security > Active rogue > Locate** option does not function in the WebUI. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.1 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.3.0.1
AOS-153742 AOS-194948	188871	**Symptom:** 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)**. **Scenario:** This issue is observed in 7010 controllers running ArubaOS 8.5.0.1 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	Controller-Datapath	7010 controllers	ArubaOS 8.5.0.1
AOS-156068	192100	**Symptom:** The **DDS** process in a managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.2.1.1
AOS-156742 AOS-156977	193031 193319	**Symptom:** A user is unable to make any change to IP Probe configuration, after forwarding a complete configuration using API. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0.1.0
AOS-157492	194064	**Symptom:** VRRP authentication fails in a managed device. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0. **Workaround:** None.	VRRP	All platforms	ArubaOS 8.2.1.0

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157795 AOS-206376	194516	**Symptom:** A few managed devices are unable to process two **APN usb-init** strings using the **uplink cellular apn** command with Huawei E3372 modem. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.3.0.6
AOS-182847	—	**Symptom:** A few users are unable to copy the **WPA Passphrase** field and **High-throughput** profile to a new SSID profile using the **Configuration > System > Profiles > Wireless LAN > SSID > <SSID_ Profile>** option in the WebUI. **Scenario:** 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. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
AOS-183706	—	**Symptom:** The tx radio power of a few APs are lesser than the tx radio power of other APs in the same network. **Scenario:** This issue is observed in APs running ArubaOS 8.3.0.6 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.3.0.6
AOS-184135 AOS-195866	—	**Symptom:** A few users are unable to download applications from Google Play Store. **Scenario:** This issue occurs when the YouTube application is blocked. This issue is observed in stand-alone controllers running ArubaOS 8.4.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.4.0.0
AOS-184947 AOS-192737	—	**Symptom:** The jitter and health score data are missing from the **Dashboard > Infrastructure > Uplink > Health** page in the WebUI. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.4 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.4

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185538 AOS-195334	—	**Symptom:** A high number of EAP-TLS timeouts are observed in a managed device. **Scenario:** 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. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.3.0.8
AOS-186133	—	**Symptom:** A few managed devices display abnormally high multicast traffic in **Performance Summary > All Radios** monitoring page. **Scenario:** This issue is observed in 320 Series access points running ArubaOS 8.3.0.6. **Workaround:** None.	AP-Wireless	320 Series access points	ArubaOS 8.3.0.6
AOS-186774	—	**Symptom:** When the **show memory cfgm** command is executed, a large memory allocation is displayed in the output of the command. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.3.0.6
AOS-187115	—	**Symptom:** The application name is incorrect in the **Configuration > Roles & Policies > Policies > <Policy name>** policy configuration WebUI page. **Scenario:** This issue occurs when the WebUI is accessed for the first time. This issue is observed in Mobility Masters running ArubaOS 8.2.2.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.2.2.0
AOS-187422 AOS-189258	—	**Symptom:** The output of **show log all** and **show audit-trail** commands displays the unencrypted password entered for non-profile commands such as **aaa test-server** command. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running ArubaOS 8.3.0.5 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.3.0.5
AOS-187834	—	**Symptom:** A few APs do not send Port VLAN IDs in an LLDP packet although the **native-vlan-id** parameter is set using the **ap system-profile** command. **Scenario:** This issue is observed in APs running ArubaOS 8.2.2.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.2.2.5

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187911	—	**Symptom:** The **Wireless Clients** section of the **Dashboard > Overview** page in the WebUI displays incorrect client usage values. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0 or later versions. **Workaround:** Add a tooltip over the usage tab to mention that the current client usage value accounts for the last 15 minutes.	WebUI	All platforms	ArubaOS 8.4.0.0
AOS-188285	—	**Symptom:** A mesh portal reboots continuously because the **wpa_hex_key** value exceeds more than 132 bytes string in **the ap mesh-recovery-profile cluster <cluster_id> wpa-hexkey <wpa_hex_key>** command. The log files list the reason for the event as **AP rebooted Tue Jun 11 10:40:01 CDT 2019; Critical process /aruba/bin/meshd [pid 2450] DIED, process marked as RESTART**. **Scenario:** This issue is observed in APs running ArubaOS 8.3.0.7 as a mesh portal. **Workaround:** 1. Modify **mesh-recovery-profile** by using **mesh-recovery-generate** command. 2. Reboot the mesh portal and issue the **setenv mesh_role 0** command on apboot in the console port of the AP. 3. Reprovision the AP to mesh portal.	Mesh	All platforms	ArubaOS 8.3.0.7
AOS-188478	—	**Symptom:** The Remote AP whitelist file does not contain the first MAC address entry. **Scenario:** This issue occurs when the user executes the **show whitelist-db rap export-css <filename>** command to export the Remote AP whitelist file to the controller directory. This issue is observed in stand-alone controllers running ArubaOS 8.3.0.5 or later versions. **Workaround:** None.	Local Database	All platforms	ArubaOS 8.3.0.5
AOS-188972 AOS-194746 AOS-208631 AOS-213627	—	**Symptom:** Mobility Master displays the blacklisted clients although the clients were removed from the managed device. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions in a cluster setup. **Workaround:** None.	DDS	All platforms	ArubaOS 8.4.0.4

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190071 AOS-190372	—	**Symptom:** A few users are unable to access websites when WebCC is enabled on the user role. **Scenario:** 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: 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.	WebCC	7005 controllers	ArubaOS 8.4.0.0
AOS-190240 AOS-192168	—	**Symptom:** The SNMP OIDs provide incorrect result in a cluster setup. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.3.0.0
AOS-191081 AOS-211007	—	**Symptom:** Some iPhones are connected to Wi-Fi but are unable to access the network. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.10 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.5.0.10
AOS-191539	—	**Symptom:** The configuration synchronization fails and **CONFIG Failure** is displayed as the status of synchronization. Also, the log files list the **Error: Tunnel is an L2 GRE Tunnel, Delete the Vlans, before changing the mode." executing "tunnel mode gre 2048** error message. **Scenario:** This issue occurs when the interface tunnel is set as 2048. This issue is observed in managed devices running ArubaOS 8.4.0.0 or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	Interface	All platforms	ArubaOS 8.4.0.1
AOS-192725	—	**Symptom:** The **Dashboard > Overview** page of the WebUI displays incorrect number of users intermittently. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.8 or later versions. **Workaround:** None. **Duplicates:** AOS-188255, AOS-190476, AOS-190946, AOS-193586, AOS-194784, AOS-196004, AOS-200375, and AOS-210787	Monitoring	All platforms	ArubaOS 8.3.0.8

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-192738 AOS-197047	—	**Symptom:** The Mobility Master list in the WebUI incorrectly displays the mac address of the primary Mobility Master for the secondary Mobility Master. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.10 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.3.0.10
AOS-193083	—	**Symptom:** The cluster upgrade fails on a 2-node cluster because the AP platform capacity of the managed device is only 4 and the hash table size is calculated as zero. **Scenario:** This issue is observed in Mobility Controller Virtual Appliances running ArubaOS 8.5.0.0 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.5.0.0
AOS-193184	—	**Symptom:** All L2 connected managed devices in a cluster move to L3 connected state after an upgrade. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.2 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.5.0.2
AOS-193560 AOS-198565 AOS-200262 AOS-204794 AOS-212249 AOS-208110 AOS-209989	—	**Symptom:** The number of APs that are DOWN are incorrectly displayed in the WebUI. However, CLI displays the correct status of APs. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.4 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.4
AOS-193775 AOS-194581 AOS-197372	—	**Symptom:** A mismatch of AP count and client count is observed between the Mobility Master and the managed device. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Monitoring	All platforms	ArubaOS 8.5.0.2

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-193883 AOS-197756	—	**Symptom:** A few APs are unable to use DHCP IPv6 addresses and option 52 for master discovery. **Scenario:** This issue occurs when the APs do not clear the previous LMS entries after an upgrade. This issue is observed in access points running ArubaOS 8.3.0.8 or later versions. **Workaround:** Delete the IPv4 addresses from AP system profile using the command, **ap system-profile** and from high availability profiles using the command, **ha.**	AP Platform	All platforms	ArubaOS 8.3.0.8
AOS-194082 AOS-196092	—	**Symptom:** A few APs crash and reboot unexpectedly. The log files lists the reason for the event as **BadPtr:00000006 PC:wlc_keymgmt_wsec+0x28/0xa4 [wl_v6] Warm-reset.** **Scenario:** This issue is observed in access points running ArubaOS 8.6.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.6.0.0
AOS-194113 AOS-203184 AOS-213027 AOS-213861	—	**Symptom:** Users are unable to perform captive portal authentication when the login URL of the captive portal profile points to ClearPass Policy Manager. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.7 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.5.0.7
AOS-194144 AOS-217873	—	**Symptom:** Some clients are unable to connect to APs. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.10 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.5.0.10
AOS-194370	—	**Symptom:** High memory utilization is observed in the **cluster manager** process of managed devices. **Scenario:** This issue is observed in managed devices running ArubaOS 8.4.0.2 or later versions in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.4.0.2
AOS-194381	—	**Symptom:** Some managed devices lose the route-cache entries and drop the VRRP IP addresses sporadically. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.7

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-194911	—	**Symptom:** An incorrect flag output is displayed for APs configured with 802.1X authentication when the **show ap database** command is executed. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.2 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.5.0.2
AOS-194925 AOS-195413	—	**Symptom:** A branch office controller is unable to failover to a secondary VPNC managed device. **Scenario:** This issue occurs because the secondary VPNC's MAC address is not updated on the running configuration of the controller. This issue is observed in Mobility Master Virtual Appliances and Branch office controllers running ArubaOS 8.5.0.2 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.5.0.2
AOS-194964	—	**Symptom:** A few users are unable to clone the configuration from an existing group to a new group in a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.1 or later versions. **Workaround:** Change the operating mode of the AP from am-mode to ap-mode using the **ap spectrum local-override** command.	Configuration	All platforms	ArubaOS 8.5.0.2
AOS-195089	—	**Symptom:** The DNS traffic is incorrectly getting classified as Thunder and is getting blocked. **Scenario:** This issue occurs when the DNS traffic is blocked and peer-peer ACL is denied for users. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.7
AOS-195100 AOS-198302 AOS-204455 AOS-206735	—	**Symptom:** The health status of a managed device is incorrectly displayed as **Poor** in the **Dashboard > Infrastructure** page of the Mobility Master's WebUI. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.3.0.7

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-195228	—	**Symptom:** The device status is always displayed as inactive when SNMP walk is performed. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.2 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.5.0.2
AOS-195434	—	**Symptom:** An AP crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.0 o or later versions in a Mobility Master-Managed Device topology. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.5.0.2
AOS-195616 AOS-196228 AOS-193980	—	**Symptom:** A few clients lose L3 connectivity though the L2 connectivity is up. **Scenario:** This issue occurs when the client enters power saving mode and the AP queues packets. This issue is observed in 200 Series access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	200 Series access points	ArubaOS 8.3.0.0
AOS-196115	—	**Symptom:** Users are unable to configure untrusted VLAN in the **Configuration > Interfaces > Ports** page of the WebUI. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.0
AOS-196864	—	**Symptom:** Although a new VLAN ID is successfully connected, the managed device displays that the VLAN ID fails with a different ID. **Scenario:** This issue is observed when new VLANs are added and the total number of VLANs are 100/101, 200/201, 300/301 and likewise. This issue is observed in managed devices running ArubaOS 8.5.0.3 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.5.0.3
AOS-196878 AOS-197216	—	**Symptom:** The **Datapath** process crashes on a managed device. The log file lists the reason for the event as **wlan-n09-nc1.gw.illinois.edu.** **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.2 or later versions. **Workaround:** None.	DPI	All platforms	ArubaOS 8.5.0.2

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-197023	—	**Symptom:** Mobility Master sends incorrect AP regulatory-domain-profile channel changes to the managed device during the initial configuration propagation. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions. **Workaround:** Either of the following steps are recommended: ■ In the CLI, execute the **ap regulatory-domain-profile** command to create an AP regulatory-domain-profile without any channel configuration, save the changes, and later add or delete channels as desired. ■ In the WebUI, create an AP regulatory-domain-profile with default channel selected, save the changes, and later add or delete channels as desired in the **Configuration > AP Groups** page.	WebUI	All platforms	ArubaOS 8.5.0.4
AOS-197210	—	**Symptom:** WebUI takes a long time to display data. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.5.0.3 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.3
AOS-197497	—	**Symptom:** AirMatch selects the same channel for two neighboring APs even after radar detection. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.3 or later versions. **Workaround:** None.	AirMatch	All platforms	ArubaOS 8.5.0.3
AOS-198281	—	**Symptom:** The details of the **Up** time in **Managed network > Dashboard > Access Points > Access Points** table does not get updated correctly. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.2.2.6 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.2.2.6
AOS-198483	—	**Symptom:** WebUI does not have an option to map the **rf dot11-60GHz-radio-profile** to an AP group. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.5.0.4 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.4

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-198787 AOS-198929	—	**Symptom:** A Remote AP does not come up on a managed device when Verizon U730L modem is used. **Scenario:** This issue is observed in managed devices running ArubaOS 8.6.0.0 or later versions. **Workaround:** None.	Remote AP	All platforms	ArubaOS 8.6.0.0
AOS-198849 AOS-198850	—	**Symptom:** Users are unable to configure 2.4 GHz radio profile in the **Configuration > System > Profiles > 2.4 GHz radio profile** page and the WebUI displays the error message, **Feature is not enabled in the license.** **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.3 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.3
AOS-200765	—	**Symptom:** Managed devices log the error message, **<199804> <4844> |authmgr| |cluster| gsm_auth.c, auth_gsm_publish_ip_user_local_section:1011: auth_gsm_publish_ip_user_local_section: ip_user_local_flags.** **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions in a cluster setup. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.3.0.7
AOS-201166 AOS-207939 AOS-209042	—	**Symptom:** A controller crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot cause: Nanny rebooted machine - httpd_wrap process died (Intent:cause:register 34:86:0:2c)**. **Scenario:** This issue occurs after a restart of the **HTTPD** process. This issue is observed in stand-alone controllers running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Web Server	All platforms	ArubaOS 8.2.0.0
AOS-201200	—	**Symptom:** The **show license-pool-profile** command does not display the output when executed in the **/mm/my node** hierarchy. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.6 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.5.0.5

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-201240	—	**Symptom:** When a trusted VLAN is added using the **Interface > Ports > Allowed VLANs** page, the Mobility Master automatically issues the **no trusted vlan** command. **Scenario:** This issue occurs when trunk mode is initially configured using the CLI and later modified using the WebUI. This issue is observed in managed devices running ArubaOS 8.5.0.2 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.2
AOS-201376		**Symptom:** The measured power, **Meas. Pow** column in the **show ap debug ble-table** command does not get updated when the Tx power of an AP is changed. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.6 or later versions. **Workaround:** None.	IoT	All platforms	ArubaOS 8.5.0.6
AOS-201439 AOS-201448	—	**Symptom:** Some APs crash and reboot unexpectedly. The log file lists the reason for the event as **PC is at skb_panic+0x5c/0x68**. **Scenario:** This issue is observed in AP-303H access points running ArubaOS 8.5.0.5 or later versions. **Workaround:** None.	AP-Wireless	AP-303H access points	ArubaOS 8.5.0.5
AOS-202034 AOS-205799 AOS-207736 AOS-208473	—	**Symptom:** The **STM** process in a managed device crashes unexpectedly, due to which few APs are unable to connect to the managed device. **Scenario:** This issue is observed in managed devices running ArubaOS 8.6.0.0 or later versions. **Workaround:** Disable **dual-5ghz-mode** parameter in the **ap system-profile** command.	Station Management	All platforms	ArubaOS 8.6.0.0
AOS-202129 AOS-204127	—	**Symptom:** The **Configuration > AP groups** page does not have the **Split radio** toggle to enable the tri-radio feature. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.6.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.6.0.0

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-202247 AOS-218834	—	**Symptom:** Some APs crash and reboot unexpectedly. The log file lists the reason for the event as **Reboot Reason: Reboot caused by kernel panic: Fatal exception.** **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.10 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.5.0.10
AOS-203097	—	**Symptom:** The WebUI prompts that additional VLANs will be deleted when a user tries to delete a VLAN. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.3.0.10 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.3.0.10
AOS-203170	—	**Symptom:** The class attribute field is missing in the accounting packets of the VIA connection profile. **Scenario:** This issue occurs when IKEv2 is enabled in the VIA connection profile. This issue is observed in managed devices running ArubaOS 8.4.0.1 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.6.0.2
AOS-203201	—	**Symptom:** The managed device is unable to download configurations from the Mobility Master using VPNC. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.2.6 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.2.6
AOS-203336	—	**Symptom:** The **Dashboard > Infrastructure > Access Points** page of the WebUI and the **show log** command display different values for the last AP reboot time. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.5 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.5
AOS-204187	—	**Symptom:** The command **vpn-peer peer-mac** does not support Suite-B cryptography for custom certificates. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.2.2.8 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.2.2.8

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-204195	—	**Symptom:** Beacon failure rates are high on 2.4 Ghz radio and hence, clients are unable to find the ESSIDs. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.8 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.5.0.8
AOS-204241	—	**Symptom:** Some managed devices log spurious DHCP DBUG messages. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.8 or later versions. **Workaround:** None.	DHCP	All platforms	ArubaOS 8.5.0.8
AOS-204414	—	**Symptom:** The VLAN range configured using the **ntp-standlaone vlan-range** command are not correctly sent to the managed devices. **Scenario:** This issue occurs when the user repeatedly modifies the VLAN range. This issue occurs in Mobility Masters running ArubaOS 8.0.1.0 or later versions. **Workaround:** Delete the VLAN range configured on the Mobility Master and re-configure the **ntp-standlaone vlan-range.**	Configuration	All platforms	ArubaOS 8.0.1.0
AOS-205010	—	**Symptom:** The **OFA** process in a managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.8 or later versions. **Workaround:** None.	SDN-Platform	All platforms	ArubaOS 8.5.0.8
AOS-205190	—	**Symptom:** The **auth** process in a managed device crashes unexpectedly. **Scenario:** This issue occurs when openflow is used to add or delete ACLs. This issue is observed in managed devices running ArubaOS 8.3.0.7 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.3.0.7
AOS-205634 AOS-212820	—	**Symptom:** The WebUI does not display the port channel membership. **Scenario:** This issue occurs when port members are added to the PC-0 port channel. This issue is observed in managed devices running ArubaOS 8.6.0.4. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.6.0.4

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-205869	—	**Symptom:** Users are unable to delete ACLs and the error message, **Invalid data: FW CP ACL not found** is displayed. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.12 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.3.0.12
AOS-206541	—	**Symptom:** The **Maintenance > Software Management** page does not display the list of all managed devices that are part of a cluster. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.5.0.8 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.8
AOS-206752	—	**Symptom:** The console log of 7205 controllers displays the **ofald| |sdn| ERRS ofconn_rx:476 <10.50.1.26:6633> socket read failed, err:Resource temporarily unavailable(11)** message. **Scenario:** This issue is observed in 7205 controllers running ArubaOS 8.5.0.9 or later versions **Workaround:** None.	SDN-Platform	7205 controllers	ArubaOS 8.5.0.9
AOS-206795	—	**Symptom:** A user is unable to rename a node from the Mobility Master node hierarchy. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.7 or later versions. **Workaround:** Restart **profmgr** process to rename the node.	Configuration	All platforms	ArubaOS 8.3.0.7
AOS-206902 AOS-208241	—	**Symptom:** AirGroup users are unable to connect to Sonos speakers. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.9 or later versions. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.5.0.9
AOS-206907	—	**Symptom:** A few APs crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: assert**. **Scenario:** This issue is observed in AP-303H access points running ArubaOS 8.5.0.5 or later versions. **Workaround:** None.	AP Datapath	AP-303H access points	ArubaOS 8.5.0.5

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-207011	—	**Symptom:** A few APs crash and reboot unexpectedly. The log file lists the reason for the event as **kernel panic: TARGET ASSERT DUE TO MORE THAN 5 RECOVERY.** **Scenario:** This issue is observed in AP-325 access points running ArubaOS 8.5.0.5 or later versions. **Workaround:** None.	AP-Wireless	AP-325 access points	ArubaOS 8.5.0.5
AOS-207114 AOS-208226	—	**Symptom:** Mesh point APs reboot when jumbo frames are enabled on the network. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.5.0.9 or later versions. **Workaround:** None.	Mesh	All platforms	ArubaOS 8.5.0.9
AOS-207245	—	**Symptom:** Some managed devices crash and reboot unexpectedly. The log file lists the reason for the event as **Hardware Watchdog Reset (Intent:cause:register 53:86:0:802c).** **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.8 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.5.0.8
AOS-207337	—	**Symptom:** After upgrading from ArubaOS 8.2.x.x to ArubaOS 8.5.0.0-FIPS or later versions, a few managed devices are stuck in the **LAST SNAPSHOT** state. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.5.0.9
AOS-207366	—	**Symptom:** The **show advanced options** menu is not available in the **Configuration > Access Points > Campus APs** page of the WebUI. **Scenario:** This issue occurs when more than one AP is selected. This issue is observed in Mobility Masters running ArubaOS 8.3.0.13. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.3.0.13

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-207691	—	**Symptom:** CLI displays incorrect IP address for a TACACS server. **Scenario:** This issue occurs when the **configuration purge-pending-config** command is executed on group nodes. This issue is observed in managed devices running ArubaOS 8.3.0.8 or later versions. **Workaround:** Restart the **profmgr** process by issuing the **process restart profmgr** command for CLI to display the correct IP address.	CLI	All platforms	ArubaOS 8.3.0.8
AOS-208553	—	**Symptom:** The **Test** button in **Diagnostics > Tools > AAA Server Test** is grayed out for read-only users. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.9 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.9
AOS-208857	—	**Symptom:** Some managed devices crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: USB disconnect.** **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.6 or later versions. **Workaround:** None.	Controller Platform	All platforms	ArubaOS 8.3.0.6
AOS-208953	—	**Symptom:** The ipsec-map list configured at the device level does not get migrated after an upgrade. **Scenario:** This issue occurs when users upgrade the network from ArubaOS 8.2.2.x to ArubaOS 8.5.0.13 version. **Workaround:** It is recommended to move the ipsec-map list configuration from device level to group level before upgrade.	IPsec	All platforms	ArubaOS 8.5.0.13
AOS-209276	—	**Symptom:** The **show datapath crypto counters** command displays the same output parameter, **AESCCM Decryption Invalid Replay Co** twice. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.5.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.5.0.0
AOS-209977	—	**Symptom:** SNMP query with an incorrect string fails to record the offending IP address. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.5.0.10

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-210482	—	**Symptom:** Some managed devices display the error message, **Invalid set request while configuring ESSID for a Beacon Report Request profile**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.6 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.3.0.6
AOS-211720	—	**Symptom:** The **STM** process crashes on managed devices and hence, APs failover to another cluster. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.5 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.5.0.5
AOS-212255	—	**Symptom:** Some APs are stuck in **Not in Progress** state during cluster live upgrade. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.10 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.5.0.10
AOS-213011	—	**Symptom:** Packet loss is observed for clients during a cluster failover. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.5.0.10
AOS-213558	—	**Symptom:** Users are unable to add a new node to an existing cluster of eight nodes. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.6 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.5.0.6
AOS-214963	—	**Symptom:** Some APs detect false radar. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.11 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.5.0.11

Table 7: *Known Issues in ArubaOS 8.5.0.13*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-214977	—	**Symptom:** Memory leak is observed in **arci-cli-helper** process. **Scenario:** This issue occurs while running an API script. This issue is observed in APs running ArubaOS 8.5.0.8 or later versions. **Workaround:** None.	Web Server	All platforms	ArubaOS 8.5.0.8
AOS-215303	—	**Symptom:** Users are unable to view file names in the **Diagnostic > Technical Support > Copy Files** page of the WebUI. **Scenario:** This issue occurs when **Flash file system** is selected as the source file. This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions. **Workaround:** None.	Controller Platform	All platforms	ArubaOS 8.5.0.11
AOS-216766	—	**Symptom:** Some APs generate sapd coredump. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.11 or later versions. **Workaround:** None.	Air Management-IDS	All platforms	ArubaOS 8.5.0.11
AOS-216874	—	**Symptom:** The virtual MAC address of the VLAN gets deleted from the bridge table and hence, results in network outage. **Scenario:** This issue is observed in managed devices running ArubaOS 8.5.0.11 or later versions. **Workaround:** None.	VLAN	All platforms	ArubaOS 8.5.0.11
AOS-218012	—	**Symptom:** The **Maintenance** tab of the WebUI displays a list of clusters that are not configured for that particular node. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.5.0.9 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.5.0.9
AOS-218404 AOS-212330	—	**Symptom:** APs are unable to ping a few clients. **Scenario:** This issue is observed in APs running ArubaOS 8.5.0.11 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.5.0.11

This chapter details software upgrade procedures. It is recommend 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 and Best Practices

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** section of 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 the 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 *Aruba Mobility Master Licensing Guide*.

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. 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 51 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 51 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 file:** 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 51 to copy the **logs.tar** files to an external server. Execute the **tar clean logs** command to delete the file from the managed device.

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

Deleting a File

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

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Logs
- Flashbackup

Backing up and Restoring Flash Memory

You can backup and restore flash using the WebUI or the 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 Compact Flash file system, 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 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 backup flash file from the external server or storage device to the compact flash file system 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 compact flash file system.

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 50.

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

In the WebUI

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

1. Download the ArubaOS image from the customer support site.
2. Upload the new software image to a PC or workstation on your network.
3. Validate the SHA hash for 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** from the **Upgrade using** drop-down list.
   b. Click **Browse** from **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 ArubaOS image from the customer support site.
2. Open an SSH session to your Mobility Master.
3. Execute the **ping** command to verify the network connection between the Mobility Master and the SCP server, FTP server, or TFTP server.

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

   or

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

   or

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

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

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Master.

```
(host)# reload
```

Verifying the ArubaOS Upgrade

Verify the upgrade using the WebUI or CLI.

In the WebUI

Log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the ArubaOS image version.

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

1. Log in to the WebUI to verify if all the managed devices are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Memory Requirements on page 50 for information on creating a backup.

In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.

4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 51 for information on creating a backup.

Downgrading ArubaOS

The 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 the 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 51.
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved ArubaOS configuration file.
4. Set the Mobility Master or managed device to boot from the system partition that contains the pre-upgrade ArubaOS version.

   When you specify a boot partition or copy an image file to a system partition, Mobility Master or managed device checks if the ArubaOS version is compatible with the configuration file. An error message is displayed if the boot parameters are incompatible with the ArubaOS version and configuration files.
5. After switching the boot partition, perform the following steps:
   - Restore pre-upgrade flash backup from the file stored on the Mobility Master or managed device. Do not restore the ArubaOS flash backup file.
   - Do not import the WMS database.
   - If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded ArubaOS version.
   - If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From the **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 the **Select destination file** drop-down list, enter a file name (other than default.cfg).
   c. Click **Copy**.

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

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

   a. Enter the FTP or TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The Mobility Master or 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 section describes how to downgrade the ArubaOS version.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:
   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```
   or
   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the controller to boot with your pre-upgrade configuration file.
   ```
   (host) # boot config-file <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your pre-upgrade ArubaOS version is stored. You cannot load a new image into the active system partition (the default boot).
   ```
   #show image version
   ```
4. Set the backup system partition as the new boot partition.
   ```
   (host) # boot system partition 1
   ```
5. Reboot the Mobility Master or 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 Technical Support:

- The status of installation (new or existing), and any recent network 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 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.