ArubaOS 8.3.0.1

aruba
a Hewlett Packard
Enterprise company

Release Notes

Open Source Code

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

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

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 05	■ Removed **Migration Guide** from the documents listed under **Related Documents** section as the Migration Tool is no longer supported. ■ Removed the **Migrating from ArubaOS 6.x to ArubaOS 8.x** section from **Upgrade Procedure** chapter as the Migration Tool is no longer supported.
Revision 04	Added bug 193777.
Revision 03	Added workaround for bug 175550.
Revision 02	Added bug 168645.
Revision 01	Initial release.

This ArubaOS release notes includes the following topics:

Throughout this document, branch controller and local controller are termed as managed device.

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

Chapter 2
New Features and Enhancements

There are no features or enhancements introduced in this release.

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 3: *Supported Controller Platforms in ArubaOS 8.3.0.1*

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 4: *Supported AP Platforms in ArubaOS 8.3.0.1*

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 4: *Supported AP Platforms in ArubaOS 8.3.0.1*

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 4: *Supported AP Platforms in ArubaOS 8.3.0.1*

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

Chapter 4
Regulatory Updates

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.

The following DRT file version is part of this release:

- DRT-1.0_65328

This chapter describes the issues resolved in this release.

Table 5: *Resolved Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154096	**Symptom:** Channels of the virtual APs were inconsistent between the managed devices and the APs when a radar event was detected in the channel. The fix ensures that the channels of virtual APs are consistent between the managed devices and the APs. **Scenario:** This issue occurred when the backup Remote AP got disconnected from the managed device. This issue was observed in 300 Series, 310 Series, 320 Series, 330 Series, and 370 Series access points running ArubaOS 8.0.0.0 or later versions.	AP Regulatory	300 Series, 310 Series, 320 Series, 330 Series, and 370 Series access points	ArubaOS 8.1.0.0	ArubaOS 8.3.0.1
167110	**Symptom:** An AP failed to set up IPsec tunnel when LMS IP was set to VRRP IP address. The fix ensures that the AP is able to set up the IPsec tunnel. **Scenario:** This issue occurred due to a race condition between **IKE** and **FPAPPS**. This issue was observed in a managed devices running ArubaOS 8.1.0.2 or later versions.	VRRP	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.3.0.1
173788 174490 178159	**Symptom:** Clients switched between APs or sometimes to the other band on the same AP. The fix ensures that the clients age out normally when roaming. **Scenario:** This issue occurred when a client sent packets that indicated it is about to roam but attempted to re-associate with the same AP. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.1
174615	**Symptom:** Cluster VRRP flapping was observed when threshold values on a managed device were modified. This issue is resolved by retaining VRRP flaps when the cluster parameters are modified. **Scenario:** This issue occurred when the cluster manager added or deleted the VRRP instances multiple times. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	VRRP	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1

Table 5: *Resolved Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175945	**Symptom:** A stand-alone controller acting as a DHCP server for multiple VLAN pools tagged DHCP-offer packets with the wrong VLAN. The fix ensures that the DHCP-offer packets are tagged with the correct VLAN. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.0.0.0.	VLAN	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.3.0.1
176434	**Symptom:** The Captive Portal page was not displayed correctly on client devices. The fix ensures that the Nginx collects the correct configuration rule. **Scenario:** This issue occurred when the Nginx collected the wrong configuration rule while searching for the CSS file. This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.2.0.2 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
176490 178407 178459 178469 179289 180554	**Symptom:** Clients were unable to send packets that are larger than 978 bytes over an IPsec tunnel. The fix ensures that the clients are able to send packets that are larger than 978 bytes over an IPsec tunnel. **Scenario:** This issue was observed in access points running ArubaOS 8.2.0.1 or later versions.	AP Datapath	320 Series access points	ArubaOS 8.2.0.1	ArubaOS 8.3.0.1
177352 179430	**Symptom:** A managed device crashed and rebooted with the error message, **Atleast 2000 MB free flash is recommended to keep system stable. Please clean up your flash file**. This issue is resolved by reducing the size of the IP packets. **Scenario:** This issue occurred when a managed device received IP packets larger than one segment. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Controller-Platform	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
177589	**Symptom:** A managed device dropped traffic although it was configured to allow traffic. The fix ensures that the managed device successfully allows traffic. **Scenario:** This issue occurred when the **override** in the **netdestination** configuration was enabled. This issue was observed in managed device running ArubaOS 8.2.0.2 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1

Table 5: *Resolved Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177789	**Symptom:** When an incorrect password was entered in an external captive portal multiple times, **errmsg=Authentication%20failed** was appended to the URL multiple times. The fix ensures that **errmsg=Authentication%20failed** is appended to the URL once. **Scenario:** This issue occurred when external captive portal was used with a non-ClearPass Policy Manager server. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1
177796	**Symptom:** A managed device's internal captive portal was displayed incorrectly when the client attempted to log in using external captive portal. The issue is resolved by displaying an appropriate reason for authentication failure if blank credentials are used to log in. **Scenario:** This issue occurred when the client tried to log in with the external captive portal using either a blank username, blank password, or both. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
177797 179433	**Symptom:** A managed device displayed an error, **An error occurred, Resource is currently unavailable. Please try again later**, when the captive portal login URL was too long. The fix ensures that when the incorrect credentials are entered, the page is redirected to login page. **Scenario:** This issue occurred when incorrect credentials were entered. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
178016	**Symptom:** Some APs detected false radar signals and changed radio channels frequently. The fix ensures that the APs do not detect false radar signals. **Scenario:** This issue occurred when the false radar Type ID was 36. This issue was observed in AP-105 access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-105 access points	ArubaOS 8.3.0.0	ArubaOS 8.3.0.1
178134	**Symptom:** The string under the **Message** column in the output of the **show configuration failure all** was truncated. This issue is resolved by increasing the string length. **Scenario:** This issue occurred when the string length under the **Message** column was more than 50 characters. This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.2.1.0.	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1

Table 5: *Resolved Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178140 179044	**Symptom:** A managed device's internal captive portal was displayed incorrectly when the client attempted to log in using the external captive portal. The issue is resolved by displaying an appropriate reason for authentication failure if incorrect credentials are used to log in. **Scenario:** This issue occurred when the client tried to log in with the external captive portal using incorrect credentials. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
178158	**Symptom:** Android devices were unable to resolve ARP requests. The fix ensures that the Android devices are able to resolve ARP requests. **Scenario:** This issue occurred because the Android client sent the ARP request as the first packet instead of a multicast packet. A multicast packet is required as a first packet to create a user entry. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Controller - Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1
178268	**Symptom:** Clients connected through VIA failed to establish an IPsec connection over SSL. The fix ensures that the clients connected through VIA are able to start SSL fallback, when IPsec connection failed. **Scenario:** This issue occurred as the clients were unable to start SSL fallback while establishing IPsec connection. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.1
178284	**Symptom:** A Mobility Master Virtual Appliance lost network connectivity. The fix ensures that the Mobility Master Virtual Appliance does not lose network connection. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.2.0.2 or later versions.	Controller - Datapath	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
178357	**Symptom:** APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **FW ASSERT at rc_get_nss_from_ chainmask()**. Improvements to the wireless driver resolved the issue. **Scenario:** This issue was observed in 300 Series, 303 Series, 310 Series, 320 Series, 330 Series, 360 Series, and 370 Series access points running ArubaOS 8.2.1.0 or later versions.	AP-Wireless	300 Series, 303 Series, 310 Series, 320 Series, 330 Series, 360 Series, and 370 Series access points	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1

Table 5: *Resolved Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178390	**Symptom:** Few APs failed to switch over to another managed device in a cluster setup. The fix ensures that the APs switch over to another managed device successfully. **Scenario:** This issue occurred when a managed device rebooted. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Cluster-Manager	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1
178609	**Symptom:** A managed device retained port channel trunk allowed VLAN configuration from the setup configuration instead of receiving the same from the Mobility Master, thereby causing device connectivity issue. The fix ensures that the managed device retains the correct configuration from the Mobility Master. **Scenario:** This issue occurred when the setup configuration was different from port channel configuration on the Mobility Master for the device node. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Configuration	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
178700	**Symptom:** The default server certificate was presented instead of the captive portal certificate. The fix ensures that the captive portal certificate is presented. **Scenario:** This issue occurred when a user attempted to log in to an external captive portal page that used HTTP instead of HTTPS. This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.3.0.1
178839	**Symptom:** When an AP with static channel or EIRP was rebooted, the opmode changed on other Dual 5 GHZ APs as well. This resulted in 2.4 GHz APs getting EIRP computed for 5 GHz AP and vice-versa. The fix ensures that the auto opmode switching is disabled for the AP when static EIRP or static channel settings are detected on the AP. **Scenario:** This issue occurred under the following conditions: ■ The Dual 5G APs were configured with static channels or EIRP. ■ The AP was rebooted. ■ The value of **dual-5ghz-mode** was set to **automatic** in the **ap system-profile**. This issue was observed in APs running ArubaOS 8.3.0.0.	AirMatch	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.3.0.1

Table 5: *Resolved Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178967 180252	**Symptom:** Clients could not associate to an AP. The log file lists the reason for the event as **UAC Down**. The fix ensures that the clients can associate to an AP successfully. The fix ensures that the association failure does not occur. **Scenario:** This issue occurred when AP load balancing was enabled and the UAC response packets did not reach the AP. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Cluster-Manager	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1
179112 179413	**Symptom:** When there was an authentication failure, the managed device did not redirect the user to the URL configured using the captive portal profile. The fix ensures that the managed device redirects the user to the URL configured. **Scenario:** This issue occurred when the client tried to log in with the external captive portal using incorrect credentials. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.3.0.1
179117	**Symptom:** Some configurations were missing in the new cluster member although the **Configuration State** on a managed device displayed UPDATE SUCCESSFUL. The fix ensures that the managed device displays the accurate configuration state. **Scenario:** This issue occurred when a new cluster member was added to an existing cluster. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1
179124	**Symptom:** A managed device displayed the following error messages: **ERRS |wms| WMS Event Table Cleanup: The system call to pthread_create() has failed with error [Resource temporarily unavailable.** Enhancements to memory management resolved the issue. **Scenario:** This issue occurred because of a memory leak. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Air Management - IDS	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.3.0.1

Table 5: *Resolved Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179215	**Symptom:** AirMatch deployed the APs with wider channel bandwidth when the number of configured channels was less than 3. The fix ensures that AirMatch deploys the APs with correct channel bandwidth. **Scenario:** This issue occurred when frequency reuse channel bandwidth selection logic did not scale well when the number of channels were less than 3. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AirMatch	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.1
179939 181520	**Symptom:** User was unable to configure **radius-interim-accounting** parameter in the **aaa profile**. The fix ensures that the user is able to configure **radius-interim-accounting** parameter in the **aaa profile**. **Scenario:** This issue occurred when the **dhcp-option-12** parameter in the **aaa derivation-rules** command and the **enforce-dhcp** parameter in **aaa profile** command were enabled. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.3.0.1
180340	**Symptom:** APs were unable to boot up using APBoot version 1.2.5.0. The fix ensures that APs are able to boot with the APBoot version 1.2.5.0. **Scenario:** This issue was observed in AP-134 and AP-135 access points running ArubaOS 8.3.0.0.	AP-Wireless	AP-134 and AP-135 access points	ArubaOS 8.3.0.0	ArubaOS 8.3.0.1

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

Known Issues

Following are the known issues observed in this release.

Table 6: *Known Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version
156149 162902	**Symptom:** The **OFA** process in a managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	SDN	All platforms	ArubaOS 8.0.1.0
159921	**Symptom:** The **Dashboard > WAN** page of the Mobility Master WebUI displays the WAN uplink status incorrectly. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.1.0.0
160389	**Symptom:** The **Dashboard > WAN> <node>** page of the Mobility Master WebUI displays only five uplinks. **Scenario:** This issue is observed in a branch office setup running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.1.0.0
168180	**Symptom:** The **profmgr** process crashes when the single instance default profile is modified by the administrator in disaster recovery mode. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0.1.0

Table 6: *Known Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version
168636	**Symptom:** Clients are unable to connect to a stand-alone controller from Aruba Central using SSH. **Scenario:** This issue is observed in 7005 controllers running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Aruba Central	7005 controllers	ArubaOS 8.0.1.0
168645 176421	**Symptom:** A managed device does not receive configuration from the secondary Mobility Master. **Scenario:** This issue occurs when a FQDN is configured for the secondary **masterip** and **l3-peer-ip** is configured as a FQDN. The primary and secondary Mobility Master do not synchronize and a managed device does not receive the configuration from the secondary Mobility Master at failover. This issue is observed in managed devices running ArubaOS 8.2.0.0 or later versions. **Workaround:** Reload the managed device.	Master-Redundancy	All platforms	ArubaOS 8.2.0.0
172857 178662	**Symptom:** The **BOCMGR** process crashes in a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.2.0.2
175138	**Symptom:** The **Configurations > Services > Guest Provisioning** page appears blank and not editable. **Scenario:** This issue occurs when user enters **&** character in the email fields and submits the changes. This issue is observed in Mobility Masters or managed devices running ArubaOS 8.2.0.2 or later versions. **Workaround:** None.	Guest Provisioning	All platforms	ArubaOS 8.2.0.2
175550	**Symptom:** Users cannot disable the security logging for the **aaa** process using the **logging security process aaa subcat aaa level debugging** command. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.2 or later versions. **Workaround:** Each time a managed device reboots, execute the following command in the CLI: ■ **Logging security subcat aaa level debugging** **Write memory** ■ **No logging security subcat aaa** **Write memory**	Configuration	All platforms	ArubaOS 8.2.0.2

Table 6: *Known Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version
176185	**Symptom:** The AirGroup profile does not take effect on a managed device when AirGroup was configured in centralized mode. **Scenario:** This issue occurs when the AirGroup feature is enabled on a managed device. This issue is observed in managed devices running ArubaOS 8.2.0.1 or later versions. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.2.0.1
176330 177428	**Symptom:** The **Diagnostics > Technical Support > Copy Files** page of the WebUI displays a success message although the TFTP file transfer fails. **Scenario:** This issue occurs when a user attempts to copy a file using TFTP. This issue is observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.0.0
176956	**Symptom:** APs fail to locate the managed device using DNS and reboots. **Scenario:** This issue occurs when IPv6 addresses are assigned to respective APs. This issue is observed in AP-315 access points running ArubaOS 8.2.0.2 or later versions. **Workaround:** None.	AP-Platform	AP-315 access points	ArubaOS 8.2.0.2
177509	**Symptom:** User is unable to ping the servers from a managed device. **Scenario:** This issue occurs when the managed device obtains configuration after a reload. This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0

Table 6: *Known Issues in ArubaOS 8.3.0.1*

Bug ID	Description	Component	Platform	Reported Version
177800	**Symptom:** Aruba Central agent debugging logs contain the hash value for the certificate sign challenge. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Logging	All platforms	ArubaOS 8.0.1.0
177891	**Symptom:** Clients are often disconnected from the network due to **Authentication** process crash. **Scenario:** This issue occurs when a ClearPass Policy Manager role download is configured but the role is improper or empty. This issue is observed in 7220 controllers running ArubaOS 8.2.0.2 or later versions. **Workaround:** None.	Base OS Security	7220 controllers	ArubaOS 8.2.0.2
193777	**Symptom:** The **authentication** process crashes when the managed device is upgraded from ArubaOS 8.2.1.1 to ArubaOS 8.3.0.5. **Scenario:** 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 **authentication** process crash. This issue is observed in managed devices running ArubaOS 8.3.0.1 or later versions. **Workaround:** None.	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.

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

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 26 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 26 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 26 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 flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```

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

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

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

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

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

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

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

Upgrading ArubaOS

Upgrade ArubaOS using the WebUI or CLI.

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 25.

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.

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 ArubaOSimage 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 26 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 26 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 26.
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.