

# ArubaOS 8.3.0.4



Release Notes

## **Copyright Information**

© Copyright 2020 Hewlett Packard Enterprise Development LP.

## **Open Source Code**

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

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

---

<b>Contents</b> .....	<b>3</b>
Revision History .....	5
<b>Release Overview</b> .....	<b>6</b>
Related Documents .....	6
Supported Browsers .....	7
Contacting Support .....	7
<b>New Features and Enhancements</b> .....	<b>8</b>
<b>Supported Platforms</b> .....	<b>10</b>
Mobility Controller Platforms .....	10
AP Platforms .....	10
Virtual Platforms .....	12
<b>Regulatory Updates</b> .....	<b>13</b>
<b>Resolved Issues</b> .....	<b>14</b>
<b>Known Issues and Limitations</b> .....	<b>31</b>
<b>Upgrade Procedure</b> .....	<b>42</b>
Important Points to Remember .....	42
Memory Requirements .....	43

---

Backing up Critical Data .....	44
Upgrading ArubaOS .....	45
Downgrading ArubaOS .....	48
Before Calling Technical Support .....	50

## Revision History

The following table provides the revision history of this document.

**Table 1:** *Revision History*

Revision	Change Description
Revision 05	<ul style="list-style-type: none"><li>Removed <b>Migration Guide</b> from the documents listed under <b>Related Documents</b> section as the Migration Tool is no longer supported.</li><li>Removed the <b>Migrating from ArubaOS 6.x to ArubaOS 8.x</b> section from <b>Upgrade Procedure</b> chapter as the Migration Tool is no longer supported.</li></ul>
Revision 04	Removed bug 189970 from the <b>Known Issues</b> section.
Revision 03	Added a feature enhancement regarding, <b>Reauthenticate Wired User on VLAN Change</b> .
Revision 02	Added bug 181143 and 193777.
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.

---

- [New Features and Enhancements on page 8](#)
- [Supported Platforms on page 10](#)
- [Regulatory Updates on page 13](#)
- [Resolved Issues on page 14](#)
- [Known Issues and Limitations on page 31](#)
- [Upgrade Procedure on page 42](#)

For the list of terms, refer [Glossary](#).

## Related Documents

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

- [ArubaOS Getting Started Guide](#)
- [ArubaOS User Guide](#)
- [ArubaOS CLI Reference Guide](#)
- [ArubaOS API Guide](#)
- [Aruba Mobility Master Licensing Guide](#)
- [Aruba Virtual Appliance Installation Guide](#)
- [Aruba Mobility Master Hardware Appliance Installation Guide](#)

## Supported Browsers

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

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

## Contacting Support

**Table 2:** *Contact Information*

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

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

## Base OS Security

### CP Firewall Limit

ArubaOS 8.3.0.4 now increases the limit of CP firewall rules from 32 to 96. You can now configure up to 96 firewall CP rules. A **Max CP firewall limit (96) reached configuration** error message is displayed when the maximum limit of 96 rules is reached.

### Reauthenticate Wired User on VLAN Change

Starting from ArubaOS 8.3.0.4, when a wired user moves across VLANs, a trigger is created to re-authenticate this user. To support this feature, a new parameter, **reauth-wired-user-vlan-change** is added in the **aaa profile** command.

To enable reauth-wired-user-vlan-change, perform the following steps:

#### In the CLI

```
(host) [mynode] (config) #aaa profile test  
(host) [mynode] (AAA Profile "test") #reauth-wired-user-vlan-change
```

#### In the WebUI

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Authentication > AAA Profiles** tab.
2. From the **AAA Profiles** list, select **Wireless LAN > AAA**.
3. To edit an existing AAA profile, select the AAA profile you want to edit. To create a new AAA profile, click + and enter a name for the new **AAA profile** in the Profile name field.
4. Configure the **AAA profile** parameter described in the table below.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.



**Table 3:** AAA Profile Parameters

Parameter	Description
<b>Reauthenticate wired user on VLAN change</b>	When a wired user moves across VLANs, a trigger is created to reauthenticate this user.

### SSH Server and Client Update

Starting from ArubaOS 8.3.0.4, OpenSSH v7.7 is supported.

This chapter describes the hardware platforms supported in this release.

### Mobility Controller Platforms

The following table displays the controller platforms that are supported in this release.

**Table 4:** *Supported Controller Platforms in ArubaOS 8.3.0.4*

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

### AP Platforms

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

**Table 5:** *Supported AP Platforms in ArubaOS 8.3.0.4*

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

**Table 5: Supported AP Platforms in ArubaOS 8.3.0.4**

AP Family	AP Model
200 Series	AP-204, AP-205
203H Series	AP-203H
205H Series	AP-205H
207 Series	AP-207
203R Series	AP-203R, AP-203RP
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303 Series	AP-303
303H Series	AP-303H
310 Series	AP-314, AP-315
318 Series	AP-318
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377

**Table 5:** Supported AP Platforms in ArubaOS 8.3.0.4

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

## Virtual Platforms

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

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

The following list displays the Mobility Controller Virtual Appliance platforms that are supported in this release.

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

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

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

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

The following DRT file version is part of this release:

- DRT-1.0\_67494

This chapter describes the issues resolved in this release.

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155936 180912 182485	<p><b>Symptom:</b> A managed device failed to respond to the PPP LCP echo request messages from a PPPoE server. Hence, the PPPoE link was not usable. The fix ensures that the managed device successfully respond to the PPP LCP echo request messages from a PPPoE server.</p> <p><b>Scenario:</b> This issue occurred when the value of PPPoE session ID was greater than 1492. This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.</p>	PPPoE	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.4
165804	<p><b>Symptom:</b> A HTTP security header was not detected on ports 8080 or 8088 in a managed device. This issue is resolved by enabling the HTTP security header in the <b>httpd</b> configuration file.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.</p>	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
165908 170224	<p><b>Symptom:</b> The <b>kernel</b> process in a Mobility Master crashed and the Mobility Master rebooted unexpectedly. The log file listed the reason for the event as <b>control processor kernel panic</b>. The fix ensures that the Mobility Master works as expected.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running ArubaOS 8.3.0.0.</p> <p>Duplicates: 171074, 171396, 173372, 174322, 174370, 174917, 175009, 177151, 177457, 177662, 178307, 180558, 180741, 181173, 183588, 185596, 186993, 187232, and 187418</p>	Controller-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
166880 188708	<p><b>Symptom:</b> Configuration failed on managed devices when the logging server was removed. The fix ensures that the configuration does not fail on managed devices.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.0.1.0 or later versions.</p>	Logging	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171594	<p><b>Symptom:</b> High volume of the error message, <b>Could not create/find bandwidth-contract for user</b> displayed in the log messages. The fix ensures that the error message is displayed only when the bandwidth-contract allocation fails.</p> <p><b>Scenario:</b> This issue occurred when the bandwidth-contract configured. This issue was observed in 340 Series access points running ArubaOS 8.3.0.0 or later versions.</p>	Base OS Security	340 Series access points	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
172326 187496 190679	<p><b>Symptom:</b> The <b>datapath</b> process crashed on a Mobility Master. The fix ensures that the <b>datapath</b> process works as expected.</p> <p><b>Scenario:</b> This issue occurred when the global WAN policy rule was re-applied with the same WAN policy. This issue was observed in Mobility Masters running ArubaOS 8.1.0.0 or later versions.</p>	Controller-Datapath	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.3.0.4
175550	<p><b>Symptom:</b> User could not disable the security logging for the <b>aaa</b> process using the <b>logging security process aaa subcat aaa level debugging</b> command. The fix ensures that the user is able to disable the security logging.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.</p>	Configuration	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.4
175669	<p><b>Symptom:</b> The <b>show ap active</b> command did not show any flag for an AP that was operating in restricted mode because of POE-AF. This issue is resolved by showing the <b>p</b> flag in the <b>show ap active</b> command for an AP that operates in restricted mode.</p> <p><b>Scenario:</b> This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.</p>	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4
175717 178608	<p><b>Symptom:</b> A managed device rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Master Initiated Reboot (Intent:cause:register 59:86:50:2)</b>.The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue occurred when a managed device was deleted and re-added in the hierarchy. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.</p>	AP-Platform	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176952	<p><b>Symptom:</b> Malicious users could create symbolic links in the directory to access the internal file system. The fix ensures that the unauthenticated users are unable to access the internal file system.</p> <p><b>Scenario:</b> This issue occurred when custom captive portal pages were uploaded to the directory. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.</p>	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
177002	<p><b>Symptom:</b> The <b>Cannot Delete Default user admin</b> error message was displayed when users executed the <b>no mgmt-user admin</b> command to remove the admin account. The issue was resolved by not allowing the users to create admin account on <b>/mm</b> node of both Mobility Master and stand-alone Mobility Master.</p> <p><b>Scenario:</b> The issue occurred when the users tried to delete the admin account from the <b>/mm</b> or <b>/mm/mynode</b> levels. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.</p>	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4
177509	<p><b>Symptom:</b> User was unable to ping the servers from a managed device. The fix ensures that the user is able to ping the servers from the managed device.</p> <p><b>Scenario:</b> This issue occurred when the managed device obtained configuration after a reload. This issue was observed in managed devices running ArubaOS 8.0.1.0 or later versions.</p>	Controller-Datapath	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.3.0.4
177618	<p><b>Symptom:</b> The <b>sapd</b> process crashed in an AP. This issue is resolved by not sending nodelist, radio, and VAP configuration to an AP whose name matches another AP that already exists in the managed device. Aruba recommends to not add an AP with a name that matches the name of another AP that already exists in the managed device.</p> <p><b>Scenario:</b> this issue occurred when a user added an AP with a name that matched the name of an AP that already existed in the managed device. This issue was observed in access points running ArubaOS 8.2.0.2.</p>	AP-Platform	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.4



**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177770	<p><b>Symptom:</b> APs crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>Kernel panic - not syncing: FW ASSERT at_tx_send_setup_ppdu_params</b>. Enhancements to the wireless driver resolved the issue.</p> <p><b>Scenario:</b> This issue occurred when an ADDBA response was received with a window size of 0 as some of the retried frames were not flushed from the frame queue. This issue was observed in 330 Series access points running ArubaOS 8.2.0.2 or later versions.</p>	AP-Wireless	330 Series access points	ArubaOS 8.2.0.2	ArubaOS 8.3.0.4
178329	<p><b>Symptom:</b> The <b>show ap active</b> command displayed incorrect 5 GHz channel information. Enhancements to the wireless driver resolved this issue.</p> <p><b>Scenario:</b> This issue occurred when an AP detected a radar within the 10 seconds interval between a lost connection and a WiFi shutdown. After the connection was re-established, the AP displayed a different channel in the <b>show ap active</b> command output. This issue was observed in 200 Series access points running ArubaOS 8.0.0.0 or later versions.</p>	AP-Wireless	200 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4
178351	<p><b>Symptom:</b> A specified GigabitEthernet interface in a managed device did not support maximum transmit rate in kilobits per second. The fix ensures that the maximum transmit rate settings also support kilobits per second.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p>	Controller-Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
178405	<p><b>Symptom:</b> The <b>show ap active</b> command displayed incorrect 5 GHz channel information. Enhancements to the wireless driver resolved this issue.</p> <p><b>Scenario:</b> This issue was observed in 100 Series access points running ArubaOS 8.0.0.0 or later versions.</p>	AP-Wireless	100 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4
178707 187686	<p><b>Symptom:</b> The <b>authorization</b> process of a managed device crashed during an AP port bounce. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p>	Base OS Security	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178719 179348 180890 186926	<p><b>Symptom:</b> A managed device rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Hardware Watchdog Reset (Intent:cause:register ee:ee:50:4)</b>. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p>	Controller-Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
178764 183584	<p><b>Symptom:</b> The <b>Syslogd</b> process in an AP crashed and generated core files frequently. The fix ensures that the crash does not occur.</p> <p><b>Scenario:</b> This issue was observed in 300 Series, 310 Series, 303 Series, 318 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points running ArubaOS 8.2.1.1 or later versions.</p>	AP-Platform	300 Series, 310 Series, 303 Series, 318 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
178783	<p><b>Symptom:</b> A managed device rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)</b>. The fix ensures that the IPv4 and IPv6 netdestination stats are indexed differently.</p> <p><b>Scenario:</b> This issue occurred because IPv4 and IPv6 netdestination stats were not indexed differently. This issue is observed in managed devices running ArubaOS 8.2.1.0.</p>	Controller-Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
178824 180650	<p><b>Symptom:</b> A client that was connected to an AP displayed low signal strength. The fix ensures that the correct signal strength is displayed.</p> <p><b>Scenario:</b> This issue occurred when a client associated with the G radio of the AP. This issue was observed in AP-207 access points running ArubaOS 8.2.0.0 or later versions.</p>	AP-Platform	AP-207 access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
179151	<p><b>Symptom:</b> Image Upgrade from ArubaOS 8.2.0.2 to ArubaOS 8.2.1.0 version failed. The fix ensures that the image upgrade is successful.</p> <p><b>Scenario:</b> This issue occurred when there was no home directory created for the account. This issue was observed in ArubaOS 8.2.1.0 or later versions.</p>	Upgrade	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179267	<p><b>Symptom:</b> The WebUI showed the <b>Invalid MAC address</b> error in the <b>Managed Network &gt; Configuration &gt; Access Points &gt; Whitelist</b> page when a MAC address was added. The fix ensures that the : (colon) character is automatically inserted when a MAC address is added.</p> <p><b>Scenario:</b> This issue occurred when a MAC address did not include the : (colon) character. This issue was observed in managed devices running ArubaOS 8.3.0.0.</p>	WebUI	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
179415	<p><b>Symptom:</b> The traffic between a managed device and the connected switch was forwarded to the next-hop list, instead of getting locally bridged to the VLAN. The fix ensures that the traffic is forwarded to the correct VLAN.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.1.0.4 or later versions.</p>	Controller-Datapath	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.3.0.4
179485	<p><b>Symptom:</b> <b>Profmgr</b> process crashed in a Mobility Master when <b>configuration purge-pending-config</b> command was executed. The fix ensures that the <b>Profmgr</b> process does not crash.</p> <p><b>Scenario:</b> This issue occurred when a <b>delete</b> command was in pending state and the user executed <b>configuration purge-pending-config</b> command to revert the configuration instead of using <b>write memory</b> command. This issue was observed in Mobility Master running ArubaOS 8.2.1.0 or later versions.</p>	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
179942	<p><b>Symptom:</b> A client was unable to send or receive traffic to or from an AP when 802.11r compatibility was enabled. The fix ensures that the client can successfully send or receive traffic to or from an AP.</p> <p><b>Scenario:</b> This issue occurred when an 802.11r capable station used 802.11r procedures and then reassociated without using this feature. This issue was observed in Mobility Master running ArubaOS 8.2.1.0.</p>	Station Management	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
180525 189738	<p><b>Symptom:</b> The error message <b>w10:PHYTX</b> error or <b>w11:PHYTX</b> error is displayed in the error logs when dual-5ghz-mode was changed from disabled to enabled. The fix ensures that the beacon is correctly sent after enabling the dual-5ghz-mode.</p> <p><b>Scenario:</b> This issue occurred in APs powered by a POE-AF switch which did not update the beacon correctly after enabling the dual-5ghz-mode. This issue occurred in 340 Series access points running ArubaOS 8.3.0.0 or later versions.</p>	AP-Wireless	340 Series access points	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
180865 182174 186333 190362	<p><b>Symptom:</b> A mismatch of AP count was observed between the Mobility Master and the managed device. The fix ensures that the correct AP count is displayed in the WebUI.</p> <p><b>Scenario:</b> This issue occurred because some APs were missing in the monitoring server table though the APs were available in the AP database table. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.</p>	Monitoring	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
181143	<p><b>Symptom:</b> The same product key was generated when the Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was cloned. This issue is resolved by generating the product key based on the UUID of the system.</p> <p><b>NOTE:</b> If a cloned Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance that runs any version lower than ArubaOS 8.2.2.0 was upgraded to ArubaOS 8.2.2.0 and higher, ArubaOS 8.3.0.2 and higher, or ArubaOS 8.4.0.0 and higher, in the respective releases, the serial number and passphrase were changed and all licenses associated with the older serial number were invalidated. Migrate or regenerate the existing licenses for the new serial number after the upgrade. Contact Aruba Technical Support before the upgrade.</p> <p><b>Scenario:</b> This issue occurred when an OVA-based Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was deployed, an OVF template was exported, and the exported OVF template was deployed. This issue was observed in Mobility Controller Virtual Appliance or Mobility Master Virtual Appliance running ArubaOS 8.2.0.0.</p>	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181221 187011	<b>Symptom:</b> Clients were unable to connect to the managed device. The fix ensures that the clients are able to connect to the managed device. <b>Scenario:</b> This issue occurred when <b>enforce-dhcp parameter</b> in <b>aaa profile</b> command was enabled and route IP table buffer overflowed. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
181355	<b>Symptom:</b> The <b>mDNS</b> process crashed on a managed device. The fix ensures that the managed devices work as expected. <b>Scenario:</b> This issue occurred because the hash table used to store MAC address is corrupt due to a race condition. This issue was observed in managed devices running ArubaOS 8.3.0.0.	AirGroup	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
181401	<b>Symptom:</b> A mesh AP came up with <b>ML</b> (unlicensed) flags. The fix ensures that the mesh AP works as expected. <b>Scenario:</b> This issue occurred after a VRRP failover. This issue was observed in APs running ArubaOS 8.0.0.0 as a mesh portal.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4
181418 183863	<b>Symptom:</b> The <b>ISAKMPD</b> process in a managed device crashed and the managed device rebooted unexpectedly. The fix ensures that the managed device works as expected. <b>Scenario:</b> This issue occurred because of memory corruption. This issue was observed in 7240 managed devices running ArubaOS 8.0.0.0 or later versions.	IPsec	7240 managed devices	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4
181553	<b>Symptom:</b> A managed device crashed when the AP was downloading a build image. The fix ensures that the managed device does not crash. <b>Scenario:</b> This issue was observed in managed devices connected to AP-325 access points that downloaded the ArubaOS 8.3.0.0 build image. This issue is not restricted to a managed device or AP model.	Controller-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
181564	<b>Symptom:</b> A Remote AP lost the gateway ARP after using Split-Tunnel mode VAP. Enhancements to the wireless driver resolved this issue. <b>Scenario:</b> This issue occurred when the Remote AP missed caching the ARP data for a specific gateway. This issue was observed in Remote APs running ArubaOS 8.0.0.0 or later versions.	Remote AP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181615	<p><b>Symptom:</b> Mobility Masters lost licenses if the Mobility Master was unplugged within 3 hours of adding the license and there were no configuration changes made on the Mobility Master. The fix ensures that the database is backed up every time the write memory command is executed.</p> <p><b>Scenario:</b> This issue occurred because the database backup was not triggered when the write memory command was not executed. This issue is not limited to any specific platform or ArubaOS version.</p>	Configuration	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
181678	<p><b>Symptom:</b> Same License key was displayed multiple times on a managed device when the <b>show license</b> command was executed. The fix ensures that the correct license count is displayed.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p>	Licensing	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
181721 178075	<p><b>Symptom:</b> Download speeds were less than normal. The fix ensures that higher download speeds are achieved even in noisy conditions.</p> <p><b>Scenario:</b> This issue occurred in extremely noisy environments on 2.4 GHz channels. This issue was observed in 300 Series access points connected to a 7010 controller.</p>	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.4
181729	<p><b>Symptom:</b> The <b>show running-config</b> command did not list an ACL although the <b>show configuration effective</b> command listed the same ACL. The fix ensures that the <b>show running-config</b> command lists the ACL.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.1.</p>	Base OS Security	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
181773	<p><b>Symptom:</b> Managed devices rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)</b>. The fix ensures that the managed devices work as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p>	Controller-Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182054	<p><b>Symptom:</b> An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as <b>Reboot caused by kernel panic: Out of memory</b>. Enhancements to the AP wireless driver resolved the issue.</p> <p><b>Scenario:</b> This issue occurred due to a memory corruption. This issue was observed in AP-335 access points running ArubaOS 8.2.1.1.</p>	AP-Wireless	AP-335 access points	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
182342 183735	<p><b>Symptom:</b> An AP transmitted an over the air frame on all scan channels that included all regulatory domain channels, rare channels, and DFS channels. Enhancements to the wireless driver resolved the issue.</p> <p><b>Scenario:</b> This issue was observed in 300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points running ArubaOS 8.2.0.0 or later versions.</p>	AP-Wireless	300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
182486	<p><b>Symptom:</b> A client was not able to access the Internet. The fix ensures that the client is able to access the Internet.</p> <p><b>Scenario:</b> This issue occurred when the PPPoE interface included the <b>ip nat outside</b> configuration. This issue was observed in managed devices running ArubaOS 8.2.1.0.</p>	VLAN	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
182612 182372	<p><b>Symptom:</b> Client were unable to resolve ARP requests. The fix ensures that the clients are able to resolve ARP requests.</p> <p><b>Scenario:</b> This issue occurred because the AP memory utilization rate was high, leading to drop in client traffic. This issue was observed in access points running ArubaOS 8.3.0.0.</p>	AP Datapath	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
182654 188378	<p><b>Symptom:</b> Mobility Controller Virtual Appliance crashed unexpectedly and the log files for the event listed the reason as <b>Datapath</b> crash. The fix ensures that the Mobility Controller Virtual Appliance works as expected.</p> <p><b>Scenario:</b> This issue occurred because an IPv6 ACL for application was configured. This issue was observed in Mobility Controller Virtual Appliance running ArubaOS 8.2.1.0 or later versions.</p>	DPI	Mobility Controller Virtual Appliance	ArubaOS 8.3.0.2	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182941	<p><b>Symptom:</b> The <b>Configuration &gt; Interfaces &gt; Ports</b> page in the WebUI displayed the <b>Expecting string of length 1 to 32</b> error message in the <b>Allowed VLANs</b> field. The issue is resolved by increasing the string length of the trusted VLAN to 255 characters.</p> <p><b>Scenario:</b> This issue occurred when the trunk allowed VLAN was added from the WebUI, which resulted in marking the same VLAN as trusted VLAN. But, the VLAN word size limit for trusted VLAN is 32 and not 255. This issue was observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions.</p>	VLAN	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
183134	<p><b>Symptom:</b> The <b>profmgr</b> process crashed multiple times. The fix ensures that the Mobility Master Virtual Appliance works as expected</p> <p><b>Scenario:</b> This issue occurred when SSID is defined on one node and Virtual APs or the AP groups were defined on lower nodes. This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.3.0.0.</p>	AP-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
183464 190191	<p><b>Symptom:</b> The output of the <b>show ap debug radio-stats</b> and <b>show ap radio-summary</b> commands displayed incorrect values of <b>Current Noise Floor, WiFi Utilization, and Interference</b> parameters. The fix ensures that the command output displays the correct values.</p> <p><b>Scenario:</b> This issue was observed in 200 Series access points running ArubaOS 8.2.0.0 or later versions.</p>	AP-Wireless	200 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
183615 180496 180615 185103 185484 185485 186458 186990 188060	<p><b>Symptom:</b> AirGroup lost all the learned server and user details and also failed to learn any new user or server. The fix ensures that AirGroup learns all users and servers appropriately.</p> <p><b>Scenario:</b> This issue occurred when AirGroup was enabled in centralized mode. This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.</p>	AirGroup	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
184082 184587	<p><b>Symptom:</b> Some APs failed to switch between Backup LMS IP and LMS IP. The fix ensures that the APs switch between Backup LMS IP and LMS IP successfully.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.</p>	AP-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4



**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
184426	<p><b>Symptom:</b> Clients connected to the APs were getting deauthenticated. Enhancements to the wireless driver resolved the issue.</p> <p><b>Scenario:</b> This issue was observed in 300 Series, AP-303H, 310 Series, 320 Series, 330 Series, and 360 Series access points running ArubaOS 8.2.1.0 or later versions.</p>	AP-Wireless	300 Series, AP-303H, 310 Series, 320 Series, 330 Series, and 360 Series access points	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
184868	<p><b>Symptom:</b> The SNMP query for <b>OID: wlsxSysExtInternalTemperature</b> was displaying 0 for a Mobility Master. The fix ensures that the query displays the actual temperature.</p> <p><b>Scenario:</b> This issue was observed in 7200 controllers running ArubaOS 8.2.1.1.</p>	SNMP	7200 controllers	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
185082	<p><b>Symptom:</b> The output of the <b>show lc-cluster group-profile &lt;profile_name&gt;</b> command did not display the active AP load balancing information. The fix ensures that the active AP load balancing information is displayed when the <b>show lc-cluster group-profile &lt;profile_name&gt;</b> command is executed.</p> <p><b>Scenario:</b> This issue was observed in managed devices in a cluster setup running ArubaOS 8.2.1.1 or later versions.</p>	Cluster-Manager	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
185420	<p><b>Symptom:</b> The <b>isakmpd</b> process crashed and rebooted on the Mobility Master Hardware Appliance. The fix ensures that the Mobility Master Hardware Appliance works as expected.</p> <p><b>Scenario:</b> This issue was observed in a Mobility Master Hardware Appliance running ArubaOS 8.2.1.1 or later versions.</p>	IPsec	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
185876 188023	<p><b>Symptom:</b> Managed devices dropped ARP packets for all the VRRP MAC address on the cluster. The fix ensures that the ARP packets are not dropped.</p> <p><b>Scenario:</b> This issue occurred because session synchronization for some high value sessions from Active UAC to Standby UAC caused session table corruption, which led to the drop in ARP packets. This issue was observed in managed devices running ArubaOS 8.2.2.0.</p>	Controller-Datapath	All platforms	ArubaOS 8.2.2.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
186110	<p><b>Symptom:</b> The configuration synchronization failed and the status of the synchronization displayed <b>CONFIG Failure</b>. This issue is resolved by changing the user-role <b>default-iap-user-role</b> as a read only role.</p> <p><b>Scenario:</b> This issue occurred when the <b>default-iap-user-role</b> was edited. This issue was observed in Mobility Masters running ArubaOS 8.3.0.1 or later versions.</p>	Base OS Security	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.3.0.4
186220 186764	<p><b>Symptom:</b> The AirGroup flows were not installed when AirGroup was enabled or the AirGroup process was restarted. Similarly, the AirGroup flows were not removed when AirGroup was disabled or <b>no airgroupprofile activate</b> command was executed. The fix ensures that the AirGroup flows work as expected.</p> <p><b>Scenario:</b> This issue occurred in the following scenarios:</p> <ul style="list-style-type: none"> <li>■ When the <b>profmgr</b> process sent the wrong AirGroup profile name during AirGroup activation or a race condition between a parent node without an AirGroup profile.</li> <li>■ When a child node with an AirGroup profile deleted the AirGroup flows at the child node during the AirGroup process restart.</li> </ul> <p>This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.</p>	AirGroup	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
186399	<p><b>Symptom:</b> Clients were steered to the same radio due to load balancing by ClientMatch even though the BSSID of the radio and the AP were same. The fix ensures that the clients are not steered to the same radio by ClientMatch.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.1.</p>	ARM	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
186410	<p><b>Symptom:</b> Wired AirGroup servers failed to update the cache entries automatically. This issue was resolved by increasing the queue size to reduce packet loss from queue overflow.</p> <p><b>Scenario:</b> This issue occurred when the packet-in dispatcher queue was overrun. This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.</p>	SDN	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
186418	<p><b>Symptom:</b> <b>mDNS</b> process crashed on a Mobility Master frequently. The fix ensures that the Mobility Master works as expected.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.</p>	AirGroup	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
186509	<p><b>Symptom:</b> A client failed dynamic WEP reauthentication with an AP. This issue is resolved by not dropping the unencrypted Rx EAPOL frames when dynamic WEP reauthentication is enabled.</p> <p><b>Scenario:</b> This issue occurred when the wireless driver dropped unencrypted Rx EAPOL frames after the WEP key was set. This issue was observed in AP-305, AP-315, and AP-335 access points running ArubaOS 8.3.0.2 and operated in bridge mode.</p>	AP-Wireless	AP-305, AP-315, and AP-335 access points	ArubaOS 8.3.0.2	ArubaOS 8.3.0.4
186815	<p><b>Symptom:</b> The CPPM profile entries were not updated in the node hierarchies when the CPPM profile was configured in AirGroup server. The fix ensures that the CPPM profile entries are updated in different node hierarchies.</p> <p><b>Scenario:</b> This issue occurred when the user added or deleted RFC 3576 servers by executing the <code>airgroupprofile cppm rfc-3576-server &lt;rfc-3576-server&gt;</code> command. This issue was observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.</p>	AirGroup	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
187364	<p><b>Symptom:</b> The configuration changes made to the system-defined <code>validuser</code> ACL rules were not applied on reboot of a managed device. The fix ensures that the configuration changes in the ACL rule are applied instead of the default ACL rules.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.</p>	Base OS Security	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
187696	<p><b>Symptom:</b> A Mobility Master failed to install the correct netdestination into datapath causing guest captive portal to fail. The fix ensures that the Mobility Master installs the correct netdestination and sends netdestination updates to datapath.</p> <p><b>Scenario:</b> This issue occurred when the Mobility Master did not receive netdestinations when there were PAPI failures. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.</p>	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4
187762 191491	<p><b>Symptom:</b> The SSID was broadcasting only in 5 GHz radios. The fix ensures that the SSID is broadcasting also in 2.4 GHz radios.</p> <p><b>Scenario:</b> This issue occurred when the dual-mode was set to <b>Auto</b>. This issue was observed in 340 Series access points running ArubaOS 8.3.0.1 or later versions.</p>	AirMatch	340 Series access points	ArubaOS 8.3.0.1	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
187819 188349	<p><b>Symptom:</b> An AP crashed and rebooted unexpectedly. The log files listed the reason for the reboot as <b>Reboot caused by kernel panic: Watchdog timeout received</b>. The fix ensures that the AP works as expected.</p> <p><b>Scenario:</b> This issue occurred due to a large number of debug messages printed in the log files. This issue was observed in AP-335 access points running ArubaOS 8.2.1.1 or later versions.</p>	AP-Wireless	AP-335 access points	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
188037	<p><b>Symptom:</b> Mesh APs were coming up unlicensed on a Data zone. The fix ensures that for a mesh AP in a MultiZone, no licenses are consumed in Data zone but in a Primary zone, the mesh APs consume licenses even if there are no Virtual APs for that mesh AP.</p> <p><b>Scenario:</b> This issue occurred when MultiZone is enabled and a virtual AP is assigned to the Data zone. This issue was observed in APs connected to managed devices running ArubaOS 8.2.1.1 or later versions in Mesh mode.</p>	AP-Platform	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.3.0.4
188130	<p><b>Symptom:</b> AP crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>kernel panic: softlockup: hung tasks</b>. The fix ensures that only 32 packets are processed in one batch.</p> <p><b>Scenario:</b> This issue occurred because the firewall processed too many packets in one batch. This issue was observed in AP-303H access points running ArubaOS 8.3.0.1 or later versions.</p>	AP Datapath	AP-303H access points	ArubaOS 8.3.0.1	ArubaOS 8.3.0.4
188135 188987	<p><b>Symptom:</b> The <b>STM</b> process in a managed device displayed the <b>the Dynamic BSS tunnel could not be setup for bssid</b> error message. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running ArubaOS 8.2.2.0 or later versions.</p>	AP-Platform	All platforms	ArubaOS 8.2.2.0	ArubaOS 8.3.0.4
188517	<p><b>Symptom:</b> Multiple APs crashed unexpectedly. The fix ensures that the APs work as expected.</p> <p><b>Scenario:</b> This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.</p>	AP-Wireless	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
189035 189956 189981	<p><b>Symptom:</b> Users were unable to connect to AirGroup servers intermittently. The fix ensures that the users are able to connect to AirGroup servers.</p> <p><b>Scenario:</b> This issue occurred when the CPPM queries sent from the clients did not reach the AirGroup servers. This issue was observed in Mobility Master Hardware Appliances running ArubaOS 8.2.1.0 in a master-standby topology.</p>	AirGroup	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.4
189064	<p><b>Symptom:</b> Jabber desktop sharing caused unwanted traffic to reach a Mobility Master. Withdrawing the support for Jabber desktop sharing resolved this issue.</p> <p><b>Scenario:</b> This issue occurred because of the wide range of ports being used by Jabber. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.</p>	UCC	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.4
189353	<p><b>Symptom:</b> The output of the <b>show ap arm client-match neighbors ap-name &lt;ap-name&gt;</b> command displayed large amount of data. The fix ensures that the <b>show ap arm client-match neighbors ap-name &lt;ap-name&gt;</b> command displays only the necessary data.</p> <p><b>Scenario:</b> This issue was observed in AP-335 access points running ArubaOS 8.2.0.0 or later versions.</p>	ARM	AP-335 access points	ArubaOS 8.2.0.0	ArubaOS 8.3.0.4

**Table 6:** Resolved Issues in ArubaOS 8.3.0.4

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
189486 189904 190298	<p><b>Symptom:</b> A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b>. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue occurred in a cluster setup when an IPv6 client initiated and stopped multiple FTP transfers. This issue was observed in 7200 Series controllers running ArubaOS 8.3.0.2 or later versions.</p>	Controller-Datapath	7200 Series controllers	ArubaOS 8.3.0.2	ArubaOS 8.3.0.4
189539	<p><b>Symptom:</b> The <b>mDNS</b> process on the Mobility Master utilized a memory space that is equal to or greater than the assigned value. The issue was resolved by clearing the memory and internal data structures of the <b>mDNS</b> packets.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running ArubaOS 8.2.2.1 or later versions in a master-standby topology.</p>	AirGroup	All platforms	ArubaOS 8.2.2.1	ArubaOS 8.3.0.4
189722	<p><b>Symptom:</b> Configuration failure was observed on a Mobility Master in standby mode. The fix ensures that all configurations are applied to the standby Mobility Master.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running ArubaOS 8.2.2.1 or later versions.</p>	Logging	All platforms	ArubaOS 8.2.2.1	ArubaOS 8.3.0.4

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

### Known Issues

Following are the known issues observed in this release.

**Table 7:** *Known Issues in ArubaOS 8.3.0.4*

Bug ID	Description	Component	Platform	Reported Version
168180	<p><b>Symptom:</b> The <b>profmgr</b> process in a managed device crashes when a single instance default profile is modified in the disaster recovery mode.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.0.1.0
162623	<p><b>Symptom:</b> The output of the <b>show ap arm history ap-name &lt;ap-name&gt;</b> command does not display the radar detection event for an AP.</p> <p><b>Scenario:</b> This issue is observed in AP-203H access points running ArubaOS 8.2.0.0.</p> <p><b>Workaround:</b> None.</p>	ARM	AP-203H access points	ArubaOS 8.2.0.0
168636	<p><b>Symptom:</b> A client is unable to connect to a controller from Aruba Central using SSH.</p> <p><b>Scenario:</b> This issue is observed in 7005 controllers running ArubaOS 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Aruba Central	7005 controllers	ArubaOS 8.0.1.0
172217	<p><b>Symptom:</b> Write memory does not show configurations committed.</p> <p><b>Scenario:</b> This issue occurs when a user configures ACLs, VLANs, and interface configuration and executes the <b>write memory</b> command. This issue is observed in managed devices running ArubaOS 8.2.0.1.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.2.0.1

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
172360	<p><b>Symptom:</b> The output of the <b>show lldp neighbor</b> command displays only the first entry from the lldp neighbors table.</p> <p><b>Scenario:</b> This issue occurs as the other neighbor entries are overwritten. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	SNMP	All platforms	ArubaOS 8.3.0.0
172857 178662	<p><b>Symptom:</b> The <b>BOCMGR</b> process in a Mobility Master crashes unexpectedly.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Controller-Platform	All platforms	ArubaOS 8.3.0.0
175138	<p><b>Symptom:</b> The <b>Configurations &gt; Services &gt; Guest provisioning</b> page appears blank and non-editable.</p> <p><b>Scenario:</b> This issue occurs when user enters <b>&amp;</b> character in the email fields and submits the changes. This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	Guest Provisioning	All platforms	ArubaOS 8.2.0.2
176330 177428	<p><b>Symptom:</b> The <b>Diagnostics &gt; Technical Support &gt; Copy Files</b> page of the WebUI displays a success message although the TFTP file transfer fails.</p> <p><b>Scenario:</b> This issue occurs when a user attempts to copy a file using TFTP. This issue is observed in Mobility Master running ArubaOS 8.2.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.2.0.0
177044 186119	<p><b>Symptom:</b> AP-103H crashes and reboots unexpectedly. The log files for the event listed the reason as <b>Reboot caused by out of memory</b>.</p> <p><b>Scenario:</b> This issue occurs as the AP has low memory. This issue is observed in AP-103H access points running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Platform	AP-103H access points	ArubaOS 8.3.0.0
177204	<p><b>Symptom:</b> The following streaming API and the CLI command on a managed device returns a value of 0 for Minimum RTT: The <b>stats_ip_probe_uplink</b> streaming API The <b>show ip health-check verbose</b> CLI command</p> <p><b>Scenario:</b> This issue occurs in managed devices with <b>Uplink Health-check</b> configuration enabled. This issue is observed in 7000 Series and 7200 Series controllers running ArubaOS 8.0.1.0.</p> <p><b>Workaround:</b> None.</p>	Controller-Datapath	7000 Series and 7200 Series controllers	ArubaOS 8.0.1.0



**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
177800	<p><b>Symptom:</b> Aruba Central agent debugging logs contain the hash value for the certificate sign challenge.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Logging	All platforms	ArubaOS 8.0.1.0
178173 185322	<p><b>Symptom:</b> The log file of a Mobility Master Virtual Appliance displays the <b>OID not increasing</b> SNMP error message.</p> <p><b>Scenario:</b> This issue is observed in a Mobility Master Virtual Appliance running ArubaOS 8.2.0.2.</p> <p><b>Workaround:</b> None.</p>	SNMP	Mobility Master Virtual Appliance	ArubaOS 8.2.0.2
178419 180044 181059	<p><b>Symptom:</b> The mDNS radius requests are sent with the NAS-IP address in reverse order to the ClearPass Policy Manager.</p> <p><b>Scenario:</b> This issue occurs because of wrong endianness. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions.</p>	AirGroup	All platforms	ArubaOS 8.3.0.0
178676 183015	<p><b>Symptom:</b> APs crash randomly and the clients fail to authenticate to an AP.</p> <p><b>Scenario:</b> This issue is observed in 330 Series access points running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Platform	330 Series access points	ArubaOS 8.3.0.0
178707 187686	<p><b>Symptom:</b> The <b>authorization</b> process of a managed device crashes during an AP port bounce.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Base OS Security	All platforms	ArubaOS 8.2.1.0
178709	<p><b>Symptom:</b> The <b>Ipsec-map name</b> drop-down list does not display the system-generated IPsec map in the WebUI.</p> <p><b>Scenario:</b> This issue occurs when the user creates a new policy rule in the <b>Configuration &gt; Roles &amp; Policies &gt; Policies &gt; &lt;policy_name&gt; &gt; &lt;new_policy_rule&gt;</b> page, and selects <b>Forward to ipsec-map</b> option from the <b>Action</b> drop-down list in the WebUI. This issue is observed in Mobility Masters running ArubaOS 8.2.1.0.</p> <p><b>Workaround:</b> None.</p>	WebUI	All platforms	ArubaOS 8.2.1.0

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
178760 179949 179950	<p><b>Symptom:</b> Instant APs connecting to a managed device is obtaining reversed IP address.</p> <p><b>Scenario:</b> This issue occurs when a MAC address of an Instant AP is configured with a remote-ip address in whitelist-db. This issue is observed in Mobility Controller Virtual Appliance running ArubaOS 8.3.0.0.</p> <p><b>Workaround:</b> None.</p>	CPsec	All platforms	ArubaOS 8.3.0.0
178936 179171	<p><b>Symptom:</b> The <b>General Information &gt; Networking</b> page in a Virtual Mobility Controller does not display the information about DNS server and IP address.</p> <p><b>Scenario:</b> This issue is observed in a Mobility Master Virtual Appliance running ArubaOS 8.3.0.0.</p> <p><b>Workaround:</b> None.</p>	Controller-Platform	All platforms	ArubaOS 8.3.0.0
179107	<p><b>Symptom:</b> A stand-alone controller displays the error message <b>Module licensemgr is busy. Please try later</b> while adding licenses.</p> <p><b>Scenario:</b> This issue is observed in stand-alone controllers running ArubaOS 8.1.0.4 or later versions in a master - local topology.</p> <p><b>Workaround:</b> None.</p>	Licensing	All platforms	ArubaOS 8.1.0.4
179347	<p><b>Symptom:</b> The default node does not change its path when the group name is changed.</p> <p><b>Scenario:</b> This issue is observed in Mobility Master Virtual Appliance running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.3.0.0
180349	<p><b>Symptom:</b> The user is not able to disable the <b>prohibit ip-spoofing</b> using the <b>Configuration &gt; Services &gt; Firewall &gt; Prohibit IP spoofing</b> check box in the WebUI.</p> <p><b>Scenario:</b> This issue was observed in a managed devices running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Controller-Datapath	All platforms	ArubaOS 8.3.0.0
180489	<p><b>Symptom:</b> CLI-based upgrade of a stand-alone controller fails with the <b>Timed out, Try again</b> error message.</p> <p><b>Scenario:</b> This issue occurs in a slow network connection when the <b>copy scp</b> command fails to download the ArubaOS image after 15 minutes. This issue is observed in stand-alone controllers running ArubaOS 8.2.1.0.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.2.1.0

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
181322	<p><b>Symptom:</b> Stand-alone controller is displayed as a Mobility Master in the WebUI.</p> <p><b>Scenario:</b> This issue is observed in stand-alone controllers running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.3.0.0
181773	<p><b>Symptom:</b> Managed devices reboot unexpectedly. The log file lists the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)</b>.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Controller-Datapath	All platforms	ArubaOS 8.2.1.0
182073	<p><b>Symptom:</b> An AP crashes and reboots unexpectedly. The log file lists the reason for the event as <b>Kernel panic - not syncing: Rebooting the AP because of FW ASSERT: rcRateFind+229; ratectrl_11ac.c:2394</b>.</p> <p><b>Scenario:</b> This issue is observed in AP-315 access points running ArubaOS 8.2.1.0.</p> <p><b>Workaround:</b> None.</p>	AP-Wireless	AP-315 access points	ArubaOS 8.2.1.0
182352	<p><b>Symptom:</b> An AP does not take the EIRP settings from the radio profile and broadcasts with High EIRP.</p> <p><b>Scenario:</b> This issue is observed in access points running ArubaOS 8.2.1.1.</p> <p><b>Workaround:</b> None.</p>	AirMatch	All platforms	ArubaOS 8.2.1.1
182486	<p><b>Symptom:</b> A client is not able to access the internet.</p> <p><b>Scenario:</b> This issue occurs when the PPPoE interface includes the <b>ip nat outside</b> configuration. This issue is observed in managed devices running ArubaOS 8.2.1.0.</p> <p><b>Workaround:</b> None.</p>	VLAN	All platforms	ArubaOS 8.2.1.0
183034	<p><b>Symptom:</b> Clients get disconnected after roaming although auto connect is enabled.</p> <p><b>Scenario:</b> This issue is observed in access points running ArubaOS 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Platform	All platforms	ArubaOS 8.2.1.1

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
183246	<p><b>Symptom:</b> Managed devices could get converted to master node automatically when a power outage occurs while a configuration change is received from the Mobility Master.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.0.1.0
184626 187077	<p><b>Symptom:</b> Mobility Master loses the user name and password for ssh mgmt-auth configuration.</p> <p><b>Scenario:</b> This issue occurs when the Mobility Master is rebooted and when the user executes <b>no ssh mgmt-auth username/password</b> command. This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Authentication	All platforms	ArubaOS 8.3.0.0
184786	<p><b>Symptom:</b> APs are not broadcasting on Virtual APs and on start up, display D flag after managed devices are rebooted in a cluster.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions in a cluster setup.</p> <p><b>Workaround:</b> Ensure the VLAN name binding on <b>virtual-ap</b> profile is same as the name of named VLAN.</p>	AP-Platform	All platforms	ArubaOS 8.2.0.2
184972	<p><b>Symptom:</b> IP OSPF message-digest key gets erased.</p> <p><b>Scenario:</b> This issue occurs when the managed device enters or returns from the disaster recovery mode. This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.2.1.1
185309	<p><b>Symptom:</b> Clients connected to AP-345 access points are unable to go online.</p> <p><b>Scenario:</b> This issue occurs when the clients are connected through bridge mode SSID. This issue is observed in AP-345 access points running ArubaOS 8.3.0.0.</p> <p><b>Workaround:</b> None.</p>	AP-Wireless	AP-345 access points	ArubaOS 8.3.0.0
185403 178564	<p><b>Symptom:</b> A Mobility Master Virtual Appliance crashes unexpectedly due to a memory corruption.</p> <p><b>Scenario:</b> This issue is observed in a Mobility Master Virtual Appliance running ArubaOS 8.1.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Logging	All platforms	ArubaOS 8.1.0.0

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
185420	<p><b>Symptom:</b> The <b>isakmpd</b> process crashes and reboots on the Mobility Master Hardware Appliance.</p> <p><b>Scenario:</b> This issue is observed in a Mobility Master Hardware Appliance running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	IPsec	All platforms	ArubaOS 8.2.1.1
185506	<p><b>Symptom:</b> A managed device is unable to synchronize its AP whitelist on Mobility Master with the Activate whitelist database.</p> <p><b>Scenario:</b> This issue occurs when the managed device is unable to contact the Mobility Master to establish IPsec tunnels. This issue is observed in managed devices running ArubaOS 8.0.1.0.</p> <p><b>Workaround:</b> None.</p>	Controller-Platform	All platforms	ArubaOS 8.0.1.0
185508	<p><b>Symptom:</b> When new licenses are added, the <b>Configuration &gt; System &gt; Licenses</b> WebUI page is unable to load.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running ArubaOS 8.3.0.1.</p> <p><b>Workaround:</b> None.</p>	Licensing	All platforms	ArubaOS 8.3.0.1
185602	<p><b>Symptom:</b> Managed devices are unable to pass traffic to the VPNC next hop.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Policy-Based Routing	All platforms	ArubaOS 8.0.1.0
186018	<p><b>Symptom:</b> Mobility Master sends a large number of authorization requests to the ClearPass Policy Manager for the AirGroup users.</p> <p><b>Scenario:</b> This issue occurs as the IPv6 addresses are aging out. This issue is observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	SDN	All platforms	ArubaOS 8.2.1.1
186110	<p><b>Symptom:</b> The configuration synchronization fails and the status of the synchronization displays <b>CONFIG Failure</b>.</p> <p><b>Scenario:</b> This issue occurs when the <b>default-iap-user-role</b> is edited. This issue is observed in Mobility Masters running ArubaOS 8.3.0.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	Base OS Security	All platforms	ArubaOS 8.3.0.1

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
186146	<p><b>Symptom:</b> The output of the <b>show ap debug port status ap-name &lt;ap-name&gt;</b> command displays the status of <b>PortFast</b> parameter as <b>unknown</b>.</p> <p><b>Scenario:</b> This issue is observed in AP-303H access points running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Platform	AP-303H access points	ArubaOS 8.2.1.1
186418	<p><b>Symptom:</b> <b>mDNS</b> process crashes on a Mobility Master frequently.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	AirGroup	All platforms	ArubaOS 8.2.1.1
186605 184774 185405	<p><b>Symptom:</b> A managed device fails to establish IPsec tunnel on its primary uplink.</p> <p><b>Scenario:</b> This issue occurs because the socket descriptor slots are not reused when the IP address is flapped in the <b>isakmpd</b> process. This issue is observed in managed devices running ArubaOS 8.0.1.0.</p> <p><b>Workaround:</b> None.</p>	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
186608	<p><b>Symptom:</b> The <b>datapath</b> process in a managed device crashes while initiating a Skype call from a wireless client.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.3.0.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	Controller-Datapath	All platforms	ArubaOS 8.3.0.1
186815	<p><b>Symptom:</b> The CPPM profile entries are not updated in the node hierarchies when the CPPM profile is configured in AirGroup server.</p> <p><b>Scenario:</b> This issue occurs when the user adds or deletes RFC 3576 servers by executing the <b>airgroupprofile cppm rfc-3576-server &lt;rfc-3576-server&gt;</b> command. This issue is observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	AirGroup	All platforms	ArubaOS 8.2.1.1
187027	<p><b>Symptom:</b> A user is unable to import a CSV file on a stand-alone controller.</p> <p><b>Scenario:</b> This issue is observed in a stand-alone controller running ArubaOS 8.3.0.1.</p> <p><b>Workaround:</b> None.</p>	Guest Provisioning	All platforms	ArubaOS 8.3.0.1

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
187191	<p><b>Symptom:</b> Mobility Master is unable to learn the wireless key host as an openflow host.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	SDN	All platforms	ArubaOS 8.2.1.1
187205	<p><b>Symptom:</b> Unable to bulk provision Remote AP to Campus AP using <b>Configuration &gt; Access &gt; Provisioning Rules</b> page of the WebUI.</p> <p><b>Scenario:</b> This issue is observed in AP-303H access points running ArubaOS 8.3.0.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	WebUI	AP-303H access points	ArubaOS 8.3.0.2
187364	<p><b>Symptom:</b> The configuration changes made to the system-defined <b>validuser</b> ACL rules are not applied on reboot of a managed device.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	Base OS Security	All platforms	ArubaOS 8.2.1.1
187390	<p><b>Symptom:</b> VoIP clients face connectivity issues when IPv6 is enabled.</p> <p><b>Scenario:</b> This issue occurs when UCC flows are processed using the IPv6 address instead of the IPv4 address of the managed device in an IPv6 cluster. This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	UCC	All platforms	ArubaOS 8.2.1.1
187735	<p><b>Symptom:</b> The configured MTU value of an AP is incorrect in the managed device.</p> <p><b>Scenario:</b> This issue occurs when the AP is rebooted after configuring the SAP MTU in the AP system-profile. This issue is observed in access points running ArubaOS 8.1.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Mesh	All platforms	ArubaOS 8.1.0.0
187744 189352	<p><b>Symptom:</b> APs are rebooting randomly. The log files for the event listed the reason as <b>Reboot caused by kernel panic: Fatal exception</b>.</p> <p><b>Scenario:</b> This issue is observed in APs running ArubaOS 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP Regulatory	All platforms	ArubaOS 8.3.0.0

**Table 7: Known Issues in ArubaOS 8.3.0.4**

Bug ID	Description	Component	Platform	Reported Version
187745	<p><b>Symptom:</b> AP requests for less Poe-at power in the LLDP negotiation, which leads to insufficient power.</p> <p><b>Scenario:</b> This issue occurs when the AP requested for 20.8W. This issue is observed in AP-318 and 370 Series access points running ArubaOS 8.3.0.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Wireless	AP-318 and 370 Series access points	ArubaOS 8.3.0.2
188135 188987	<p><b>Symptom:</b> The <b>STM</b> process in a managed device displays the <b>the Dynamic BSS tunnel could not be setup for bssid</b> error message.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.2.2.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Platform	All platforms	ArubaOS 8.2.2.0
188497	<p><b>Symptom:</b> A 7240 controller sends <b>RSSI AMON</b> messages even though the location is disabled in the management server profile.</p> <p><b>Scenario:</b> This issue is observed in 7240 controllers running ArubaOS 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	AMON	7240 controllers	ArubaOS 8.2.1.1
188601	<p><b>Symptom:</b> Managed Devices are unable to synchronize the configuration due to a system-generated ACL.</p> <p><b>Scenario:</b> This issue is observed in managed devices running ArubaOS 8.2.1.0.</p> <p><b>Workaround:</b> None.</p>	Base OS Security	All platforms	ArubaOS 8.2.1.0
189270	<p><b>Symptom:</b> An attribute, <b>Filter-ID</b> that assigns VLANs to the users is missing from a managed device even though the attribute is available in the device configuration settings.</p> <p><b>Scenario:</b> This issue is observed in managed devices in a cluster setup running ArubaOS 8.2.1.1.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	ArubaOS 8.2.1.1
189523	<p><b>Symptom:</b> APs randomly go offline on a 4-node cluster and the IPsec traffic is stalled until the AP reboots.</p> <p><b>Scenario:</b> This issue occurs when CPsec is enabled. This issue is observed in managed devices in a cluster setup running ArubaOS 8.0.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Platform	All platforms	ArubaOS 8.3.0.2



**Table 7:** *Known Issues in ArubaOS 8.3.0.4*

Bug ID	Description	Component	Platform	Reported Version
189795	<p><b>Symptom:</b> Mesh point fails to come up after the mesh portal is rebooted.</p> <p><b>Scenario:</b> This issue occurs when the Mobility Master fails to setup a mesh link. This issue is observed in Mobility Masters running ArubaOS 8.3.0.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	Mesh	All platforms	ArubaOS 8.3.0.2
184849	<p><b>Symptom:</b> Clients are unable to make or receive calls, and are getting a <b>Network busy</b> error message.</p> <p><b>Scenario:</b> This issue occurs when WMM is disabled on the managed device. This issue is observed in AP-315 access points running ArubaOS 8.2.1.1.</p> <p><b>Workaround:</b> None.</p>	WMM	AP-315 access points	ArubaOS 8.2.1.1
193777	<p><b>Symptom:</b> The <b>authentication</b> process crashes when the managed device is upgraded from ArubaOS 8.2.1.1 to ArubaOS 8.3.0.4.</p> <p><b>Scenario:</b> When the system configuration contains netdestination aliases and they are included in ACLs as an ACE entry, the aliases are expanded as hit entries. This issue is observed when the number of hit entries exceed the maximum limit of 8K (maximum of 8192), post which the new hit entries are not accepted and the system is vulnerable to <b>authentication</b> process crash. This issue is observed in managed devices running ArubaOS 8.3.0.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	Base OS Security	All platforms	ArubaOS 8.3.0.1

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



CAUTION

---

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

---

Topics in this chapter include:

- [Important Points to Remember on page 42](#)
- [Memory Requirements on page 43](#)
- [Backing up Critical Data on page 44](#)
- [Upgrading ArubaOS on page 45](#)
- [Downgrading ArubaOS on page 48](#)
- [Before Calling Technical Support on page 50](#)

## Important Points to Remember

To upgrade your Mobility Master or managed device:

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

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

## Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log files, crash data, or flash backups from your managed device to a desired location. Deleted the following files to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 44](#) 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 44](#) to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 44](#) to copy the **logs.tar** file to an external server. Execute the **tar clean logs** command to delete the file from the managed device.



---

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

---

## Deleting a File

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

### In the WebUI

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

## In the CLI

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

## Backing up Critical Data

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

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

## Backing up and Restoring Flash Memory

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

### In the WebUI

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

1. In the Mobility Master node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the flash memory to the **flashbackup.tar.gz** file.
3. Click **Copy Backup** to copy the file to an external server.  
You can copy the backup file from the external server to the flash memory using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the flash memory, navigate to the **Maintenance > Configuration Management > Restore** page and click **Restore**.

### In the CLI

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

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

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

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

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

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

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

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

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

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

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

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

## Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.



CAUTION

---

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see [Memory Requirements on page 43](#).

---



NOTE

---

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

---

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

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



NOTE

---

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

---

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

1. Log in to the vSphere client.

2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
  3. Click **Edit Virtual machine settings**.
  4. From the **Hardware** tab, select and remove a network adapter that is not active.
- Before upgrading to ArubaOS 8.3.0.0 from ArubaOS 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a Mobility Master Virtual Appliance or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
    1. From the **Managed Network** node hierarchy, select the managed device.
    2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
    3. Click **Submit** and click **Continue** in the reload popup.
    4. Click **Pending Changes**.
    5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

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

```
(host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
```

- Before upgrading to ArubaOS 8.3.0.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

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

## In the WebUI

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

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




---

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

---

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

- b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. Disable the same, if you do not want to reboot immediately.



---

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

---

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

## In the CLI

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

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

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

or

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

or

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

```
(host) #show image version
```
5. Execute the **copy** command to load the new image to the non-boot partition.  

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

or

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

or

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

or

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

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

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

7. Reboot the Mobility Master.

```
(host)# reload
```

## Verifying the ArubaOS Upgrade

Verify the upgrade using the WebUI or CLI.

### In the WebUI

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

1. Log in to the WebUI to verify if all the managed devices are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See [Backing up Critical Data on page 44](#) for information on creating a backup.

### In the CLI

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

1. Log in to the CLI to verify that all your managed devices are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 44](#) for information on creating a backup.

## Downgrading ArubaOS

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



## Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see [Backing up Critical Data on page 44](#).
2. Verify that the control plane security is disabled.
3. Set the Mobility Master or managed device to boot with the previously saved configuration file.
4. Set the Mobility Master or managed device to boot from the system partition that contains the pre-upgrade ArubaOS version.

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

5. After switching the boot partition, perform the following steps:
  - Restore pre-upgrade flash backup from the file stored on the Mobility Master or the managed device. Do not restore the ArubaOS flash backup file.
  - Do not import the WMS database.
  - If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded ArubaOS version.
  - If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

## In the WebUI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP or TFTP server, copy the file to the Mobility Master or the managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
  - a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
  - b. From **Select destination file** drop-down list, enter a file name (other than default.cfg).
  - c. Click **Copy**.
2. Determine the partition on which your pre-upgrade ArubaOS version is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If a pre-upgrade ArubaOS version is not stored on your system partition, load it into the backup system partition by performing the following steps:



---

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

---

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

- b. Select the backup system partition.
  - c. Enable **Reboot controller after upgrade**.
  - d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The Mobility Master or the managed device reboots after the countdown period.
  4. When the boot process is complete, verify that the Mobility Master or the managed device is using the correct ArubaOS version by navigating to the **Maintenance > Software Management > About** page.

## In the CLI

The following steps describe how to downgrade the ArubaOS version:

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

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

or

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

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

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

3. Execute the **show image version** command to view the partition on which your pre-upgrade ArubaOS version is stored. You cannot load a new image into the active system partition (the default boot).

```
#show image version
```

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

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

5. Reboot the Mobility Master or the managed device.

```
(host) # reload
```

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

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

## Before Calling Technical Support

Provide the following information when you call Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with the IP addresses and Interface numbers.

- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information.