ArubaOS 8.2.1.0

a Hewlett Packard
Enterprise company

Release Notes

Open Source Code

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

Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	■ Removed **ArubaOS 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 the **Upgrade Procedure** chapter as the Migration Tool is no longer supported.
Revision 03	Added bug 168645.
Revision 02	Added 90 Series access points in the **Supported Platforms** section.
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.

Related Documents

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

- *ArubaOS Release Notes*
- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- *ArubaOS 8.x Syslog Message Guide*
- *Aruba Mobility Master Licensing Guide*
- *Aruba Mobility Master and VMC Installation Guide*
- *Aruba Wireless Access Point 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 higher on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 8.0 or later on macOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	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

The following features or enhancements are introduced in this release.

AirMatch

New Commands

The following commands are introduced in ArubaOS 8.2.1.0:

- **show airmatch network-tech-support**—This command collects the output for all the radios that are in the same partition for a specified Radio AP name. This command also lists and describes the AP Radios that will be handled further.

The following example displays a partial output of the **show airmatch network-tech-support ap-name F-16-a-QCA** command:

```
(host) [mynode]#show airmatch network-tech-support ap-name F-16-a-QCA
 Summary of included radios
 AP Name: F-16-a-QCA Radio: ac:a3:1e:59:b4:c0 Band: 2GHz RF domain: 001 partition: 000
 Num radios: 40 New radios: false

   Radio             AP Name

   ----------------- -----------
   ac:a3:1e:59:b4:c0 F-16-a-QCA
   a8:bd:27:d0:69:e0 F-PP-a-QCA
   9c:1c:12:8c:6e:a0 Fremont-sniffer-225
   ac:a3:1e:59:9e:00 F-12
   70:3a:0e:52:22:40 F-PP-b
   ac:a3:1e:59:c7:80 F-16-c-QCA
   ac:a3:1e:59:97:e0 F-RVR-d
   ac:a3:1e:59:98:20 F-Multiclient-a
   70:3a:0e:52:23:a0 F-17-QCA
   a8:bd:27:d0:5e:80 F-19-a
```

```
70:3a:0e:52:28:e0 F-15-a
18:64:72:7e:af:20 F-15-b-QCA
a8:bd:27:59:fc:e0 F-19-c
a8:bd:27:59:fc:00 F-18-c
a8:bd:27:59:f4:e0 F-18-b
ac:a3:1e:59:aa:a0 F-13
a8:bd:27:d0:5f:c0 F-19-b
ac:a3:1e:53:b8:00 F-16-b-QCA
ac:a3:1e:59:b7:40 F-RVR-g
a8:bd:27:59:fb:e0 a8:bd:27:cd:9f:be
18:64:72:fd:67:a0 18:64:72:c7:d6:7a
18:64:72:d3:81:00 F-11-BRCM
ac:a3:1e:59:9e:80 F-front-door-1
9c:1c:12:87:33:60 F-4-BRCM
ac:a3:1e:59:9d:00 F-RVR-e
ac:a3:1e:59:9a:c0 F-14-QCA
70:3a:0e:6e:5e:20 F-RVR-b
a8:bd:27:d0:94:a0 F-18-a
ac:a3:1e:59:a0:00 1344-2-AP04
18:64:72:7e:c5:c0 F-15-c-QCA
```

- **show airmatch tech-support** —This command collects the output for the AP or the radio.

The following example displays a partial output of the **show airmatch tech-support mac ac:a3:1e:59:b4:c0** command:

```
(host) [mynode] #show airmatch tech-support mac ac:a3:1e:59:b4:c0
```

```
show airmatch debug reporting-radio MAC ac:a3:1e:59:b4:c0

Field                Value
-----                -----
Band                 2GHz
AP Ethernet MAC      ac:a3:1e:cd:9b:4c
Radio MAC            ac:a3:1e:59:b4:c0
AP Name              F-16-a-QCA
AP Model             AP-325
LMS IP               192.168.200.15
Switch IP            192.168.200.15
Last Update          2017-11-16 02:57:57
Channel              7
Bandwidth            20MHz
Channel Reason       AirMatch - Solver
Channel Update Time  2017-11-14 10:42:53
EIRP                 10.0 (dBm)
EIRP Reason          AirMatch - Solver
EIRP Update Time     2017-11-16 02:55:19
Is Active            true
Is Static Chan       false
Is Static EIRP       false
Is Static CSR        false
Deploy Hour          N/A
Retries              5
Last Retry Time      2017-11-14 09:00:38
Local Time           PST8PDT,M3.2.0,M11.1.0
```

- **show airmatch debug advanced stat** —This command displays detailed statistics about the APs or radios on a Mobility Master.

The following example indicates the AirMatch statistics related to the APs:

```
(host)#show airmatch debug advanced stat ap
```

```
Field Value
----- -----
Number of APs 2304
+----------------------------------+
|Number of 5GHz Radios per AP model|
+----------------------------------+
AP Model Count
-------- -----
AP-205H 1224
AP-224 47
AP-225 976
AP-275 55
AP-365 1
+----------------------------------+
|Number of 2.4GHz Radios per AP model|
+----------------------------------+
AP Model Count
-------- -----
AP-205H 1224
AP-224 47
AP-225 976
AP-275 56
AP-365 1
```

- **show airmatch debug db-dump status** —This command collects information about the status of the AirMatch debug database dump.

The following example indicates the status of the AirMatch debug database dump:

```
(host)#show airmatch debug db-dump status

dbdump status info
------------------
Field                Value
-----                -----
dbdump status        SUCCESS
Begin time           2018-03-19 15:58:50
End time             2018-03-19 15:58:53
```

AP-Wireless

No Support for Cell Size Reduction

Starting from ArubaOS 8.2.1.0, the **cell-size-reduction** parameter in the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands does not take effect for 300 Series access points. If the **cell-size-reduction** parameter has any configured value, the 300 Series access points disregard the value.

Base OS Security

Enable Telnet

To enable telnet on managed devices, execute the following commands:

```
(host) [mynode] (config) #firewall cp
(host) [mynode] (config-submode) #ipv4 permit any proto 6 ports 23 23
(host) [mynode] (config-submode) #!
(host) [mynode] (config-submode) #exit
(host) [mynode] (config) #exit
```

Modified Command

Starting from ArubaOS 8.2.1.0, the output of the **show netdestination** command displays the netdestination ID along with the netdestination name. The following sample shows the output of the **show netdestination** command:

```
(host) [mynode] #show netdestination
Name: sep23-ipv4
Destination ID: 34
Position  Type  IP addr   Mask-Len/Range
--------  ----  -------   --------------
1         host  1.1.1.1   32
2         name  0.0.0.8   google.com
```

Certificate Manager

Successful Download Message

Starting from ArubaOS 8.2.1.0, Mobility Master continuously tries to synchronize the certificates to a managed device until it is successful. If the synchronization fails, the failure logs are listed under the **show switches** command as **CONFIG-FAILURE**. To view the list of failed certificate synchronizations, execute the **show configuration failure** command.

Controller-Datapath

Datapath Route Limits

Starting from ArubaOS 8.2.1.0, the datapath route limits are increased to match the route limits of the control plane.

Table 3: *New Datapath Route Limits*

Controller Family	New Datapath Limits
7005	4K
7008	4K
7024	4K
7030	8K
7205	16K
7210	16K
7220	16K
7240	32K
7240XM	32K
7280	32K

Controller-Platform

NTP Authentication Option

Starting from ArubaOS 8.2.1.0, a new NTP authentication option using SHA1 digest is available. A new parameter, **sha1**, is introduced in the **ntp authentication-key** command. You can configure this option in the CLI as shown in the following example:

```
(host)[mynode](config) #ntp authentication-key <keyid> sha1 <keyvalue>
```

The authentication key ID must be in the range of 1–65534. The key value must be up to 255 ASCII characters.

The **show ntp authentication-keys** command helps you verify the NTP authentication key type. The output of this command displays the SHA1 key type and the secret field (in encoded format), when SHA1 authentication is configured. The following example shows the output of the **show ntp authentication-keys** command:

```
(host) [mynode] # show  ntp authentication-keys
Key Id     Key Type     Secret
------     --------     ------
41          sha1        ********
```

Retrieving Crash Information from Managed Devices

To access the crash files after upgrading a managed device to ArubaOS 8.2.1.0, you must clear the old crash files. Remember the following important points regarding the old crash files cleanup:

- Before you upgrade to ArubaOS 8.2.1.0, ensure that you clean up the old crash files if any, using the **tar crash** command.
- If you have upgraded a managed device to ArubaOS 8.2.1.0 before cleaning up the old crash files and if there are no new crashes after the upgrade, you must still clean up the old crash files using the **tar crash** command.
- If you execute the **tar crash** command:
  - before cleaning up the old crash files, the **crash.tar** and **crash1.tar** files are created.
  - after cleaning up the old crash files, only the **crash.tar** file is created.

When you report a crash, execute the **copy** command to copy the **crash.tar** and **crash1.tar** files (if applicable), and share the files with Technical Support.

DHCP

Enhancements to Specify Option 43 as a Hex String

Starting from ArubaOS 8.2.1.0, support for specifying option code with hex data string is introduced. The following example shows the output of the **ip dhcp pool** command:

```
(host) [mynode] (config-submode)# option 43
hex                     Hex String. Max hex characters allowed is 22.
ip                      Specify IP address
text                    Option string(Max 512 Characters allowed)
```

OSPF

Enhancements to show ip route Command

Starting from ArubaOS 8.2.1.0, the output of the **show ip route** command is modified to display the administrative distance and cost in **[AD/Cost]** format. In the previous releases, the information was in **[Cost/AD]** format.

Following is the modified output of the **show ip route** command. **[1/0]** in the following output represents the **[AD/Cost]**, respectively.

```
Codes: C - connected, O - OSPF, R - RIP, S - static
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.7.73.77 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0   [1/0] via 10.7.73.77*
S     172.0.0.0/8   [1/0] via 172.16.1.253*
```

Enhancements to show ip ospf interface Command

Starting from ArubaOS 8.2.1.0, the output of the **show ip ospf interface vlan** command displays the **Tx Err** and **Rx Err** parameters to indicate any errors in the transmitted and received packets. This information is helpful to analyze defects based on the tech-support logs.

The following example displays the output of the **show ip ospf interface vlan 1** command:

```
Vlan 1 is up, line protocol is up
Internet Address 170.1.0.1, Mask 255.255.255.0, Area 2.0.1.1
Router ID 16.1.0.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 0
Designated Router id 0.0.0.0, Interface Address 170.1.0.1
Backup designated Router id 0.0.0.0, Interface Address 170.1.0.1
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Neighbor Count is 0
Tx Stat: Hellos 7 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 7
Tx Err:  BufNull 0 BufCorrupt 0 NoMem 0 SendFail 0
Rx Stat: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 0
LoopSend 0 RxVirtualLink 0
Rx Err:  DisCd 0 BadVer 0 BadNet 0 BadArea 0 BadDstAdr 0 BadAuType 0
BadAuth 0 BadNeigh 0 BadPckType 0 BadVirtLink 0
IntfDown 0 MySource 0 Legal 0
```

SNMP

Enhancement to SNMP Authentication Failed Trap

Starting from ArubaOS 8.2.1.0, the **SNMP Authentication Failure** trap includes the IPv4 address of the source that fails authentication.

VRRP

Support for Unique Local Address Configuration on VRRP

Starting from ArubaOS 8.2.1.0, you can configure a unique local address as the VRRP IPv6 address on the Mobility Master and the managed devices.

WebCC

Support for Clearing WebCC Statistics on Managed Devices

Starting from ArubaOS 8.2.1.0, you can clear the WebCC statistics from managed devices using the **clear web-cc md stats** command.

WebUI

Source Address Field Introduced Under DHCP settings

Starting from ArubaOS 8.2.1.0, **Source Address** field is introduced under **DHCP Helpers** in the **Configuration** > **Interfaces** > **VLANs** > **IPv6** tab. This field is used to configure **DHCP Helpers** with specific IPv6 address of an interface VLAN that has multiple IPv6 addresses.

EAP-TLS Provisioning Parameter

Starting from ArubaOS 8.2.1.0, the **EAP-TLS** option is added to the **Uplink authentication** parameter listed under **Configuration** > **Access Points** page of the WebUI.

Support for WLAN Forwarding Mode Options

Starting from ArubaOS 8.2.1.0, new options, **Split-Tunnel** and **Bridge**, are added to the **Forwarding mode** drop-down list in the **WLANs > General** page.

This chapter describes the hardware platforms supported in this release.

Mobility Controller Platforms

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

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.2.1.0*

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

AP Platforms

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

Table 5: *Supported AP Platforms in ArubaOS 8.2.1.0*

AP Family	AP Model
90 Series	AP-92, AP-93
93H Series	AP-93H
100 Series	AP-104, AP-105
103 Series	AP-103
103H Series	AP-103H

Table 5: *Supported AP Platforms in ArubaOS 8.2.1.0*

AP Family	AP Model
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135
170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1
200 Series	AP-204, AP-205
203H Series	AP-203H
205H Series	AP-205H
207 Series	AP-207
203R Series	AP-203R, AP-203RP
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303H Series	AP-303H
310 Series	AP-314, AP-315
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
360 Series	AP-365, AP-367

Table 5: *Supported AP Platforms in ArubaOS 8.2.1.0*

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

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

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

The following DRT file version is part of this release:

- DRT-1.0_63516

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
103312	**Symptom:** A WebUI using certificate authentication returned an invalid value for a session cookie. This issue is resolved by setting an empty value for the session cookie when it is created. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Web Server	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
126176	**Symptom:** LLDP requests from multiple clients triggered unnecessary wired authentication requests that failed. The fix ensures that unnecessary wired authentication requests are blocked. **Scenario:** This issue occurred when wired authentication was linked with MAC authentication. This issue was observed in managed devices running ArubaOS 8.0.0.0.	LLDP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
133304	**Symptom:** A user was unable to assign a static IP to a Remote AP using the WebUI. The fix ensures that the user can assign a static IP to a Remote AP. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.0.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
134824 139171 142938 147661 147662 153682 154385 160315 161477	**Symptom:** A managed device crashed unexpectedly and while rebooting, it experienced additional exceptions. The log file listed the reason for the event as **kernel panic**. The fix ensures that when the managed device reboots, the debug details are stored so that the original cause of reboot can be identified. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0.	Controller-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140695	**Symptom:** A newly added AP operated incorrectly on maximum EIRP value. The fix ensures that the AP uses the average of the EIRP values configured on the AP and that of the hardware. **Scenario:** This issue occurred during the initial bootup or factory reset of an AP. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AirMatch	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
140779	**Symptom:** SNMP enterprise-specific traps did not contain the enterprise trap OID. The fix ensures that the traps contain the enterprise trap OID. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.2.0.0.	SNMP	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
143057	**Symptom:** The values displayed for the following parameters in the output of the corresponding **show** commands were inaccurate: ■ The **Channel Busy** value of **show ap debug radio-stats** ■ The **Utilization(%)** value of **show ap spectrum channel-metrics** Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-205H, 210 Series, 220 Series, and AP-277 access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-205H, 210 Series, 220 Series, and AP-277 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
151817	**Symptom:** After migration, the entries of the APs that were in DOWN status in the ArubaOS 6.x.x.x setup were missing from the global AP database of ArubaOS 8.x.x.x setup. The fix ensures that the global AP database is updated correctly. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.0.1.0 or later versions	Migration	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.2.1.0
154899	**Symptom:** The **BLE Relay** process in a managed device crashed unexpectedly. The fix ensures that the **BLE Relay** process does not crash and the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	BLE	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
156484 171487 172129	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Unable to handle kernel paging request for data at address 0x00000000**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in 200 Series access points running ArubaOS 8.0.0.0.	AP-Platform	200 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
158459	**Symptom:** An SNMP query in a managed device returned an incorrect value for the associated user count in an AP. The fix ensures that the SNMP query returns the correct value. **Scenario:** This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
158719 158720	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Intent:cause:register 56:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when an AP with two physical ports was connected to a switch, which led to a CPU stack overflow. This issue was observed in 7000 Series and 7200 Series controllers running ArubaOS 8.0.0.0 or later versions.	Controller - Datapath	7000 Series and 7200 Series controllers	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
160725 171492	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the TPM certificate was corrupted. This issue was observed in AP-305 access points running ArubaOS 8.2.0.0 or later versions.	AP-Platform	AP-305 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
160793	**Symptom:** A client was unable to pass traffic and a VRRP failover occurred. The fix ensures that the client is able to pass traffic. **Scenario:** This issue occurred when the LACP striping IP was configured as the VRRP IP. This issue was observed in 220 Series and 320 Series access points running ArubaOS 8.0.0.0 or later versions.	AP Datapath	220 Series and 320 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
160854	**Symptom:** Some voice clients failed to pass traffic because they did not receive an ARP response. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when CAC and aggregation were enabled on voice clients. This issue was observed in managed devices running ArubaOS 8.0.0.0.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
161825	**Symptom:** An IF MIB showed the same values for all interfaces. The fix ensures that the correct value for each interface is displayed. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	SNMP	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
162011	**Symptom:** VLAN interface was displayed as DOWN although the interface operstate was UP. The fix ensures that the VLAN interface state is displayed correctly. **Scenario:** This issue occurred due to a log error. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Mesh	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
162021 167981	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Assertion failed! (pdev->ar_rx_ops->attn_msdu_done(rx_desc)):htt_rx_debug**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 8.2.0.0.	AP-Wireless	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
162605	**Symptom:** A wireless client appeared to be active on two different APs at the same time because one of the APs failed to age out the client entry from its user table. The fix ensures that the AP ages out the client entry from its user table. **Scenario:** This issue occurred when the wireless client roamed from one AP to another AP that terminated on a different managed device. This issue was observed in 200 Series access points running ArubaOS 8.1.0.0 or later versions.	AP-Wireless	200 Series access points	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
162870	**Symptom:** Clients experienced a slow connection when an AP used a 4G modem for uplink. The fix ensures that clients get the optimal connection speed. **Scenario:** This issue was observed in AP-203R, AP-203RP, AP-205, and AP-205H access points running ArubaOS 8.2.0.0 or later versions.	AP-Platform	AP-203R, AP-203RP, AP-205, and AP-205H access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
162977 167907	**Symptom:** Incorrect roles were applied to the client after authentication. The fix ensures that the correct roles are applied. **Scenario:** This issue was observed in bridge users connected to APs. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
163066	**Symptom:** A managed device rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
163117	**Symptom:** When a factory-reset managed device joined a Mobility Master, it overwrote the 'trusted' attribute of Ethernet interfaces on the Mobility Master configuration. This issue is resolved by ensuring that only the port that gets the DHCP information during ZTP is overwritten with the 'trusted' attribute. **Scenario:** This issue occurred because, during ZTP, all ports were overwritten with the 'trusted' attribute in the setup file. This issue was not limited to any specific platform or ArubaOS version.	Configuration	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
163547 170184	**Symptom:** The console log of an AP displayed the **nul_get_max_amsdu_size(2126): WARN: AMSDU size is not explicitly configured** warning message. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in APs running ArubaOS 8.1.0.0.	AP-Wireless	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
164073	**Symptom:** The SNMP trap messages incorrectly indicated that a client's location had changed. But the voice client was associated to an AP and did not make any call or roam. This issue is resolved by ensuring that an unconditional SNMP trap notification is sent only when a client entry is created for the first time; also, subsequent notifications are sent only when the client's location has changed. **Scenario:** This issue occurred when the voice client was registered to multiple SIP servers and sent SIP register messages. This issue was not limited to any specific platform and was observed in managed devices running ArubaOS 8.0.0.0.	UCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
164338	**Symptom:** When an outdoor AP is powered up using an AF powered switch, the AP moved to APM mode. The fix ensures that the AP does not move to APM mode. **Scenario:** This issue occurred because the logic in the AP tried to shut down both radios if the power source was AF. A channel validation check was triggered assuming the radios were up and running and moved the AP to APM mode. This issue was observed in AP-275 access points connected to managed devices running ArubaOS 8.1.0.0.	ARM	AP-275 access points	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
164388	**Symptom:** When IPM was enabled, the system LED displayed an amber light although no power restriction was applied. Improvements to the wireless driver resolved the issue. **Scenario:** This issue occurred because the IPM disabled an option that periodically checks the system power supply status. This issue was observed in access points running ArubaOS 8.1.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
164545 171736 174858	**Symptom:** The WebUI displayed an alert message, **WebCC licenses exceeded**, although no WebCC license was installed. The fix ensures that the alert message is displayed only when the WebCC feature is enabled. **Scenario:** This issue occurred when the WebCC feature was enabled and the number of AP licenses exceeded the WebCC limit. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Licensing	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
164659	**Symptom:** The output of the **show ap debug dot11r efficiency** command displayed 0% as the value in the **Hit (%)** and **Miss (%)** columns. The fix ensures that the CLI output displays the correct values. **Scenario:** This issue occurred in managed devices operating in tunnel mode. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Station Management	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
164986 167374	**Symptom**: The logs were flooded with multiple kernel print messages. The fix ensures that the managed device logs are not flooded with these messages. **Scenario:** The issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
165900 171831	**Symptom:** For wired users, an ARP entry was not displayed on a managed device. The fix ensures that the ARP entry is displayed. **Scenario:** This issue occurred because the **inter-tunnel-flooding** parameter was disabled when the **interface tunnel** command was executed on the managed device. This issue was observed in managed devices running ArubaOS 8.1.0.1 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.1.0.1	ArubaOS 8.2.1.0
166154	**Symptom:** A user observed inconsistent GRE headers in DNS packets sent by Apple devices. The fix ensures that the flags are not set in the GRE header. **Scenario:** This issue was observed in a Mobility Master where the GRE tunnels were statically configured and keepalive was disabled. This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
166183 169183	**Symptom:** An AP did not boot. When the AP was manually rebooted, it displayed the **bcm96xxx-wdt ff800428.watchdog: Watchdog timer stopped** message in the console log. The fix ensures that the AP boots correctly. **Scenario:** This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
166293	**Symptom:** Wired clients using bridge forwarding mode were unable to pass MAC authentication. The fix ensures that clients successfully pass MAC authentication. **Scenario:** This issue occurred when the clients were connected to IPv6 APs. This issue was not limited to any specific AP platform or ArubaOS release version.	Authentication	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
166366	**Symptom:** Users were unable to delete multiple IPM entries in the **Configuration > System > Profiles > All Profiles > AP system** page of the WebUI. The fix allows users to delete multiple IPM entries simultaneously. **Scenario:** This issue occurred when users attempted to delete multiple IPM entries simultaneously. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
166426 167050 170409	**Symptom:** A Mobility Master rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.2.0.0.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
166596	**Symptom:** Clients connected to an AP were continuously in sleep mode. As a result, clients lost data connectivity for a few seconds before recovering automatically. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the AP lost synchronization with clients in the power save state. This issue was observed in AP-215 access points running ArubaOS 8.1.0.0 or later versions.	AP-Wireless	AP-215 access points	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
166678	**Symptom:** A Remote AP authenticated a wired client without any credential check. This issue is resolved by deleting all Remote AP users with the same MAC address if they are wired clients and their ports are changed. **Scenario:** This issue occurred when a wired client that used a spoofed MAC address of an authenticated client was connected to a Remote AP. This issue was observed in Remote APs running ArubaOS 8.1.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
166838	**Symptom:** The output of the **show ap debug radio-stats** command displayed incorrect values for Tx Data Bytes. The fix ensures that the output of the **show ap debug radio-stats** command displays the correct values for Tx Data Bytes. **Scenario:** This issue was observed in AP-305 access points running ArubaOS 8.1.0.0 or later versions.	AP-Wireless	AP-305 access points	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
166865 169423	**Symptom:** The output of the **show ap debug radio-stats** command displayed incorrect values for Tx and Rx data bytes. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 802.11ac or 802.11n clients that were connected to AP-207 access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-207 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
166945	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in 200 Series access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	200 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
166963 167520 167719 171713	**Symptom:** An AP rebooted unexpectedly due to an external watchdog reset. Also, the AP rebootstrapped due to a broken heartbeat tunnel. The fix ensures that the AP works as expected. **Scenario:** The issue was observed in AP-207 access points running ArubaOS 8.0.0.0 or later versions.	AP Datapath	AP-207 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
167056	**Symptom:** The **Remote Intf** parameter in the output of the **show lldp neighbor** and **show ap lldp neighbors** commands displayed the port description TLV. The issue is resolved at both the AP side and managed device side in the following ways: ■ **AP fix**: Providing both port ID and port descriptions separately. ■ **Managed device fix**: Displaying only port number even when the port description is configured. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	LLDP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
167089	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167111	**Symptom:** Some clients were unable to pass traffic although they received the IP address from the correct VLAN. This issue is resolved by making multiple control plane attempts to configure the ACL on the data plane. **Scenario:** This issue occurred when the netdestination configurations were updated. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
167454 168103	**Symptom:** The following GSM Section publish errors were observed in the log files: **uthmgr[3709]: <522310> <3709> <ERRS> |authmgr| auth_gsm_publish_ip_user_section: gsm_section_update failed for ip 15.111.201.84 mac 34:36:3b:d3:05:1a result error_htbl_key_not_found size 288**. The issue is resolved by removing the unnecessary GSM channel publish events. **Scenario:** This issue occurred when RADIUS accounting was enabled for the users. 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 8.2.1.0
167467 174516	**Symptom:** A VRRP process crashed. Enhancements to the wireless driver fixed this issue. **Scenario:** This issue occurred when VRRP configurations were deleted and re-created using a script. This issue was observed in managed devices running ArubaOS 8.2.0.0.	VRRP	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
167479 167829	**Symptom:** Managed devices rebooted unexpectedly without generating a core dump file. The fix ensures that the core dump is collected as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
167679	**Symptom:** A Mobility Master tried to reach the wrong IP address of an Airwave server. This issue is resolved by correcting the endianess of the IP address. **Scenario:** This issue occurred because of wrong endianess. This issue was observed in a Mobility Master running ArubaOS 8.1.0.2.	SNMP	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167747 171565 172711	**Symptom:** An AP crashed and rebooted unexpectedly due to a firmware assert. The log file listed the reason for the event as **Unable to handle kernel NULL pointer dereference at virtual address**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the debug logging and the core dump generation were halted. This issue was observed in AP-325 access points running ArubaOS 8.0.0.0.	AP-Wireless	AP-325 access points	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
167825 167826 171609	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when AP-205 access point was added on to the managed device. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
167919	**Symptom:** A scanner declined the action frames sent by APs. This resulted in poor wireless performance. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in AP-205, 210 Series, 220 Series, and 270 Series access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-205, 210 Series, 220 Series, and 270 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
168039	**Symptom:** Users were unable to connect to VIA. The fix ensures that the users connect to VIA. **Scenario:** This issue occurred when an incorrect value for **NAS-Port-Type** was sent for VIA web authentication. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	RADIUS	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
168060 173578 173582	**Symptom:** The **authentication** process in a managed device crashed multiple times. The fix ensures that the **authentication** process does not crash. **Scenario:** This issue occurred when per-user bandwidth contract was enabled. This issue was observed on managed devices running ArubaOS 8.1.0.2 or later versions.	Base OS Security	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168157 170007 173928 174042	**Symptom:** The output of the **show ap mesh active** command displayed the following: ■ A mesh portal working in 2.4 GHz mode ■ The mesh point EIRP and maximum EIRP values as 0 But the **flex-radio** mode in the **ap system-profile** was configured as **2.4GHz-and-5GHz**. The fix ensures that the mesh portal works in the configured mode and the output of the command displays the correct EIRP and maximum EIRP values. **Scenario:** This issue was observed in access points running ArubaOS 8.0.0.0.	Mesh	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
168170	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-315 and AP-325 access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-315 and AP-325 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
168279 172750	**Symptom:** The configured bandwidth contracts were not applied for some clients. The fix ensures that clients do not exceed the contract speed. **Scenario:** This issue occurred when user role derivation was delayed after a MAC authentication. This issue was observed in managed devices running ArubaOS 8.0.0.0	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
168492 175310	**Symptom**: A Mobility Master displayed the error, **mDNS proxy runtime error at ag_send_packet_unicast 1105 Packet send failed error**. The fix ensures that the mDNS proxy runtime error is not seen on the Mobility Master. **Scenario**: This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	AirGroup	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168499 168711	**Symptom:** APs in AM-mode intermittently switched back to the AP-mode. The fix ensures that the APs do not randomly switch from their configured mode. **Scenario:** This issue occurred due to a mismatch between the current operating bandwidth and the configured bandwidth on the AP when scanning a 40 MHz radio channel. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	ARM	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
168551 169669	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **<0>[274540.243478] NMI watchdog: BUG: soft lockup - CPU#0 stuck for 22s! [sapd:1676]**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred during a cluster failover. This issue was observed in access points running ArubaOS 8.2.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
168692	**Symptom:** A client connected to a Mobility Master Hardware Appliance was unable to obtain a DHCP IP address after the initial setup wizard was launched. The issue is resolved by enabling the DHCP service in the Mobility Master Hardware Appliance. **Scenario:** This issue occurred because the DHCP service was disabled in the Mobility Master Hardware Appliance. This issue was observed in a Mobility Master Hardware Appliance running ArubaOS 8.1.0.0 or later versions.	DHCP	Mobility Master Hardware Appliance	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
168697	**Symptom:** The WebUI did not display the correct count of the APs that operated in AM mode. The fix ensures that the WebUI displays the correct count of the APs in AM mode. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Monitoring	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
168795	**Symptom:** A WebCC URL cloud lookup failed on a managed device. The log file listed the reason for the event as **<ERRS> |web_cc| web_cc_callback: URL lookup failed**. The fix ensures that the WebCC URL cloud lookup is successful. **Scenario:** This issue occurred when WebCC was enabled. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	WebCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168798 175902	**Symptom:** An **authentication** process crashed in a managed device. The fix ensures that the **authentication** process does not crash. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.1 in a cluster topology.	Base OS Security	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
168888	**Symptom:** False radar events were detected on an AP. The fix ensures that false radar events are not detected. **Scenario:** This issue occurred when DFS was enabled on the 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 8.2.1.0
168909	**Symptom:** The noise floor value in a DFS channel was higher than that expected. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when ARM scanning was enabled. This issue was observed in AP-315 and AP-335 access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-315 and AP-335 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
168984 170072 173647 174375 174998	**Symptom:** A managed device failed to update the syslog server. The issue is resolved by enhancing the logging mechanism. **Scenario:** This issue occurred because the syslog file size increased due to excess and incorrect logging from the managed device. 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 8.2.1.0
169012	**Symptom:** Multizone was not enabled on an AP. The fix ensures that although the AP has not acquired the RFP license, the MultiZone remains enabled. **Scenario:** This issue occurred when RFP was enabled after assigning MultiZone profile to an AP group. This issue was observed in a cluster running ArubaOS 8.2.0.0.	AP Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169091	**Symptom:** The **configuration** process failed in the startup wizard. The issue is resolved by sending the value selected by the user instead of the default value for Port mode and Port. **Scenario:** This issue was observed when a non-default port was used for the Mobility Master to communicate with the managed device. This issue was not limited to any specific managed device model or ArubaOS version.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169105	**Symptom:** The WebUI startup wizard displayed an error - **answer 'PST' is not valid.** The fix ensures that the user's timezone is selected if a timezone is not specified. **Scenario:** This issue occurred when a timezone was not specified. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169111	**Symptom**: In the startup wizard of a managed device, some of the configuration options were not displayed when the value for the **Connection to mobility master** parameter was modified. The fix ensures that all the configuration parameters are displayed. **Scenario**: This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169131 170473 171299 171823 175747	**Symptom:** The AppRF feature failed to block the traffic. The fix ensures that the AppRF feature works as expected. **Scenario:** This issue occurred when DPI classification and WebCC were enabled. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169184	**Symptom:** The managed devices continuously dropped the IPv6 traffic. The fix ensures that the traffic is uninterrupted. **Scenario:** This issue occurred when managed devices without a PEFNG license received packets from H323 VoIP clients. This issue was observed in managed devices running ArubaOS 8.1.0.0.	Controller-Datapath	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
169288	**Symptom:** An incorrect error message, **An internal system error has occurred at file aeroscout.c function rtls_send_message line 190 error sendto failed - e-101 l-74 ip-192.168.20.100 port-27425**, was displayed in the log files. The fix ensures that the correct error message is displayed. **Scenario:** This issue occurred when RTLS server was configured in the AP system profile. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	Air Management - IDS	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
169329	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP rebooted caused by internal watchdog reset**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-275, AP-277, AP-325, and AP-335 access points running ArubaOS 8.1.0.3 or later versions.	AP-Wireless	AP-275, AP-277, AP-325, and AP-335 access points	ArubaOS 8.1.0.3	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169416	**Symptom:** A client disconnected from an AP and did not reconnect. The status of the AP was displayed as **Unprovisioned, no such group in the data zone**. This issue is resolved by disabling the virtual AP of the zone which does not have the AP group. **Scenario:** This issue occurred when MultiZone was assigned to an AP group. This issue was observed in a cluster setup running ArubaOS 8.2.0.0.	AP Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169444	**Symptom:** BLE features such as beacon management and asset tracking did not function on a Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance. Enhancements to ble-relay resolved this issue. **Scenario:** This issue occurred because the **ble** process was not active in a Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance. This issue was observed in non-hardware controllers running ArubaOS 8.2.0.0 or earlier versions.	BLE	Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169474	**Symptom:** Some wireless clients were unable to obtain IP address after roaming to a new AP. The fix ensures that the 802.11r clients obtain the IP address. **Scenario:** This issue occurred when an 802.11r client in tunnel-mode roamed to a new AP with VLAN derivation. This issue was not limited to any specific AP model or ArubaOS release version.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
169494	**Symptom**: Clients were unable to connect to APs. The log file listed the reason for the event as **AP is resource constrained**. The fix ensures that the APs send an ageout interval to the **STM** process when the authentication is unsuccessful. **Scenario**: This issue occurred because the **STM** process was not notified after an unsuccessful authentication, which resulted in stale STA entries. 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 8.2.1.0
169526	**Symptom:** Database synchronization failed between a primary and a secondary Mobility Master. The fix ensures that database synchronization is successful. **Scenario:** This issue occurred when L2 synchronization and L3 synchronization were executed simultaneously. This issue was observed in a Mobility Master running ArubaOS 8.2.0.0.	Database	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169535	**Symptom:** A client was unable to view the custom captive portal page in a standby managed device. The fix ensures that the client can view the custom captive portal page in a standby managed device. **Scenario:** This issue occurred when a user added a new standby managed device which did not have the custom Captive Portal page. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	Database	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
169622	**Symptom:** A syslog server reported the **aruba_change_channel 512 channel 6 mode 3 not found** error for some APs. This issue is resolved by reporting the **channel-not-found** error only when the AP is not in monitoring mode. **Scenario:** This issue was observed in AP-314 and AP-315 access points running ArubaOS 8.2.0.0.	AP-Wireless	AP-314 and AP-315 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169626	**Symptom:** An unwanted attribute (FIlter-ID) was sent to the RADIUS server in the interim accounting packets by a managed device. The fix ensures that RADIUS accounting interim update does not contain Filter-Id attribute for an IPv6 client. **Scenario:** This issue occurred when RADIUS interim accounting was enabled on the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	RADIUS	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
169631	**Symptom:** The WebUI of the Mobility Master displayed an incorrect count of APs and clients. The issue is resolved by reducing the ageout time of clients from 6 minutes to 3 minutes. **Scenario:** This issue was observed in Mobility Master and managed devices running ArubaOS 8.1.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
169661	**Symptom:** The Site-to-Site crypto map failed to match the traffic selectors when the **ANY** subparameter was added to the **src-net** command. The fix ensures that the Site-to-Site crypto map matches the any-any traffic selectors. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0 versions.	IPsec	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169726	**Symptom:** An SNMP query to retrieve the total number of clients associated with a managed device returned an inflated count. This issue is resolved by ensuring that only the count of active clients associated with the managed device is retrieved. **Scenario:** The issue occurred when dormant clients were also considered while retrieving the total number of clients. Hence, the SNMP query results did not tally with the value obtained through CLI or WebUI. This was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	SNMP	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
169973	**Symptom:** Some IAP clients incorrectly derived the logon role on a Mobility Master and failed to pass traffic. The fix ensures that the Instant AP users derive the correct role. **Scenario:** This issue occurred when a heavy load was encountered in an IAP tunnel. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
170002	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred due to a race condition in the WLAN firmware. This issue was observed in 300 Series access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	300 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170056	**Symptom:** WebUI-based image upgrade for some image files using the **Local File** option failed. The fix ensures that the WebUI-based image upgrade is successful. **Scenario:** This issue occurred when the image upgrade was attempted using Chrome or Safari, but not while using Firefox. This issue was not limited to any specific platform or ArubaOS version.	Upgrade	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170085	**Symptom:** The **Transmit EIRP** values configured in the 802.11a and 802.11g radio profiles were lost and reset to the default value (15 dBm) after a managed device reload. The fix ensures that the configured **Transmit EIRP** values are retained. **Scenario:** This issue occurred only when the **Transmit EIRP** value was set to either 51 dBM or 127 dBm in the radio profile. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170116	**Symptom: Slog_flash** process crashed multiple times and generated the core files frequently. The fix ensures that the crash does not occur. **Scenario:** This issue occurred when a USB with no storage space was inserted into a 7000 Series controller. This issue was observed in 7000 Series controllers running ArubaOS 8.1.0.2 or later versions.	Cluster-Manager	7000 Series controller	ArubaOS 8.1.0.2	ArubaOS 8.2.1.0
170136	**Symptom**: An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **softlockup: hung tasks**. The fix ensures that the AP does not crash and reboot unexpectedly. **Scenario**: This issue was observed in 310 Series and 320 Series access points running ArubaOS 8.2.0.0 or later versions.	AP Datapath	310 Series and 320 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170203 170832	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **Fatal exception in interrupt @ ol_rx_flush_handler+0x40/0x118 [umac] / ol_rx_indication_handler**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-305 access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-305 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170275	**Symptom:** A logout window popped up incorrectly after a successful captive portal authentication although the **logout-popup-window** parameter was disabled in the captive portal profile. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170389	**Symptom:** When an AP rebooted, there was an increase in the number of kernel messages, with severity as critical. The fix ensures that the severity level of the kernel messages is reduced. **Scenario:** This issue was observed in APs running ArubaOS 8.1.0.4 or later versions.	AP-Platform	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0
170425	**Symptom:** Clients were requested to increase the maximum interim accounting interval, because the default timer value increased the workload of a managed device and captive portal. The issue was resolved by increasing the upper limit of timeout value to 60 minutes. **Scenario:** 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 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170522	**Symptom:** APs rebooted unexpectedly at various locations due to a random memory corruption. The fix ensures that the APs do not crash. **Scenario:** This issue was observed in access points running ArubaOS 8.0.0.0 or later versions. **Duplicates:** 167229, 167548, 167831, 167864, 168537, 168658, 168972, 168973, 169050, 169078, 169199, 169563, 169712, 170137, 170202, 170252, 170431, 170786, 170823, 170824, 170834, 170914, 170948, 171189, 171231, 171499, 171697, 171919, 171935, 172894, 172897, 172958, 172961, 173211, 173333, 173497, 173777, 173786, 173942, 173970, 174021, 174120, 174124, 174171, 174296, 174642, 174710, 174720, 175226, and 175415.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
170569	**Symptom:** Stale ARP entries were observed in the route cache table of cluster nodes. The fix ensures that stale entries are deleted appropriately. **Scenario:** This issue was observed in a cluster setup running ArubaOS 8.0.0.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
170659	**Symptom:** Sometimes, the bulk user download process failed on a cluster. The log file listed the reason for the event as, **<ERRS> |authmgr| System encountered an internal communication error. Error occurred when message is being sent from source application authmgr destination application sibyte_raw at file message.c function send_message_sibyte line 8284**. The fix ensures that the bulk user download process downloads only six users at a time to avoid this error. **Scenario:** This issue occurred when there were more than 6 user entries in a bulk user download message. This issue was observed in a cluster setup running ArubaOS 8.2.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170693 171762	**Symptom:** The following error messages were observed in managed devices in a cluster setup: **<ERRS> |authmgr| Datapath-UserAction (IPv4/L2) failed, No error handling**. The fix ensures that the error messages are not displayed unnecessarily. **Scenario:** This issue was observed in a cluster setup running ArubaOS 8.2.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170747	**Symptom:** The **arci-cli-helper** process was intermittently seen to be taking higher than usual CPU cycles. This issue is resolved by ensuring that the socket descriptor is closed when no data is received. **Scenario:** This issue occurred when existing TCP sessions to **arci-cli-helper** were not gracefully shut down due to which the socket descriptors were not cleared. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Monitoring	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170813	**Symptom:** Some clients failed to associate with an 802.1X SSID after an AP failed over to the LMS from the backup LMS. This issue is resolved by clearing the stale configuration entries in the AP driver log after a failover. **Scenario:** This issue occurred when 802.11r configuration was enabled on the backup LMS but not on the LMS. This issue was not limited to any specific managed device model or ArubaOS release version.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
170816	**Symptom:** A certificate-based Remote AP failed to come up. The fix ensures that the following events take place: ■ The Remote AP attempts authentication against all authentication servers that are part of an authentication server group. ■ The Remote AP attempts authentication starting from the first authentication server in the authentication server group if authentication fails. **Scenario:** This issue occurred when a Remote AP failed to authenticate against all authentication servers that were part of an authentication server group. Although authentication failed, the Remote AP stored the name of the last authentication server and attempted other authentication requests against the same server. This issue was observed in Remote APs running ArubaOS 8.2.0.0 or later versions.	Certificate Manager	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170872 172034 172573	**Symptom:** A Mobility Master crashed due to a memory corruption in the **AirGroup** process. The fix ensures that the memory corruption does not occur. **Scenario:** This issue occurred when a high volume of SSDP packets were received from the same MAC address but with different IP addresses. This issue was observed in Mobility Master running ArubaOS 8.1.0.3 or later versions.	AirGroup	All platforms	ArubaOS 8.1.0.3	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170903 174289	**Symptom**: APs failed to broadcast SSIDs after a managed device was upgraded. The fix ensures that the AP broadcasts the SSIDs after a managed device is upgraded. **Scenario**: This issue occurred because the SSIDs were lost whenever a broken mesh link was re-established. This issue was observed in AP-274 and AP-275 access points running ArubaOS 8.2.0.0 or later versions.	Mesh	AP-274 and AP-275 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170916	**Symptom:** The DNS server IP address was reserved as master candidates. In addition, it was displayed as HA standby even though HA is disabled. The fix ensures that the resolved IP addresses are taken as master candidate and HA standby is displayed only when HA is enabled and standby IP configuration is synchronized with the managed device. **Scenario:** This issue was observed in access points running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
170931	**Symptom:** A standby managed device displayed incorrect EIRP and MaxEIRP values for some APs. The fix ensures that the managed device displays the correct EIRP and MaxEIRP values for all the APs. **Scenario:** This issue occurred when an AP detected more than 32 neighboring radios. This issue was observed in managed devices running ArubaOS 8.2.0.1.	AP-Platform	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
170936 172424	**Symptom:** A user with AP provisioning role was unable to provision APs through the WebUI. The fix ensures that the user can provision APs through the WebUI. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
171001 171121	**Symptom:** Some stale ARP entries for clients on L2 VLAN did not age out and were found in the datapath route cache. This issue is resolved by ensuring that ARP entries are not added during OFC- or OFA-initiated ARP exchanges. **Scenario:** This issue occurred when the datapath route cache ARP entries and the kernel ARP entries were not synchronized. This issue was not limited to any specific platform or ArubaOS version.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171093	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Critical process /aruba/bin/sapd [pid 30240] DIED**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when an adhoc network advertising a valid SSID was detected by the AP under the following configuration conditions: ■ The WMS was disabled. ■ The **detect-valid-ssid-misuse** and **protect-ssid** parameters were enabled in the **ids unauthorized-device-profile**. This issue was observed in AP-325 access points running ArubaOS 8.0.0.0 or later versions.	Air Management - IDS	AP-325 access points	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
171099	**Symptom:** The standby User Anchored Controllers (S-UAC) in a cluster setup failed to track the correct VLAN usage count for dormant clients. The fix ensures that the VLAN usage counters are updated correctly. **Scenario:** This issue occurred when redundancy was enabled. This issue was observed in a cluster setup running ArubaOS 8.2.0.0 or later versions.	Station Management	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
171230	**Symptom:** Clients experienced intermittent packet loss. This issue is resolved by setting a limit on the number of retries when the client is unresponsive. **Scenario:** This issue occurred when some clients did not send a deauthentication or disassociation request to an AP and became unresponsive. The AP attempted to communicate with the unresponsive clients and created an RTS and BAR storm in the network. Hence, other clients in the network experienced intermittent packet loss. This issue was observed in AP-205, AP-215, and AP-225 access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-205, AP-215, and AP-225 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
171233	**Symptom:** A Site-to-Site VPN failed to come up. The fix ensures that the datapath route-cache entry is deleted when the corresponding security association related to a 32-bit destination network mask is deleted and the Site-to-Site VPN comes up as expected. **Scenario:** This issue occurred when the IKE/IPsec security association related to a 32-bit destination network mask was broken but the corresponding datapath route-cache entry persisted. This issue was observed in managed devices running ArubaOS 8.1.0.0.	IPsec	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171241	**Symptom:** Users were not allowed to enter IPsec key length that exceeded 7-8 characters. This issue is resolved by making internal code changes that allows 6-64 characters. **Scenario:** This issue occurred when a user tried to configure an IPv4 or IPv6 address of a managed device for PSK authentication. This issue was observed in a managed device running ArubaOS 8.2.0.1.	WebUI	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171316	**Symptom:** An error, **dot1x_gsm_set_pmkcache(): GSM: Failed to publish PMK-cache object. Error:error_no_free_slots** was frequently displayed on a managed device when PMK cache GSM channel was full. The fix ensures that the error message is not displayed on the managed device. **Scenario:** This issue was observed in a cluster setup running ArubaOS 8.2.0.1.	Base OS Security	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171324	**Symptom:** Some authentication servers disappeared from the server group that was configured on a managed device. The fix ensures that re-ordering the servers or server rules in a server group does not delete the authentication servers. **Scenario:** This issue occurred when authentication servers or server rules in a server group were re-ordered from the Mobility Master WebUI. This issue was observed in managed devices running ArubaOS 8.2.0.1.	Configuration	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171347 173138	**Symptom:** In the WebUI, the APs operating in AM mode were not counted in the **Configurations > AP Group** page of the managed device although the status of these APs were displayed as UP in the **Dashboard > Access Points** page of the Mobility Master. The fix ensures that the APs are counted in the **Configurations > AP Group** page. **Scenario:** This issue occurred when APs changed to AM mode. This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.	Monitoring	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171382 174540	**Symptom:** The signal strength of the 2.4g radio in an AP reduced to a low value unexpectedly. The fix ensures that the AP retains the correct radio signal strength. **Scenario:** This issue was observed in AP-207 access points running ArubaOS 8.1.0.4.	AP-Platform	AP-207 access points	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171392	**Symptom:** Configuration involving netdestinations and ACLs using netdestinations caused a datapath module crash on a managed device. The fix ensures that the process does not crash. **Scenario:** This issue occurred due to the debug statements that were printed when the ACLs were applied on the traffic. This issue was observed in managed devices running ArubaOS 8.2.0.1.	Controller-Datapath	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171398	**Symptom:** The captive portal page did not display the correct background and also the image was missing. The fix ensures the captive portal page displays the correct background and the image. **Scenario:** This issue occurred when the captive portal profile name exceeded the maximum limit. This issue was observed in a managed device running ArubaOS 8.2.0.0 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
171411 175624	**Symptom:** An unexpected STM runtime error was displayed in the logs. The fix ensures that the error log is printed only when there is a valid error code. **Scenario:** This issue occurred when the ARM statistics health update was in progress. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Station Management	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171433 173001	**Symptom:** The **show running config** command output indicated that ADP was enabled on a managed device though it was disabled from the Mobility Master. This issue is resolved by ensuring that the **STM** process is updated correctly after a restart. **Scenario:** This issue occurred either after an **STM** process restart or when a managed device rebooted. This issue was observed in a Mobility Master running ArubaOS 8.0.1.0 or later versions.	Station Management	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171498	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **AP process crash (core file: core.rapper.18-64-72-cf-e6-62.AP-334.62115)**. The fix ensures that the AP drops the unwanted IKE request packets to avoid the crash. **Scenario:** This issue occurred when the AP was flooded with VPN requests. This issue was observed in AP-334 and AP-335 access points running ArubaOS 8.2.0.1.	AP-Platform	AP-334 and AP-335 access points	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171502	**Symptom:** The **ip helper-address** command failed when executed on non-device nodes from a Mobility Master. The fix ensures that the **ip helper-address** command can be executed from non-device nodes. **Scenario:** This issue occurred because the command could be executed only on device nodes. This issue was observed in a Mobility Master running ArubaOS 8.2.0.1 or later versions.	DHCP	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171580 172626	**Symptom:** When a user upgraded from ArubaOS 8.2.0.0. to ArubaOS 8.2.0.1, an AP entry appeared twice in the aggregation node level. The fix ensures that there is only entry in the aggregation node level**.** **Scenario:** This issue occurred because the **Mon-serv** manager updated an existing AP as well as created it once again in the monitoring database. This issue was observed in a cluster setup with APs terminating on them, but is not restricted to any specific ArubaOS version.	Monitoring	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171582	**Symptom:** The allowed VLAN list on a port channel interface was missing from a managed device after upgrading the image and executing the **ccm-debug full-config-sync** command for a full configuration synchronization. The fix ensures that the allowed VLAN list on the port channel is displayed after upgrading the image. **Scenario:** This issue occurred when a managed device was upgraded from ArubaOS 8.1.0.1 to ArubaOS 8.1.0.4. The issue was observed in managed devices running ArubaOS 8.1.0.4.	Configuration	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0
171587	**Symptom:** A managed device falsely detected a FATA-jack attack and raised an IDS event for clients that used 802.11r and initiated a re-association request. This issue is resolved by checking for authentication algorithm values greater than 3. **Scenario:** This issue was observed when 802.11r (Fast BSS Roaming) was enabled and supported clients roamed using WPA authentication algorithm 2. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Air Management - IDS	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171614 172310 174525 175401	**Symptom:** The **datapath** process on a managed device crashed. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the **datapath** process does not crash due to invalid memory access. **Scenario:** This issue occurred due to an invalid memory access. This issue was observed in managed devices running ArubaOS 8.1.0.4.	Controller-Datapath	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0
171680	**Symptom:** A Mobility Master lost the masterip configuration for devices after upgrading. Due to this, the managed device became the Master from standby. The fix ensures that the device synchronization is successful. **Scenario:** This issue was observed in a cluster setup running ArubaOS 8.1.0.4.	Configuration	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0
171705	**Symptom:** The RADIUS authentication failed after upgrading a Mobility Master to ArubaOS 8.2.0.1 when managed devices are in a cluster. The fix ensures that the RADIUS authentication is successful. **Scenario:** This issue occurred when configuring **aaa** authentication servers for managed devices. This issue was observed in a cluster setup running ArubaOS 8.2.0.1.	RADIUS	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171733	**Symptom:** The output of the **kernel coredump** command displayed an error when executed on a Mobility Master. This issue is resolved by increasing the crash kernel memory. **Scenario:** This issue occurred when the configuration was sent to the managed devices using the **kernel coredump** command. This issue was observed in managed devices running ArubaOS 8.2.0.1.	Controller-Datapath	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171819	**Symptom:** Clients connecting to an AP failed to load the captive portal page. The fix ensures that the captive portal page loads successfully. **Scenario:** This issue occurred when the AP was configured as a Remote AP in split-tunnel forwarding mode. This issue was observed in 200 Series, 300 Series, 310 Series and 320 Series access points running ArubaOS 8.2.0.1.	AP Datapath	200 Series, 300 Series, 310 Series and 320 Series access points	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171931	**Symptom:** Some APs reported a high packet rate value for the uplink traffic in the AMON message. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred because of inconsistent handling of NULL frames in the Rx data statistics. This issue was observed in 300 Series, AP-303H, 310 Series, 320 Series, 330 Series, and 360 Series access points running ArubaOS 8.2.0.1 or later versions.	AP-Wireless	300 Series, AP-303H, 310 Series, 320 Series, 330 Series, and 360 Series access points	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
171976	**Symptom**: The output of the **show ap debug radio-stats** command did not display accurate counter values. The fix ensures that accurate values are displayed. **Scenario**: This issue occurred when 802.11ac and 802.11n clients were connected to APs. This issue was observed in AP-207 access points running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	AP-207 access points	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172095	**Symptom:** Sometimes, the crash directory was missing from 7200 Series controller. This issue is resolved by moving all crash files to a fixed location. **Scenario:** This issue occurred when a process in a 7200 Series controller crashed. This issue was observed in 7200 Series controllers running ArubaOS 8.0.0.0 or later versions.	Controller-Platform	7200 Series controllers	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172243 175921	**Symptom:** Although LLDP-MED configuration was enabled on all ports of an AP, it was disabled for ports E1 through E3. The fix ensures that LLDP-MED is enabled for ports E1 through E3. **Scenario:** This issue was observed in AP-303H access points running ArubaOS 8.2.0.1 or later versions.	AP-Platform	AP-303H access points	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
172279 175985	**Symptom:** Clients were unable to pass captive portal authentication. The fix ensures that the clients are able to pass captive portal authentication. **Scenario:** 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 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172388	**Symptom:** A managed device failed to download certificates from the Mobility Master. The fix ensures that the certificates are imported to the managed device. **Scenario:** This issue occurred due to a mismatch in the object type defined in XML and profile manager. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	Certificate Manager	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172462 173388	**Symptom**: The **Managed Network > Dashboard > Access Points** page in the WebUI displayed the status of an AP as UP although the AP was DOWN. The fix ensures that the WebUI does not display UP for the APs that are DOWN. **Scenario**: This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172468	**Symptom:** A client failed authentication against a RADIUS server. Enhancements made to the **authentication** process resolved this issue. **Scenario:** This issue occurred when the **authentication** process in a managed device could not assign a sequence-number to a RADIUS request. As a result, the managed device did not sent RADIUS requests to the RADIUS server. This issue was observed in managed devices running ArubaOS 8.1.0.0.	RADIUS	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
172506	**Symptom:** A managed device discarded the first TCP SYN packet when a client connected to an FTP server. The fix ensures that the managed device does not discard the first TCP SYN packet. **Scenario:** This issue occurred in a managed device with DPI enabled. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172610 173537 174713 176560	**Symptom:** AP was not seen on a backup LMS, when both the active and standby LMS were rebooted and the backup LMS was restored with HA enabled. The fix ensures that the AP comes up on both the primary and backup LMS after a reboot. **Scenario:** This issue was observed when both the active and standby LMS were disconnected. This issue is not restricted to any controller model or ArubaOS version.	AP-Platform	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172638 174128	**Symptom:** A managed device rebooted multiple times. The log file listed the reason for the event as **Datapath timeout**. The fix ensures that the reboot does not occur. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
172647 172786	**Symptom:** A user was unable to move an existing configuration node to a new node. The fix ensures that the user is able to move a configuration node. **Scenario:** This issue occurred when the encrypted password was sent for validation. This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.	Configuration	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
172703	**Symptom:** A Remote AP attempted to obtain an IPv6 address even though it had already obtained an IPv4 address. Hence the Remote AP failed to boot. The fix ensures that the Remote AP boots when it obtains either an IPv4 address or an IPv6 address. **Scenario**: This issue occurred in Remote APs with dual-stacked FQDN containing both IPv4 and IPv6 addresses. This issue was observed in Remote APs running ArubaOS 8.2.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172709 175404 176375	**Symptom:** The **Dashboard** > **Access Points** page on a Mobility Master failed to display the radio statistics for an AP. The fix ensures that the AP and radio statistics are displayed correctly. **Scenario:** This issue occurred because the status of the AP was DOWN when the Mobility Master monitoring database processed the radio statistics. This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	Monitoring	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172740	**Symptom**: The **Dashboard > Controllers** and **Configuration > Controllers** page of the WebUI displayed an incorrect status of managed devices. The fix ensures that the WebUI displays the correct status of the managed devices. **Scenario**: This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172758	**Symptom:** The AP image preload operation failed when executed from a managed device. The fix ensures that the AP image preload operation works as expected. **Scenario:** This issue was observed in 7240 controllers running ArubaOS 8.1.0.0.	Controller-Platform	7240 controllers	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
172763	**Symptom:** A Mobility Master stopped sending traps to AirWave when the SNMP V3 Engine ID was configured. The fix ensures that the Mobility Master sends traps to AirWave. **Scenario**: This issue occurred when the SNMP V3 Engine ID value started with 8. This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	SNMP	Mobility Master	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
172788	**Symptom:** A query on the following SNMP OIDs each reported an incorrect value of zero: ■ **monAPInfoMonitorTime - 1.3.6.1.4.1.14823.2.2.1.6.7.1.1.1.6** ■ **monAPInfoInactivityTime 1.3.6.1.4.1.14823.2.2.1.6.7.1.1.1.7** The fix ensures that the query displays the correct value. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Air Management-IDS	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
172803	**Symptom:** Clients were unable to connect to an AP. The log file listed the reason for the event as **UAC Down**. The fix ensures that the clients successfully connect to an AP. **Scenario:** This issue occurred when the LMS IP was configured as the VRRP IP with AP load balancing enabled. This issue was observed in a cluster setup running ArubaOS 8.1.0.4.	AP Datapath	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0
172877	**Symptom:** A managed device rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172959	**Symptom:** The **Profmgr** process displayed as busy for few minutes on a managed device. The fix ensures that the **Profmgr** process state is displayed correctly. **Scenario:** This issue occurred when the **show config datastore** command was executed on the managed device. This issue was observed in managed devices running ArubaOS 8.1.0.4 or later versions.	Configuration	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0
173009	**Symptom:** VIA profile failed to download on a stand-alone controller after establishing a VPN connection. This issue is resolved by adding correct logic to check the VIA license in the **authentication** process. **Scenario:** This issue was observed in 7005 stand-alone controllers running ArubaOS 8.2.0.1 or later versions.	IPsec	7005 controllers	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
173145	**Symptom:** A timer on an AP expired in advance after a cluster failover caused the **SAPD** process to crash. The fix ensures that the **SAPD** process does not crash due to a cluster failover. **Scenario:** This issue occurred when an AP failed over to a backup LMS and then detected the LMS. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.2.1.0
173360	**Symptom:** Source NAT application was not effective on the voice traffic. The fix ensures that source NAT is effective for the voice traffic when OpenFlow is enabled. **Scenario:** This issue occurred when OpenFlow was enabled on a Mobility Master. This issue was observed in a Mobility Master running ArubaOS 8.0.0.0 or later versions.	SDN-Platform	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
173404	**Symptom:** A managed device was unable to download the configuration from a Mobility Master and displayed the error, **CONTROLLER-IP/V6 NOT SET**. The fix ensures that the managed device is able to download the configuration file seamlessly. **Scenario:** This issue occurred only when controller-ip is configured for a managed device through a bulkedit CSV file. This issue was observed in a Mobility Master running ArubaOS 8.1.0.0 or later versions.	Controller - Platform	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173427	**Symptom:** APs displayed up with an ID flag in the AP database. The log file listed the reason for the event as **Error: Duplicate LLDP-MED application type "voice"**. The fix ensures that APs do not come up with an ID flag. **Scenario:** This issue occurred due to two voice applications in the AP LLDP profile. This issue was observed in access points running ArubaOS 8.1.0.2.	AP-Platform	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.2.1.0
173436	**Symptom:** The **mcellsolverstart** process crashed in a Mobility Master unexpectedly. This issue is resolved by updating the DB schema. **Scenario:** This issue occurred as the DB schema in the Mobility Master was outdated. This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	AirMatch	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
173468 173567 173656 173697 173922	**Symptom**: An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception NIP [e2dd2424] set_eth_loopback+0x1484/0x2060 [asap_mod]**. The fix ensures that the AP does not crash and reboot. **Scenario**: This issue was observed in AP-335 access points running ArubaOS 8.2.0.2 or later versions.	AP Datapath	AP-335 access points	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
173535	**Symptom:** Users were unable to log into a Mobility Master using the WebUI. The issue is resolved by automatically rebooting the Mobility Master when the storage disk is remounted in read-only mode. **Scenario:** This issue occurred because the VM server storage disk was remounted in read-only mode on the Mobility Master Virtual Appliance due to disk timeouts. This issue was observed in Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance running ArubaOS 8.0.0.0 or later versions.	Controller-Platform	Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
173990	**Symptom:** A user was unable to upload a VIA installer package using the **Configuration > Services > VPN > VIA** page of the WebUI. The fix ensures that the VIA installer package upload is successful. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.2.	WebUI	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174017	**Symptom:** The **halt** command did not work in a managed device. The fix ensures that the **halt** command works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
174193	**Symptom:** The **Configuration** > **Task** > **Provision new Campus APs** page displayed the message **AP Provisioning is currently being managed by Clearpass**. The fix ensures that the message is not displayed. **Scenario:** This issue occurred when the **default-cap** or **default-rap server-group** configuration was changed. This issue was observed in managed devices running ArubaOS 8.2.0.1 or later versions.	WebUI	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
174280	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **TIMED OUT WAITING FOR STOPPED EVENT**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-334 access points running ArubaOS 8.2.0.2 or later versions.	AP-Wireless	AP-334 access points	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
174375	**Symptom:** A managed device failed to update the syslog server. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when a managed device created incorrect log entries and the log file size increased. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.2.1.0
174534	**Symptom**: HPE switches using the factory or TPM certificates were unable to establish an IPsec connection with a managed device. The fix ensures that the HPE switches can establish an IPsec connection with a managed device. **Scenario**: This issue occurred because the Certificate Policies extension OID of the HPE switch did not match with the preferred OIDs on the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174611	**Symptom:** The IPM priority was displayed incorrectly in the WebUI of a Mobility Master. The fix ensures that the IPM priority is displayed correctly in the WebUI. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.2.0.2.	Configuration	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
174744	**Symptom:** The server certificate was not deleted when the web-server profile was deleted. The fix ensures that the server certificate is deleted. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.2.	Certificate Manager	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
174746	**Symptom:** Clients failed to receive RAs when the IPv6 proxy RA was enabled on a managed device. The issue is resolved by prioritizing the RA traffic appropriately. **Scenario:** This issue occurred because the IPv6 router solicitation packets were discarded when the managed device was overloaded with untrusted multicast traffic. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	IPv6	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
174756 174088	**Symptom:** Some Windows clients did not connect to an AP with VHT capabilities. The fix ensures that the clients connect to the AP that has VHT capabilities. **Scenario:** This issue occurred when a virtual AP was created in legacy mode without HT/VHT. This issue was observed in access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
174823 175163	**Symptom:** The **authentication** process crashed unexpectedly. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the **aaa test-server verbose** command was executed. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
174864 175413 175448 175549	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when DPI was enabled. This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Datapath	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174943	**Symptom:** The **tx rate** value was displayed incorrectly when the **show ap debug radiostats** command was executed. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 300 Series, 310 Series, 320 Series, and 330 Series access points running ArubaOS 8.2.0.1 or later versions.	AP-Wireless	300 Series, 310 Series, 320 Series, and 330 Series	ArubaOS 8.2.0.1	ArubaOS 8.2.1.0
174979	**Symptom:** The size of the **ale.log** file increased on a Mobility Master. This issue is resolved by updating only the consolidated data to the **ale.log** once a day. **Scenario:** This issue occurred due to frequent processing of AMON messages. This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	NBAPI	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
175060	**Symptom:** The **Dashboard > Performance** page of a Mobility Master displayed the most significant digit of the total client count. The fix ensures that the **Dashboard > Performance** page displays the correct client count. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.2.0.0.	WebUI	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0
175120	**Symptom:** The output of the **show ip route** command displayed a client's IP route address in reverse order. The fix ensures that the IP route address is displayed in correct order. **Scenario:** This issue occurred due to missing endianness of the IP route address in the Mobility Master Virtual Appliance. This issue was observed in a Mobility Master Virtual Appliance running ArubaOS 8.2.0.2 or later versions.	IPsec	Mobility Master Virtual Appliance	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
175126 175128	**Symptom:** A Mobility Master incorrectly deleted the certificates uploaded in flash when deleting them from a child node device that had inherited these certificates. The fix ensures that an error is displayed when trying to delete an inherited certificate from a child node. **Scenario:** This issue occurred when there was no reference to the certificate being deleted in the local node. This issue was observed in a Mobility Master running ArubaOS 8.2.0.0 or later versions.	Certificate Manager	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.2.1.0

Table 6: *Resolved Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175240	**Symptom:** The **CTF MAC** field in the output of the **show ap remote debug uac-list** command displayed incorrect values. The fix ensures that the **CTF MAC** field displays the correct values. **Scenario:** This issue was observed in access points running ArubaOS 8.2.0.2.	AP Datapath	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
175475 175727	**Symptom:** The **mDNS** process in a managed device displayed high memory utilization. This issue is resolved by sending ClearPass Policy Manager requests only for AirGroup users. **Scenario:** This issue occurred when AirGroup was disabled but a ClearPass Policy Manager request was sent for each authenticated user. This lead to a memory leak. This issue was observed in managed devices running ArubaOS 8.2.0.2.	AirGroup	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0
175937	**Symptom:** A managed device crashed and rebooted unexpectedly without collecting the crash information. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:40:2)**. The fix ensures that the USB does not disconnect while collecting the core dump. **Scenario:** This issue occurred when the USB got disconnected while collecting the core dump. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.2.1.0
176183	**Symptom:** The **mDNS** process crashed on a Mobility Master Virtual Appliance. This fix ensures that the **mDNS** process does not crash. **Scenario:** This issue occurred when a high memory address range was assigned to the timer. This issue was observed in a Mobility Master Virtual Appliance running ArubaOS 8.2.0.2.	AirGroup	Mobility Master Virtual Appliance	ArubaOS 8.2.0.2	ArubaOS 8.2.1.0

This chapter describes the issues identified in this release.

Table 7: *Known Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version
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
160551	**Symptom:** An AP keeps declaring a stale IP as the master, and fails to come up even after purging the stale master IP from the AP boot environment variables. **Scenario:** This issue occurs because the AP restores all the cleared variables due to a backup restore feature. This issue is observed in APs running ArubaOS 8.1.0.0 or later versions. **Workaround:** Execute the **bootenv_backup.sh** script to clear the saved record.	AP-Platform	All platforms	ArubaOS 8.1.0.0
167288	**Symptom:** A stand-alone controller does not display the wired client icon, list, and count of users in the WebUI. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.2.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.2.0.0
168180	**Symptom:** The **profmgr** process crashes when a 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
168636	**Symptom:** Clients are unable to connect to a 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

Table 7: *Known Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version
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-Redund-ancy	All platforms	ArubaOS 8.2.0.0
169827	**Symptom:** Encapsulated ARP packets with inner payload size lesser than 64 bytes are dropped by an Aruba HPE switch. **Scenario:** This issue occurs when the Aruba HPE switch is connected to a wired tunnelled node port of a managed device. This issue is observed in managed devices running ArubaOS 8.1.0.4. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.1.0.4
170611	**Symptom:** A user is unable to disable TLS 1.0 and TLS 1.1 versions on a FIPS build within SSL protocol. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Web Server	All platforms	ArubaOS 8.2.0.0
171611	**Symptom:** A crypto map is incorrectly picked during IKE and IPsec negotiation on a managed device if **vpn-peer peer-mac** command is configured along with **masterip** and **vpnip** commands pointing to the same MAC address. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.4. **Workaround:** Execute the **no vpn-peer peer-mac** command on the managed device.	IPsec	All platforms	ArubaOS 8.1.0.4
172534	**Symptom:** WEP clients are unable to pass traffic on cluster failover and switchover to standby mode. **Scenario:** This issue occurs when the clients are connected to static or dynamic WEP-enabled WLAN in a cluster deployment. This issue is observed in a cluster setup running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version
173083	**Symptom:** When configured as redundant Mobility Master, the label for the Mobility Master is incorrectly displayed as **Mobility Controller** in the WebUI. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.2.0.1. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.2.0.1
173816	**Symptom:** A managed device displays the **500 Internal Server Error** message when a user attempts local file upgrade. **Scenario:** This issue occurs with some image file sizes. This issue is observed in managed devices running ArubaOS 8.2.0.1 **Workaround:** Use SCP, FTP, or TFTP to upgrade the managed devices.	Image Upgrade	All platforms	ArubaOS 8.2.0.1

174644
174925
	Symptom: AirGroup loses all the learned server and user details and also fails to learn any new user or server details.
	Scenario: This issue occurs whenever an AirGroup service or profile is modified. This issue is observed in ArubaOS 8.2.0.0 or later versions.
	Workaround: Re-enable AirGroup on the node by using the following commands:
	`no airgroupprofile activate`
	`!`
	`airgroupprofile activate airgroupprofile <profile-name > mode <mode>`
	`!`
		AirGroup	All platforms	ArubaOS 8.2.0.2

Table 7: *Known Issues in ArubaOS 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version
174788	**Symptom:** A Mobility Master incorrectly allows users to execute the **aaa user delete** command from the **/mm** or **/mm/mynode** levels. However, the command is not effective because it is applicable only at the managed device level **(/md/<device>)**. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** Execute the **aaa user delete** command from a managed device.	Base OS Security	All platforms	ArubaOS 8.0.0.0
176444	**Symptom:** The startup wizard does not allow adding licenses to a stand-alone controller. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.2.1.0. **Workaround:** None.	Controller - Platform	All platforms	ArubaOS 8.2.1.0

176998	**Symptom:** The client traffic is dropped when the **enforce-dhcp** parameter is enabled.
	Scenario: This issue occurs when clients roam from one AP to another AP that terminates on a different managed device and has no context of the client. The client does not initiate DHCP discovery after authentication, but sends traffic which is dropped by the managed device.
	Workaround:
	1. Disable **enforce-dhcp** parameter in the AAA profile using either the WebUI or the CLI:
	WebUI
	In the Managed Network node hierarchy, navigate to **Configuration > Authentication > AAA Profile**.
	Select an AAA Profile and clear the **Enforce DHCP** check box.
	CLI:
	Execute the following commands in the CLI:
	`(host) [mynode] (config) # aaa profile <default>`
	`(host) [mynode] (AAA Profile "<default>") # no enforce-dhcp`
	2. Renew the DHCP lease on the client if the traffic is blocked.
		Base OS Security	All platforms	ArubaOS 8.2.1.0

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

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

Topics in this chapter include:

Migrating Licenses from ArubaOS 8.0.x to ArubaOS 8.2.x

If you are migrating from ArubaOS 8.0.x to ArubaOS 8.2.x, migrate the MC-VA licenses if the country type is restricted (US, JP, IL, EG).

Manually delete and add all MC-VA licenses after upgrading to the new ArubaOS version.

- Upgrade from ArubaOS 8.0.1.x or later releases.
  - No change if MC-VA license is not used.
  - If country type is one of restricted country type (US, JP, IL, EG), there is no country lock behavior.
  - Aruba recommends to upgrade to ArubaOS 8.1.0.0 for the country lock feature.
- New order in ArubaOS 8.0.1.0
  - After My Networking Portal (MNP) is updated based on the new country lock, use the part numbers that are part of ArubaOS part 8.1.0.0.
  - Use only MC-VA-XX-RW from MNP.
  - In ArubaOS 8.0.1 MC-VA-XX-US, MC-VA-XX-JP, MC-VA-XX-IL, MC-VA-XX-EG country licenses cannot be used after MNP update.

- Transfer to ArubaOS 8.0.1.x
  - Applicable in case of RMA of ArubaOS 8.0.1.x.
  - Transfer of license from MNP is supported only for RW license type.
- Upgrade from ArubaOS 8.0.1.x to ArubaOS 8.1.x
  - If you have configured one of the restricted country type (US, JP, IL, EG):
    - The existing licenses are considered as RW licenses. APs will be in unlicensed state for the restricted country types (US, JP, IL, EG).
    - Delete the existing MC-VA license.
    - Obtain a new license from MNP according to the country based on the order.
    - Apply the new license on standalone controller or Mobility Master to get country lock MC-VA.
    - Licenses other than MC-VA are not impacted.
  - If you have configured any country apart from the restricted country type (US, JP, IL, EG):
    - Existing licenses are considered as RW licenses.
    - APs will advertise the channels based on country if previous license are present.
    - No impact for non-restricted country types.

Important Points to Remember

To upgrade your managed device or Mobility Master:

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of the network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** page in the WebUI, or by executing the **show ap active** or **show ap database** commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS runs on your managed device have?
  - 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, refer *Aruba Mobility Master Licensing Guide*.

Memory Requirements

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

- Do not proceed with upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with 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 space, free some used memory. Copy any log files, crash data, or flash backups from your managed device, to any desired location. Delete the following files from the managed device to free some memory before upgrading:
  - **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 65 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 65 to back up the flash directory to a file named **flash.tar.gz**, and then 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 65 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 card. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

Deleting a CLI

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
- Flashbackup

Backing up and Restoring Compact Flash Memory

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

In the WebUI

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

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

Upgrade ArubaOS using the WebUI or CLI

The following sections provide the procedures for upgrading your WLAN network to the latest ArubaOS version 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 64.

NOTE

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

Before you upgrade Mobility Master from ArubaOS 8.0.0.0 to ArubaOS 8.2.0.0, take a note of the following points:

- ArubaOS 8.2.0.0 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 8.2.0.0 to avoid upgrade failure. To remove a network adapter from ArubaOS 8.0.0.0 Mobility Master Virtual Appliance:

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.

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 8.2.0.0 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 8.2.1.0, 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 a local file.

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

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded at the factory. The Mobility Master or the 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 does not take effect until reboot. If you choose to reboot after upgrade, Mobility Master or the managed device reboots automatically.

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

In the CLI

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

1. Download ArubaOS image from the customer support site.
2. Open an SSH session on 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
```

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

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

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 number. 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 device 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 65 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 the APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory, to an external server or mass storage facility. See Backing up Critical Data on page 65 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.

Before You Begin

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 65.
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.