ArubaOS 8.4.0.0

aruba
a Hewlett Packard
Enterprise company

Release Notes

Open Source Code

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

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

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 05	Removed the **Migrating from ArubaOS 6.x to ArubaOS 8.x** section from **Upgrade Procedure** chapter as the Migration Tool is no longer supported.
Revision 04	Added a note regarding MU-MIMO support in 510 Series APs.
Revision 03	Added a limitation regarding Role Based VLAN for issue, 181826.
Revision 02	■ Added description for known issue, 194140. ■ Removed description of known issue, 188600.
Revision 01	Initial release.

This ArubaOS release notes includes the following topics:

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

For the list of terms, refer Glossary.

Related Documents

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

- *ArubaOS Getting Started Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- Aruba *Mobility Master Licensing Guide*
- *Aruba Virtual Appliance Installation Guide*
- *Aruba Mobility Master Hardware Appliance Installation Guide*

Important Points

This section describes the important points to remember before you upgrade the managed device to this release of ArubaOS.

- If you use an image server to upgrade the managed device from the CLI, you must configure an upgrade profile on the Managed Network node.
- Ensure that the IANA timezone is configured exactly the same for each managed device. All the network nodes have to be NTP synchronized.

- Time changed manually in a managed device is not automatically adjusted for a scheduled upgrade.
- DST time change hour is not automatically adjusted for a scheduled upgrade.

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

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

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

AirGroup

AP Name

The **show airgroup aps** command is modified to list the name of the neighbor AP, if available, in the **Neighbor AP name** parameter. If the name of the neighbor AP name is not available, the BSSID of the neighbor AP is listed.

Air Management - IDS

Legend Alphabetizing

Starting from ArubaOS 8.4.0.0, the output legends like flags and statuses for the command, **show ap debug client-table** is sorted in alphabetical order to increase readability.

AMON

Support for Smart AMON

AMON feeds are now made programmable and cloud friendly to help minimize the AMON telemetry traffic between the controller and the Cloud.

This feature enables the following new capabilities to the AMON feeds to Cloud destination over Websockets:

- Tuned for per-destination-tuned low-over head AMON feeds
- Cloud bootstrapping support
- AMON feed compression

AP Platform

IEEE 802.11ad Support

IEEE 802.11ad, also known as WiGig, is a multi-gigabit Wi-Fi technology that allows managed devices to communicate at multi-Gigabit speeds over a 60 GHz frequency band. This technology comprises of two radios, 5 GHz and 60 GHz.

IEEE 802.11ax Support

IEEE 802.11ax, also known as High-Efficiency WLAN (HEW), is a multi-gigabit Wi-Fi technology that allows managed devices to communicate on both the 2.4 GHz and 5 GHz frequency bands. This technology improves spectrum efficiency and area throughput in dense deployment scenarios of APs or stations in both indoor and outdoor environments.

510 Series Campus Access Points

The 510 Series Campus Access Points is categorized under **Early Availability** release. Refer to the following section, for a list of features that are targeted for a future release.

The Aruba 510 Series Campus APs (AP-514 and AP-515) are high-performance, multi-radio wireless devices that can be deployed in either controller-based (ArubaOS) or controller less (Aruba Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting legacy 802.11a/b/g/n/ac wireless services.

The Aruba 510 Series Campus APs are equipped with an integrated BLE and Zigbee radio that provide the following capabilities:

- Location beacon applications
- Wireless console access
- IoT gateway applications

Ethernet ports on the access points are used to connect the device to the wired networking infrastructure and provide (802.3at class 4) PoE power to the device. The access points are equipped with a USB-A port that is compatible with selected cellular modems and other peripherals. When active, this port can supply up to 5W/1A to a connected device.

The 510 Series Campus Access Points do not support UL MU-MIMO and DL MU-MIMO.

The following features are targeted for future releases and are currently not supported on the Aruba 510 Series Campus APs:

- Orthogonal Frequency Division Multiple Access (OFDMA)
- Transmit Beam Forming (TxBF)
- BSS Coloring
- Target Wait Time (TWT)
- Multi Band Operation (MBO)
- Spectrum analysis
- Mesh
- Cellular modem support
- 512 associated clients per radio (currently limited to 230 clients)

For complete technical details see the *Aruba 510 Series Campus APs Datasheet*. For installation instructions, see the *Aruba 510 Series Campus APs Installation Guide*.

AP-303P Campus Access Points

The AP-303P access point is a high-performance dual-radio wireless device that supports IEEE 802.11ac Wave 2 standard. This AP uses MU-MIMO (Multi-User Multiple-Input, Multiple-Output) technology to provide secure wireless connectivity for both 2.4 GHz 802.11 b/g/n/ac and 5 GHz 802.11 a/n/ac Wi-Fi networks.

This AP provides the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatibility with IEEE 802.3af/at/bt PoE
- Supports PoE (E1 port) with PSE power
- Integrated BLE/Zigbee radio

For complete technical details, see the *Aruba 303 Series Campus Access Points datasheet*. For installation instructions, see the *Aruba AP-303P Campus Access Points Installation Guide*.

AP-387 Access Points

The AP-387 outdoor access points are high-performance dual-radio wireless devices that support IEEE 802.11ad Wave 2 standard. This AP uses MU-MIMO (Multi-User Multiple-Input, Multiple-Output) technology to provide secure mesh connectivity for both 5 GHz 802.11a, 802.11n, and 802.11ac, and 60 GHz 802.11ad Wi-Fi networks. The AP-387 series access points can be deployed in either a controller-based (ArubaOS) or controller-less (InstantOS) network environment.

This AP provides the following capabilities:

- Point-to-point mesh deployment in 60 GHz and 5 GHz radios
- Compatibility with IEEE 802.3af and IEEE 802.3at PoE power sources
- Integrated BLE radio

AP-387 does not support wireless access.

For complete technical details and installation instructions, see *Aruba AP-387 Series Outdoor Access Points Installation Guide*.

NetInsight Integration with AirMatch

ArubaOS is now integrated with NetInsight, Aruba's Network Analytics and Assurance solution. The analytics engine in NetInsight can push radio profile EIRP recommendations, channel-bandwidth recommendations, and regulatory domain profile recommendations to an AP. The following command is introduced as part of this feature:

- **show ap analytics recommendations**

IP Conflict Detection

Starting from this release, APs can detect and resolve an IP conflict.

Green AP

ArubaOS now supports a power saving feature, where based on NetInsight inputs, the feature dynamically enables, disables, or reduces functionality of an allocated AP to reduce the consumption of energy.

510 Series access points support the Green AP feature.

Support for Channels 169 and 173

ArubaOS supports channel 169 and 173 for outdoor APs on 5 GHz band subject to country compliance rules.

Support for Inseego U730L 4G Modem

ArubaOS 8.4.0.0 supports Inseego U730L 4G modems for Verizon network on Mobility Controllers and Remote APs. AP-203R, AP-203RP, and AP-303H access points support the U730L modem.

The U730L modem must be setup in the enterprise mode before it can be plugged into the USB port of an AP, managed device, or Mobility Controller.

To enable the U730L modem in enterprise mode:

1. Plug the U730L modem into a laptop running Windows or MacOS and ensure that the wireless adapter is U730L.
2. Navigate to http://my.usb/labtestinfo in a web browser.
3. Click **Enterprise Mode**.
4. Click **OK** in the pop-up window.

Wait for the U730L modem to reboot and come up before unplugging it from the laptop.

Support for Wired AP Mode

ArubaOS supports **Wired AP mode** to bridge the port E1 and port E0 wired traffic.

Support for ZTE MF861 4G Modem for AT&T network

ArubaOS 8.4.0.0 supports ZTE MF861 4G modems for AT&T network on Mobility Controllers and Remote APs.

WIDS

You can configure to reduce the number of frames copied for the purpose of WIDS aggregate MPDU optimization from the AP system profile.

WMM DSCP mapping

Starting from this release, the WMM DSCP mapping supports IPv6 packets only in the upstream direction of the decrypt tunnel mode.

Auto-Provisioning of APs

ArubaOS now allows you to automate and simplify AP provisioning by assigning pre-provisioning rules to new APs.

Configuring Preferred Uplink

Starting ArubaOS 8.4.0.0 Ethernet port1 can be configured as the primary uplink and Ethernet port0 can be configured as the downlink interface, in an active-standby uplink mode of deployment. This enhancement is supported in AP-318, AP-374, AP-375, and AP-377.

AP-Wireless

Mute AP Radio

From this release, the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands include the **am-tx-mute** parameter. Enable the **am-tx-mute** parameter to prevent an AP that operates in the Air Monitor or spectrum mode from creating spurious transmissions during AP boot. By default, the **am-tx-mute** is disabled.

Enable the **am-tx-mute** parameter in the **rf dot11a-radio-profile** or **rf dot11g-radio-profile** command only for APs that operate in the Air Monitor or spectrum mode.

To enable the **am-tx-mute** parameter, execute the following commands:

```
(host) (config) #rf dot11a-radio-profile default
(host) (config) (rf dot11a-radio-profile "default")#am-tx-mute
```

Authentication

802.11w Support for Tunnel Mode

The 802.11w standard is now supported in tunnel mode with a Virtual AP configured with WPA3 security mode.

EAP-TLS Fragmentation

As part of 802.1X authentication, ArubaOS supports EAP-TLS fragmentation in non-termination mode.

Multiple Pre-Shared Key for WLAN SSID Profile

WPA2 PSK-based deployments generally consist of a single passphrase configured as part of a WLAN SSID profile. This single passphrase is applicable for all clients that associate with the SSID. Starting from ArubaOS 8.4.0.0, Multiple Pre-Shared Key (MPSK) in conjunction with ClearPass Policy Manager are supported for WPA and WPA2 PSK-based deployments. Every client connected to the WLAN SSID may have its own unique PSK.

Support for New Wi-Fi Alliance Security Enhancements

ArubaOS supports new WPA3 and enhanced-open security improvements with the following features:

- WPA3
  - Simultaneous Authentication of Equals (SAE) replaces WPA2-PSK with a password based authentication resistant to dictionary attacks.
  - WPA3-Enterprise optionally adds usage of Suite-B 192-bit minimum-level security suite aligned with CNSA for enterprise networks.
- Enhanced Open replaces open unencrypted wireless networks thereby mitigating exposure of user data to passive traffic sniffing

ArubaOS implements WPA3 (including the optional CNSA mode) and the optional Enhanced Open enhancement as specified in the certification programs of Wi-Fi Alliance. The 300 Series310 Series, 320 Series, 340 Series, 360 Series, 370 Series, AP-514, and AP-515 access points support WPA3 and Enhanced Open.

EAP-TLS Supplicant Support

The EAP-TLS supplicant support allows you to add a Fully Qualified Domain Name (FQDN) as a suffix to an AP name or a group of APs for factory certificates.

Base OS Security

CP Firewall Limit

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

Firewall Visibility

Prioritize RTP Traffic

Starting from this release, the RTP traffic is prioritized based on the DSCP value set by the end user device. This allows the RTP traffic to pass through the managed devices.

Management Users

Admin Password Recovery

Starting from this release, ArubaOS allows you to disable the default password recovery feature and create an alternate password recovery user to reset the admin password.

Implementing Management User Audits

The administrator can track the following details:

- Location of the last successful login
- Date and time stamp of the last successful login
- Number of successful attempts over a period of time
- Number of unsuccessful attempts since the last successful login

Implementing Password Validation

When a PSK-based management user changes the password, a check is added to ensure that there is at least a difference of 8 characters between the new password and the old password.

Configuring Concurrent Sessions

A check is added to limit the number of concurrent sessions that an administrator account can maintain. If the admin user tries to create a new session after the maximum concurrent user sessions limit is reached, then the system displays an error message and does not allow the user to login although the login credentials entered are valid.

This option can be configured only using the CLI.

Maintaining Standard Mandatory Notice and Consent Banner

Starting from this release, a configuration option is added to enable retaining the Login Banner on the WebUI login page until the user clicks the **I Accept** button, only after which the login prompt is displayed.

Zeroizing TPM Keys

Starting from this release, you can zeroize a cryptographic module. This involves erasing sensitive parameters such as electronically stored data, cryptographic keys, and critical security parameters from a controller or an AP to prevent disclosure of information if the equipment is permanently and irrevocably decommissioned.

VIA Client Audit

Starting from this release, when a user authenticates and accesses the VIA client, a notification with details about the last successful logon date and time stamp is provided.

Jumbo Frames

Starting from this release, Jumbo Frames is supported on Mobility Controller Virtual Appliance.

BLE

IoT Enhancements

ArubaOS supports IoT applications through BLE. ArubaOS supports multiple transport mechanisms, payload encoding, payload content, and periodicity of information updates. For example, some door locks from Assa Abloy use ZigBee for back-end connectivity. An AP with a USB ZigBee radio provides gateway services to relay the door lock information to a management server.

Branch Office

Using ZTP with DHCP to Provision Managed Devices

Managed devices can get the information required for provisioning from a DHCP server instead of Activate. You can use Option 43 of DHCP to broadcast the master information to the managed devices.

Enhancements to Uplink Configuration

The uplink configuration is now simplified and enhanced to configure multiple WAN paths to the VPN Concentrator for a branch office network by allowing you to specify the link type and link names.

Hub and Spoke VPN Support

ArubaOS provides support for Hub and Spoke VPN which enables automatic VPN tunnel establishment with the VPN concentrators for managed devices in a branch network.

Support for Static IP Routing using Automatic VPN Tunnel

ArubaOS supports forwarding of IP routes using the IPsec tunnel to VPN Concentrator that is established using the Hub and Spoke VPN configuration in a branch network.

Captive Portal

Support for Captive Portal URL VSA

Starting from this release, ArubaOS supports **Aruba-Captive-Portal-URL** VSA attribute to dynamically redirect users to Captive Portal home page.

Adding AP's MAC address in the redirection URL

Starting from this release, you can include the AP's MAC address in the redirection URL when using external captive portal servers.

Cluster

EST Support for Cluster

The cluster members use enrolled certificate for IPsec tunnel authentication instead of using factory certificates.

Remote AP support with Cluster behind NAT

Remote APs can map the managed device's private address to a public space by obtaining the private IP and public IP address mapping from a cluster. Therefore, the cluster behind NAT is supported with Remote APs.

Scheduled Cluster Upgrade

Scheduled cluster upgrade feature allows you to schedule the upgrade to a specified time to avoid manual intervention. The cluster is upgraded automatically at the scheduled time. You can view, delete, or reschedule the scheduled cluster upgrade.

CLI Enhancements

Show user-table

If the **show user-table** command is executed from the **[mynode]** or **[mm]** prompts of the Mobility Master CLI, the following alert message is displayed:

This command is not applicable on master switch

Show ap mesh debug link-table

The **Show ap mesh debug link-table** command is introduced to display the mesh link table information for a remote mesh point or remote mesh portal.

ClientInsight

ClientInsight for ArubaOS

ClientInsight is designed to support the next generation data-driven wireless network automation. It is an integration of ClientMatch and NetInsight.

High Availability

AP Ageout

The AP Ageout process now allows the controller to age out the APs based on the last activity timestamp of the AP.

IPv6 Support

IPsec Support

Starting from this release, Remote APs support IPv6 clients in Split-Tunnel forwarding mode in a VAP profile.

Aeroscout and RTLS Server Support

Starting from this release, an AP can connect to the Aeroscout or RTLS location server using a configurable IPv6 address.

MultiZone Profile

Starting from this release, you can configure an IPv6 address in one data zone of an AP MultiZone profile.

External Captive Portal

ArubaOS now supports external captive portal for IPv6.

WebCC Support

Starting from this release, the WebCC feature also supports classification of IPv6 sessions on the managed device.

License Management

License Management with ASP

Starting from this release, the ArubaOS License Automation feature is supported, where the Mobility Master obtains the ArubaOS licenses from ASP or LMS automatically. The users need not manually add the licenses on the Mobility Master.

Mesh

Mesh Auto Role Detection

ArubaOS now allows you to set **mesh auto** under **Configuration** > **Access Points** > **Provision** > **Mesh role**. Mesh auto enables auto-detection of mesh point or mesh portal based on system initialization or operation. The **mesh-auto** parameter is introduced under the **provision-ap** command to enable auto-detection of mesh using the CLI.

NetDestination

NetDestination and NetServices Alias

NetDestination and NetServices aliases can now be configured using the ArubaOS 8.4.0.0 WebUI.

PPPoE

Support for Multiple PPPoE Uplinks

Starting from this release, managed devices can be configured to support the same gateway IP address over multiple PPPoE uplinks.

SES-imagotag ESL System

SES-imagotag ESL System for ArubaOS

The USB aerials for SES-imagotag's Electronic Shelf Label (ESL) is now supported on AP-303H, 300 Series access points, 310 Series access points, 320 Series access points, 330 Series access points, 340 Series access points, and 510 Series access points. The following commands are introduced as part of this feature:

- **sesimagotag-esl-channel**
- **sesimagotag-esl-serverip**
- **show ap debug esl-status**
- **show ap debug ses-esl-log**

SNMP

Support for SNMP Traps over Websocket

A controller's SNMP traps can now be sent over Websocket.

Enhancements to LinkUp and LinkDown Traps

The **IfDescr** and **IfName** objects are added to the **LinkUp** and **LinkDown** traps to include the description and name details of the interface.

Enhancements to wlxBSSIDIsup and wlxBSSIDIsdown Traps

The name of the AP is added to the **wlxBSSIDIsup** and **wlxBSSIDIsdown** traps. The output of the **show snmp trap-queue** command lists the name and MAC address of the APs associated with the BSSID.

Tunnel Node

Support for Trusted and Untrusted VLANs on a Single L2 GRE Tunnel

Starting from this release, a single IPv4 and IPv6 Layer-2 GRE tunnel can carry both trusted and untrusted VLANs.

Aruba Dynamic Segmentation Solution

The Dynamic Segmentation solution is Aruba's ability to assign policy (roles) to a wired port, based on the access method of a client. Further, using ClearPass Policy Manager, we can add context such as time-of-day and type-of-machine. The solution also provides users the ability to segment client

traffic via traditional, locally switched VLANs or to tunnel traffic back to an Aruba Mobility Controller.

Starting from this release, enhancements made to the WebUI provides visibility into wired clients, tunneled switches, and so on. The Aruba Dynamic Segmentation solution removes the need for user VLANs to be created on the Aruba access switch. Instead it uses user-role based VLANs to assign roles for Dynamic Segmentation users so that user's traffic gets classified in a VLAN.

Support is extended for downloadable user roles in cluster deployments. This feature provides seamless redundancy for dynamic policy assignments.

Starting from this release, IPv6 support is available for Aruba Dynamic Segmentation solution.

Starting from this release, a license is required to activate the Dynamic Segmentation feature and is similar to AP licensing. If the license is not installed, controllers will not be allowed to form tunnels to the Aruba access switch and the feature will not function.

UCC

Support for Microsoft Teams

ArubaOS 8.4.0.0 can detect, classify, and prioritize voice and video services for Teams, which is the new cloud-based UCC application from Microsoft. The information for Microsoft Teams traffic is currently monitored and represented in the UCC dashboard as Skype for Business traffic because the client media session attributes are unchanged between Skype for Business and Teams.

Web Server

Backward Compatibility

ArubaOS 8.4.0.0 introduces the Backward Compatibility feature that enables managed devices to receive register requests on the older HTTP port 80. This option is beneficial when managed devices and Instant APs have not been upgraded to ArubaOS 8.4.0.0 simultaneously in a network. When only managed devices are upgraded, users must enable this feature so that managed devices do not drop register requests received on the older HTTP port 80, which can result in service disruption.

WebUI

AP Packet Capture

AP Packet Capture feature allows you to manually start capturing AP packets on an access point that is UP and download the files using the WebUI.

AirMatch

Starting from this release, a toggle switch is added to enable the **Automatically deploy AirMatch optimizations** setting.

ARM Profile

Starting from this release, the following ARM profile configuration parameters are available only on stand-alone controller and master controller mode.

- **Assignment**

- **Allowed bands for 40 MHz channels**
- **80 MHz support**
- **Max TX EIRP**
- **Min TX EIRP**

Client Match

Starting from this release, a single check box is added to enable or disable Client Match on both 2.4 GHz and 5 GHz radio settings.

Dashboard Monitoring

New **Dashboard** is not supported in the Master controller mode.

RF Management

Starting from this release, the following RF management configuration parameters are available only on the Mobility Master mode.

- **Max Channel Bandwidth**
- **Min Channel Bandwidth**
- **Min EIRP**
- **Max EIRP**
- **eirp-offset**

Scheduled Upgrade

The ArubaOS version of the managed devices or cluster members can be scheduled to upgrade at a predetermined date and time through the WebUI. The managed devices or cluster members can be scheduled to manually download and install the predetermined ArubaOS image from a FTP, SCP, or TFTP server or a local file at the scheduled date and time. The date and time of a scheduled upgrade can be changed or the scheduled upgrade can be canceled through the WebUI. The WebUI displays the status of the scheduled upgrade in graphical and tabular views with details like name of managed device or cluster member, current version of ArubaOS installed, version of ArubaOS to install, number of access points connected to the managed device or members in a cluster.

Support for Unicode Characters

Support for unicode characters in ESSID is added.

VIA VPN Client Capability

The VIA client now provides a new Vendor Identifier string that forwards Layer-2 GRE packets containing Ethernet frames using the IPsec tunnel established with the managed device.

VIA VPN Client Visibility

The VIA client users are separately displayed on the WebUI for VPN client visibility. You can view the client users in the **Dashboard > Clients > Remote Clients** page in the WebUI.

VIA Unique Identifier

Client's MAC address is used as the unique identifier when authentication is sent to ClearPass Policy Manager.

Dashboard Monitoring

ArubaOS now supports the option to delete one or more inactive APs that are either replaced or no longer used in a deployment.

Support for New Parameter in AP System Profile

Starting from this release, a new parameter, **AP USB Power mode**, is introduced to the **Advanced** accordion of the **AP system profile** option in the **Configuration** > **System** > **Profiles** page. This parameter enables or disables the USB port on various AP platforms that have external ports.

Support for Redirect-DNS

Starting from this release, you can configure and redirect the domain to a dedicated DNS server in an IPv4 and IPv6 domain.

Enhancement to the Controller WebUI

Starting from this release, you can perform the following tasks on the controllers using the WebUI:

- Drag and Drop
- Edit Action

This chapter describes the platforms supported in this release.

Mobility Master Platforms

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

Table 3: *Supported Mobility Master Platforms in ArubaOS 8.4.0.0*

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

Mobility Controller Platforms

Table 4: *Supported Mobility Controller Platforms in ArubaOS 8.4.0.0*

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

AP Platforms

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

Table 5: *Supported AP Platforms in ArubaOS 8.4.0.0*

AP Family	AP Model
100 Series	AP-104, AP-105
103 Series	AP-103
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135
170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1
200 Series	AP-204, AP-205
203H Series	AP-203H
205H Series	AP-205H
207 Series	AP-207
203R Series	AP-203R, AP-203RP
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
228 Series	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
303 Series	AP-303, AP-303P
303H Series	AP-303H
310 Series	AP-314, AP-315
318 Series	AP-318

Table 5: *Supported AP Platforms in ArubaOS 8.4.0.0*

AP Family	AP Model
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
340 Series	AP-344, AP-345
360 Series	AP-365, AP-367
370 Series	AP-374, AP-375, AP-377
_	AP-387
510 Series	AP-514, AP-515
RAP 155 Series	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
RAP 3 Series	RAP-3WN, RAP-3WNP

Virtual Platforms

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

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

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

- MC-VA-10
- MC-VA-50

- MC-VA-250
- MC-VA-1K

Chapter 4
Regulatory Updates

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

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller 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_67861

This chapter describes the issues resolved in this release.

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
149222	**Symptom:** The WebUI of a Mobility Master did not display any devices. The fix ensures that the **local-ip** related commands are restricted only to /mm path. **Scenario:** This issue occurred when a user configured a managed device from the **/mm/mynode** node hierarchy using CLI. This issue was observed in the WebUI of Mobility Masters running ArubaOS 8.0.0.0 or later versions.	IPsec	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
154096	**Symptom:** The channel of a virtual AP was inconsistent after a radar event was detected. This issue is resolved by allowing a managed device to change the channel when a virtual AP is created and a radar event is detected on the channel. **Scenario:** This issue occurred when a virtual AP in bridge-always forwarding mode had disconnected from a managed device detected a radar event on the channel and selected a new channel. This issue was observed in 300 Series access points running ArubaOS 8.2.0.0.	AP Regulatory	300 Series access points	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
157199	**Symptom:** An AP crashed unexpectedly. The log file lists the reason for the event as **kernel BUG at kernel/timer.c:869!**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-225 access points running ArubaOS 8.4.0.0.	AP-Wireless	AP-225 access points	ArubaOS 8.4.0.0	ArubaOS 8.4.0.0
159973	**Symptom:** Certificates loaded on a managed device failed to synchronize between Mobility Master and the standby Mobility Master. The fix ensures that the certificates loaded on a managed device are synchronized successfully. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.1.0.0 or later versions.	Certificate Manager	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
161891	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when clustering was enabled. 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 8.4.0.0
162623	**Symptom:** The output of the **show ap arm history ap-name <ap-name>** command did not display a radar detection event for an AP. The fix ensures that the output of the **show ap arm history ap-name <ap-name>** command displays a radar detection event when a radar event is detected for an AP. **Scenario:** This issue was observed in APs running ArubaOS 8.2.0.0.	ARM	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
165804	**Symptom:** The HTTP security header was not detected on ports 8080 or 8088 in a managed device. This issue is resolved by enabling the HTTP security header in the **httpd.conf** file. **Scenario:** This issue was observed in managed devices running ArubaOS 8.4.0.0.	Controller-Platform	All platforms	ArubaOS 8.4.0.0	ArubaOS 8.4.0.0
165908	**Symptom:** A Mobility Master crashed and rebooted unexpectedly. The log file listed the reason for the event as **Control Processor Kernel Panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred due to a softlock causing the crash. This issue was observed in 7200 Series controllers running ArubaOS 8.2.0.0 or later versions. **Duplicates:** 170224, 171074, 171396, 173372, 174322, 174370, 174917, 175009, 177151, 177457, 177662, 178307, 180558, 180741, 181173, 183588, 185596, 186993, 187232, 187418	Controller-Platform	7200 Series controllers	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
166800 173645 176278	**Symptom:** False detections of type-5 radars were triggered in the FCC domain. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169256 175610 176992 182160	**Symptom:** A managed device did not learn some of the ARP response that it received from an AP. The fix ensures that the managed device learns the ARP responses. **Scenario:** This issue occurred when the session table was corrupted during synchronization of high value sessions between active UAC and standby UAC. Hence, some ARP sessions had the **d** or deny flag and the managed device dropped the corresponding ARP responses. This issue was observed in managed devices running ArubaOS 8.1.0.2 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.1.0.2	ArubaOS 8.4.0.0
170249 172066 175830 175931 176688 179004 181990 182574 182752	**Symptom:** A client was unable to connect to an AP that reported 100% CPU utilization. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 8.3.0.1.	AP-Wireless	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.4.0.0
172217	**Symptom:** The **write memory** command did not show the configurations that were committed. The fix ensures that the **write memory** command works as expected. **Scenario:** This issue occurred when a user configured ACLs, VLANs, and interface configuration and issued the **write memory** command. This issue was observed in managed devices running ArubaOS 8.2.0.1.	Configuration	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.4.0.0
173353	**Symptom:** The **TM** column (time used by MGMT frames) in the output of the **show ap radio-summary dot11g** command always displayed 100. The fix ensures that the actual value is displayed. **Scenario:** This issue was observed in access points running ArubaOS 8.0.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
173788 174490 178159	**Symptom:** Clients switched between APs or sometimes to the other band on the same AP. The fix ensures that the clients age out normally when roaming. **Scenario:** This issue occurred when a client sent packets that indicated it is about to roam but attempted to re-associate with the same AP. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174799	**Symptom:** A managed device displayed the **Module Authentication is busy. Please try later** message when the **show firewall dns-names** command was executed. The fix ensures that the managed device processes the **show firewall dns-names** command as expected. **Scenario:** This issue occurred when multiple DNS names were configured in a managed device and one DNS name had too many IP addresses associated with it. This issue was observed in managed devices running ArubaOS 8.4.0.0.	Base OS Security	All platforms	ArubaOS 8.4.0.0	ArubaOS 8.4.0.0
175087	**Symptom:** An AP buffered packets for a long time and replies to the **ping** command was delayed. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-207 access points running ArubaOS 8.0.0.0.	AP-Wireless	AP-207 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
175138	**Symptom:** The **Configurations > Services > Guest provisioning** page appears blank and non-editable. The fix ensures that the **Guest Provisioning** page is displayed correctly. **Scenario:** This issue occurred when a user entered the **&** character in the email field. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Guest Provisioning	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
175140	**Symptom:** AP-325 access points were not coming up on the managed device. This issue was resolved by fixing IP reassembly code. **Scenario:** This issue occurred because of an issue in the reassembly code of the managed devices. This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.0.0.0 or later versions.	Controller - Datapath	AP-325 access points	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
175550	**Symptom:** A user could not disable the security logging for the **aaa** process using the **logging security process aaa subcat aaa level debugging** command. The fix ensures that a user can disable the security logging for the **aaa** process. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Configuration	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175669	**Symptom:** The **show ap active** command did not show any flag for an AP that was operating in restricted mode because of 802.3af PoE (POE-AF). This issue is resolved by showing the **p** flag in the **show ap active** command for an AP that operates in restricted mode. **Scenario:** This issue was observed in access points running ArubaOS 8.0.0.0	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
176105	**Symptom:** The configuration of an AP was lost and the AP rebooted repeatedly. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred due to a missing boot environment configuration. This issue was observed in AP-205 access points running ArubaOS 8.0.0.0 or later versions.	AP-Platform	AP-205 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
176330 177428	**Symptom:** The **Diagnostics > Technical Support > Copy Files** page of the WebUI displayed a success message although the TFTP file transfer failed. The fix ensures that the WebUI displays the correct message. **Scenario:** This issue occurred when a user attempted to copy a file using TFTP. This issue was observed in Mobility Master running ArubaOS 8.2.0.0 or later versions.	Configuration	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
176434	**Symptom:** The Captive Portal page was not displayed correctly on client devices. The fix ensures that the Nginx collects the correct configuration rule. **Scenario:** This issue occurred when the Nginx collected the wrong configuration rule while searching for the CSS file. This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.2.0.2 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
176444	**Symptom:** The startup wizard did not allow adding licenses to a stand-alone controller. The fix ensures that the licenses are added successfully. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.2.1.0.	Controller - Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176622	**Symptom:** The UCC data export function was missing from the ArubaOS version running on a Mobility Master. This issue was resolved by adding the **show ucc call-info cdrs filelog** command, allowing the output of the command to be exported as a .csv file. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	UCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
176774 177016	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-225 access points running ArubaOS 8.0.0.0.	AP-Wireless	AP-225 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
176902	**Symptom:** Managed devices dropped ARP response from silent clients. The fix ensures that managed devices do not drop ARP responses from silent clients. **Scenario:** This issue occurred when the protect ARP spoofing feature was enabled and a managed devices deleted the datapath user entries of silent clients. This issue was observed in managed devices running ArubaOS 8.0.0.0.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
176927	**Symptom:** High channel utilization and beacon failures were observed in some APs, and the issues continued to be displayed until the APs were rebooted. The fix ensures that these performance issues are not observed in the APs. **Scenario:** This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
176930	**Symptom:** An AirGroup server that was connected as a Per User Tunneled Node client was not showing up as an AirGroup server on the Mobility Master. This issue is resolved by using tunneled_user GSM channel for subscription. **Scenario:** This issue occurred when a tunneled_node GSM channel was used for user subscription. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	SDN-Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176952	**Symptom:** The **/flash/upload** directory was available to unauthenticated users. The fix ensures that the **/flash/upload** directory sends a **permission denied** message for unauthenticated users. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
176957	**Symptom:** The user-name attribute in a RADIUS response message was not populated in the user table during captive portal authentication. The fix ensures that managed devices update the username in the user table with the value received as an attribute in a RADIUS response. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0.	Radius	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
177017	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-225 access points running ArubaOS 8.0.0.0.	AP-Wireless	AP-225 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
177045 180877	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **external watchdog reset**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when radio in the AP tried to reset PHY and the driver was stuck. This issue was observed in AP-203H and AP-207 access points running ArubaOS 8.3.0.0 or later versions.	AP-Platform	AP-203H and AP-207 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
177162	**Symptom:** The position of an ACL that was configured on the default **user-role** was changed unexpectedly. The fix ensures that a managed device retains the ACLs in the correct positions. **Scenario:** This issue occurred when a managed device was reloaded and the ACLs were loaded in the wrong sequence at startup. This issue was observed in managed devices running ArubaOS 8.3.0.0.	Configuration	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177420	**Symptom:** The HSTS Security header was missing in the HTTP response from the Mobility Master WebUI. The fix ensures that the HSTS header is included in the HTTP response. **Scenario:** This issue was not limited to any specific controller model or ArubaOS release version.	Web Server	All platforms	ArubaOS 8.2.0.1	ArubaOS 8.4.0.0
177618	**Symptom:** The **sapd** process crashed in an AP. This issue is resolved by not sending the nodelist to the AP when there are two APs configured with the same name. **Scenario:** This issue occurred when two APs had the same AP name. This issue was observed in access points running ArubaOS 8.2.0.2.	AP-Platform	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
177653	**Symptom:** The console log of an AP listed multiple user-miss and resource temporarily unavailable messages. The log on AMP listed multiple sessions for the same client connected to the Remote AP using split-tunnel forwarding mode. The fix ensures that the AP console log does not unnecessarily list user-miss and resource temporarily unavailable messages. **Scenario:** This issue was observed in access points running ArubaOS 8.0.0.0.	Remote AP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
177770	**Symptom:** APs crashed and rebooted unexpectedly. The log files listed the reason for the event as **Kernel panic - not syncing: FW ASSERT at tx_send_setup_ppdu_params**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue occurred when an ADDBA response was received with a window size of 0 as some of the retried frames were not flushed from the frame queue. This issue was observed in AP-335 access points running ArubaOS 8.2.0.2 or later versions	AP-Wireless	AP-335 access points	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
177788	**Symptom:** A client experienced a slow network or network connectivity issue although the number of sessions in the AP did not reach the maximum value. The fix ensures that clients get a better network experience. **Scenario:** This issue was observed in AP-315 access points running ArubaOS 8.0.0.0.	AP Datapath	AP-315 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177789	**Symptom:** When an incorrect password was entered in an external captive portal multiple times, the error message string **errmsg=Authentication%20failed** was appended to the URL multiple times. The fix ensures that the **errmsg=Authentication%20failed** is appended to the URL once. **Scenario:** This issue occurred when external captive portal was used with a non-cppm server. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
177796	**Symptom:** Internal captive portal was displayed incorrectly when the client attempted to log in with blank credentials, using external captive portal. The issue is resolved by displaying an appropriate reason for authentication failure if blank credentials are used to login. **Scenario:** This issue occurred when the client tried to log in with external captive portal using either a blank username, blank password, or both. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
177891	**Symptom:** The **Authentication** process in a managed device crashed unexpectedly and a client was disconnected. This issue is resolved by ensuring that the role name is valid and not empty. **Scenario:** This issue occurred when a CPPM role download was configured but the role name was invalid or empty. This issue was observed in 7220 controllers running ArubaOS 8.2.0.2 or later versions.	Base OS Security	7220 controllers	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
178032	**Symptom:** An AP was unresponsive for a short period (up to 1.5 seconds) which led to client disconnections. The fix ensures that active-scan in an AP returns to its home channel and clients retain connectivity. **Scenario:** This issue occurred when active-scan was enabled in an AP. With active-scan enabled, an AP left its home channel to scan another channel. However, the AP did not return to its home channel and aborted the channel scanning after 1.5 seconds. While the AP was scanning another channel, clients lost connectivity with the AP and attempted to find another AP. The AP did not complete the channel scan successfully and did not report neighbors in the active scanning channels (2.4 GHz and non-DFS 5 GHz channels). This issue was observed in access points running ArubaOS 8.2.0.0.	AP-Wireless	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178114 180746	**Symptom:** A Remote AP failed to come up. The fix ensures that the Remote AP works as expected. **Scenario:** This issue occurred when the MTU was not adjusted automatically. This issue was observed in AP-305 access points running ArubaOS 8.0.1.0 or later versions.	AP Datapath	AP-305 access points	ArubaOS 8.0.1.0	ArubaOS 8.4.0.0
178119	**Symptom**: A client was unable to connect to the AP. The fix ensures that the client is able to connect to the AP. **Scenario**: This issue occurred when the AP stopped broadcasting the configured SSID. This issue was observed in AP-225 and AP-325 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-225 and AP-325 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
178182 179612	**Symptom:** A user experienced intermittent Skype call drops. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when an AP stopped transmitting packets for a few seconds to track power save status. This issue was observed in access points running ArubaOS 8.0.0.0.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
178221 189525	**Symptom:** The **show airgroup aps** command does not list AirGroup APs on a managed device. The fix ensures that the **show airgroup aps** command lists the AirGroup APs. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.0.	AirGroup	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
178247 178268	**Symptom:** The VIA connection did not work with IKEv2 and SSL-fallback mode. The fix ensures that the VIA connection works with IKEv2 and SSL-fallback mode. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.0.	IPsec	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
178284	**Symptom:** A Mobility Master Virtual Appliance lost network connectivity. The fix ensures that the Mobility Master Virtual Appliance does not lose its network connection. **Scenario:** This issue was observed in Mobility Master Virtual Appliances running ArubaOS 8.2.0.2 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178324	**Symptom:** The 5 GHz channel of an outdoor AP switched to channel 46 which was excluded in the regulatory-domain profile. This issue is resolved by sending only the outdoor channel EIRP list for an outdoor AP. **Scenario:** This issue occurred when an outdoor AP randomly picked up a channel designated for use by an indoor AP from the exhaustive EIRP list. This issue was observed in outdoor access points running ArubaOS 8.2.0.0.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
178329	**Symptom:** The **show ap active** command on an AP displayed an incorrect 5 GHz channel. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when an AP detected a radar within the 10 seconds interval between a lost connection and a Wi-Fi shutdown. After the connection was re-established, the AP displayed a different channel in the **show ap active** command output. This issue was observed in AP-205 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-205 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
178351	**Symptom:** A specified GigabitEthernet interface in a managed device did not support maximum transmit rate in kilobits per second. The fix ensures that the maximum transmit rate settings also support kilobits per second. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
178357	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **FW ASSERT at rc_get_nss_from_chainmask()**. Improvements to the wireless driver resolved the issue. **Scenario:** This issue was observed in 300 Series access points running ArubaOS 8.2.1.0 or later versions.	AP-Wireless	300 Series access points	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
178390	**Symptom:** A few APs failed to switch over to another managed device in a cluster. The fix ensures that the APs switch over to another managed device successfully. **Scenario:** This issue occurred when a managed device rebooted. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Cluster-Manager	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178394	**Symptom:** When an incorrect password was entered in an external captive portal, **errmsg=Authentication%20failed** was appended incorrectly to the URL and the login page did not load correctly. The fix ensures that the login page loads correctly after an authentication failure. **Scenario:** This issue occurred when external captive portal was used with a non-ClearPass Policy Manager server. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Captive Portal	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
178407 178459 176490 178469 179289	**Symptom:** Clients were unable to send packets that were larger than 978 bytes over an IPsec tunnel. The fix ensures that the clients are able to send packets that are larger than 978 bytes over an IPsec tunnel. **Scenario:** This issue was observed in access points running ArubaOS 8.2.0.1 or later versions.	AP Datapath	320 Series access points	ArubaOS 8.2.0.1	ArubaOS 8.4.0.0
178498	**Symptom:** AirGroup users could use Apple TVs on different AP groups. The fix ensures that the AirGroup users show all available information for the user. **Scenario:** This issue occurred when AirGroup was enabled in centralized mode with auto association. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions in a cluster setup.	AirGroup	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
178405	**Symptom:** The output of the **show ap active** command displayed incorrect 5 GHz Channel. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the radar detection was set to random, causing the command output to display an incorrect channel. This issue was observed in 100 Series access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	100 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
178419 180044 181059	**Symptom:** The mDNS RADIUS requests were sent with the NAS-IP address in reverse order to the ClearPass Policy Manager. 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 managed devices running ArubaOS 8.3.0.0 or later versions.	AirGroup	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178609	**Symptom:** A managed device retained the port-channel **trusted** and **trunk allowed vlan** in the setup configuration instead of receiving it from the Mobility Master. This lead to a connectivity issue. The fix ensures that the managed device retains the correct port-channel configuration that is received from the Mobility Master. **Scenario:** This issue occurred when the port-channel in the setup configuration of the managed device was different from the configuration that was received from the Mobility Master. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	Configuration	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
178633	**Symptom:** An AP console displayed the **fsl_dpa ethernet.17 eth0: Err FD status = 0x00000020** error message. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the AP received bad checksum uplink packets. This issue was observed in AP-335 access points running ArubaOS 8.3.0.0 or later versions.	AP Datapath	AP-335 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
178709	**Symptom:** The **Ipsec-map name** drop-down list was blank under the **Configuration** > **Roles & Policies** > **Policies** > **Route Policy** > **New forwarding Rule** table. This issue is resolved by adding the drop-down options and also providing a text box for adding the IPsec map name manually. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	WebUI	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
178719 179348 180890 186926	**Symptom:** Managed devices crashed and rebooted unexpectedly. The log files listed the reason for the event as **Reboot Cause: Hardware Watchdog Reset (Intent:cause:register ee:ee:50:4).** **Scenario:** This issue occurred when the CPU memory was full. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178758	**Symptom:** A split-tunnel user was stuck with large idle time on a managed device. This issue is resolved by aging out the station when a client is not responsive after associating with an AP but does not complete the 4-way handshake in bridge, split-tunnel, or D-tunnel forwarding modes. **Scenario:** This issue occurred because of stale entries in the client-table of the driver. This issue was observed in access points running ArubaOS 8.0.0.0.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
178760 179950 189003	**Symptom:** Instant APs connected to a managed device obtained reversed IP addresses. The fix ensures that the Instant APs get the IP addresses in the correct format. **Scenario:** This issue occurred when a MAC address of an Instant AP was configured with a remote-ip address in the remote whitelist database using the **whitelist-db rap add mac-address** command. This issue was observed in Mobility Controller Virtual Appliance running ArubaOS 8.3.0.0 or later versions.	CPsec	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
178764 183584	**Symptom:** The **Syslogd** process in an AP crashed and generated core files frequently. The fix ensures that the crash does not occur. **Scenario:** This issue was observed in 300 Series, 310 Series, 303 Series, 303H Series, 318 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points running ArubaOS 8.2.1.1 or later versions.	AP-Platform	300 Series, 310 Series, 303 Series, 303H Series, 318 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178839	**Symptom:** When an AP with static channel or EIRP was rebooted, the opmode changed on other Dual 5 GHz APs as well. This resulted in 2.4 GHz APs getting EIRP computed for 5 GHz AP and vice-versa. The fix ensures that the auto opmode switching is disabled for the AP when static EIRP or static channel settings are detected on the AP. **Scenario:** This issue occurred under the following conditions: ■ The Dual 5G APs were configured with static channels or EIRP. ■ The AP was rebooted. ■ The value of **dual-5ghz-mode** was set to **automatic** in the **ap system-profile**. This issue was observed in APs running ArubaOS 8.3.0.0.	AirMatch	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
178870	**Symptom:** Changes did not reflect in DPI classification when a single rule was deleted in the custom application. The fix ensures that the changes made in the custom application reflect in the DPI classification. **Scenario:** This issue occurred when multiple rules were configured within the custom application and a single rule was deleted. This issue was observed in managed devices running ArubaOS 8.3.0.0.	DPI	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
179047	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **PC is at wlc_apps_bss_ps_off_done+0x54/0x118 [wl] and LR is at wlc_mbss_shm_ssid_upd+0x2f8/0x330 [wl]**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-345 access points running ArubaOS 8.3.0.0.	AP-Wireless	AP-345 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
179107	**Symptom:** A stand-alone controller displayed the error message, **Module licensemgr is busy. Please try later**. The fix ensures that a validation check is added to prevent addition of unsupported licenses. **Scenario:** This issue was observed in Mobility Controller Virtual Appliance running ArubaOS 8.1.0.4 or later versions.	Licensing	All platforms	ArubaOS 8.1.0.4	ArubaOS 8.4.0.0
179124	**Symptom:** A managed device displayed the following error messages: **ERRS |wms| WMS Event Table Cleanup: The system call to pthread_create() has failed with error [Resource temporarily unavailable.** Enhancements to memory management resolved the issue. **Scenario:** This issue occurred because of a memory leak. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Air Management - IDS	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179151	**Symptom:** Mobility Master failed to upgrade from ArubaOS 8.2.0.2 to ArubaOS 8.2.1.0 version. The fix ensures that the Mobility Master is able to upgrade to the latest ArubaOS version. **Scenario:** This issue occurred when the ArubaOS version was copied to an incorrect directory causing an error in upgrading the Mobility Master. This issue occurred in Mobility Masters running ArubaOS 8.2.0.2.	Image Upgrade	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
179215	**Symptom:** AirMatch deployed the APs with wider channel bandwidth when the number of configured channels was less than 3. The fix ensures that AirMatch deploys the APs with correct channel bandwidth. **Scenario:** This issue occurred when frequency reuse channel bandwidth selection logic did not scale well when the number of channels were less than 3. This issue was observed in APs running ArubaOS 8.2.0.0 or later versions.	AirMatch	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
179347	**Symptom:** The default node did not change its path when the group name was changed in a Mobility Master. **Scenario:** This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.3.0.0 or later versions.	Configuration	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
179360	**Symptom:** A managed device displayed the **Module L2TP is busy. Please try later error** message and did not provide an L2TP IP address. The fix ensures that the managed device provides an L2TP IP address and works as expected. **Scenario:** This issue occurred when the **show vpdn l2tp local pool** command was executed. This issue was observed in managed devices running ArubaOS 8.0.0.0.	IPsec	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
179408	**Symptom:** The log of a Mobility Master displayed the **|localdb| |wl-sync| Skipping db_sync** message. The fix ensures that the Mobility Master does not log the message for unnecessary managed devices. **Scenario:** This issue occurred when a Mobility Master synchronized the whitelist database to managed devices by using the MAC address of the managed device. This issue was observed in 7220 controllers running ArubaOS 8.0.0.0.	802.1X	7220 controllers	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179483	**Symptom:** A user was unable to delete **folder _config1** folder on the Mobility Master WebUI. This issue is resolved by adding a check at the end of datastore initialization. **Scenario:** This issue occurred due to dummy nodes created in the datastore that were not deleted after a executing a configuration difference. This issue was observed in a Mobility Master Virtual Appliances running ArubaOS 8.2.1.0.	Configuration	Mobility Master Virtual Appliance	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
179485	**Symptom:** Mobility Master rebooted unexpectedly. The log file listed the reason for the event as **profmgr** process crash. The fix ensures that Mobility Masters work as expected. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.1.0.	L2 Forwarding	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
179627	**Symptom:** The **FPAPPs** process was stuck in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when the initial full-setup wizard was used to switch a 7205 controller that was running in stand-alone mode to a managed device and an invalid netmask was entered. This issue was observed in 7205 controllers running ArubaOS 8.2.1.0.	L2 Forwarding	7205 controllers	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
179656	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception in interrupt**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the mesh role in the AP provisioning profile was set to mesh point in 300 Series access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	300 Series access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
179837 182068	**Symptom:** The usage time was incorrectly displayed in the **Dashboard > Usage** page. There was a time difference when compared to the controller's clock that was set through NTP. The fix ensures that the correct usage time is displayed. **Scenario:** This issue occurred because the DST was not considered when calculating the usage time. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179867	**Symptom:** An AP switched to APM mode unexpectedly. This issue is resolved by checking the AP certificate information if the new bandwidth has channels available during bandwidth upgrade. If a channel is not available for the new bandwidth, a debug message is logged with the reason for the unsuccessful bandwidth upgrade. **Scenario:** This issue occurred during bandwidth upgrade when AirMatch changed the min-channel-bandwidth in the 5 GHz radio profile of an AP to a value that did not match the AP certificate information for the country code. This issue was observed in access points running ArubaOS 8.2.1.0.	AirMatch	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
179869	**Symptom:** A managed device did not display any validation error message when the user deleted role default session ACL by executing the **no access-list session apprf-<role name>-sacl** command. The fix ensures that the appropriate validation message is displayed when the user tries to delete the role default session ACL. **Scenario:** This issue occurred when the system flags applicable to the user role were erased on reboot of the Mobility Master. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions in a Mobility Master-Managed Device topology.	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
179936 189520	**Symptom:** A few APs stopped responding to pings randomly. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-105 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-105 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
179942	**Symptom:** A client was not able to send or receive traffic to or from an AP. The fix ensures that the AP sends a PAPI message to the User Anchor Controller (UAC) and the clients are able to send or receive traffic to or from an AP. **Scenario:** This issue occurred when the **station management** process in an AP sent a PAPI message to the AP Anchor Controller (AAC) instead of the UAC. This issue was observed in a cluster topology running ArubaOS 8.2.1.0 with 802.11r enabled.	Station Management	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
179970	**Symptom:** The **flags** column in the output of the **show ap bss-table** displayed wrong characters for AP Ethernet wired clients. This issue is resolved by setting the first bytes of the flags to null before checking if an Ethernet wired port is enabled. **Scenario:** This issue occurred when both wireless radios were disabled and the wired Ethernet port was enabled but the flags were not initialized. This issue was observed in managed devices running ArubaOS 8.0.0.0.	Station Management	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
180033	**Symptom:** When the port was connected to a 1 Gbps switch, some 340 Series access points failed to enable the Eth0 interface. The fix ensures that the Ethernet link is stable after the switch is restarted by physically turning off the power supply and turning it on again. **Scenario:** This issue occurred only when the switch was restarted by turning off the power to the switch. If you have not upgraded to ArubaOS 8.3.0.3, restart the switch without interrupting the power supply as a workaround. This issue was observed in 340 Series access points running ArubaOS 8.3.0.0 or later versions	AP-Platform	340 Series access Points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
180045 185407	**Symptom:** The **Configuration** > **Roles and Policies** page of the WebUI displayed an incorrect position for the policies for each user role. The fix ensures that the WebUI displays the correct position of the role policies. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	Configuration	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
180118	**Symptom:** An AP broadcasted an SSID that was configured with opensystem encryption as a WEP SSID. The fix ensures that the AP broadcasts the SSID with opensystem encryption as expected. **Scenario:** This issue occurred when the **sapd** process failed to copy the BSSID and MAC address as part of storing HA keys. This issue was observed in access points running ArubaOS 8.4.0.0.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
180146 188443	**Symptom:** 802.1X clients failed RADIUS authentication. The fix ensures that the clients do not fail RADIUS authentication. **Scenario:** This issue occurred when termination was enabled on the managed device and the TLS handshake failed. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	802.1X	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
180340	**Symptom:** An AP failed to boot using APBoot version 1.2.5.0. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-135 access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-135 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
180398	**Symptom:** A cluster upgrade did not go beyond the first node in a cluster. This issue is resolved by updating the correct model name of the device during upgrade. **Scenario:** This issue occurred when a wrong model name was applied to a device during upgrade. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Configuration	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
180400	**Symptom:** The derived VLAN of a client was changed to a different VLAN. This issue is resolved by not synchronizing the registration information of the client. Hence, MAC authentication occurs for the first time after a client disconnects and reconnects. The VLAN is cached for reuse during the next iteration. **Scenario:** This issue occurred when a client disconnected and reconnected back to the Standby User Anchor Controller (S-UAC) after a cluster failover. This issue was observed in a cluster topology with managed device running ArubaOS 8.2.1.0 or later versions.	Cluster-Manager	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
180489	**Symptom:** The CLI-based upgrade of a managed device failed with the **Timed out, Try again** error message. The fix ensures that CLI-based upgrade of a managed device works as expected. **Scenario:** This issue occurred in a slow network connection when the **copy scp** command failed to download the ArubaOS image after 15 minutes. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Image Upgrade	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
180496 180615 183615 185103 185484 185485 186458 186990 188060	**Symptom:** AirGroup lost all the learned server and user details and also failed to learn any new user or server. The fix ensures that AirGroup learns all users and servers appropriately. **Scenario:** This issue occurred when AirGroup was enabled in centralized mode. This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	AirGroup	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
180601 184241 186662	**Symptom: mDNS** process crashes on a Mobility Master. The fix ensures that the **mDNS** process does not crash. **Scenario:** This issue occurred because of memory corruption. This issue was observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions.	AirGroup	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
180879	**Symptom:** Active client entries were incorrectly deleted from AirGroup. The fix ensures that only the stale client entries are deleted. **Scenario:** This issue occurred because the **mDNS** service incorrectly identified the active client entries as stale entries. This issue was observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions.	AirGroup	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
181043	**Symptom:** APs crashed and rebooted unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue occurred because of retransmitted PAPI messages. This issue was observed in AP-225 access points running ArubaOS 8.0.0.0 or later versions.	Station Management	AP-225 access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
181143	**Symptom:** The same product key was generated when the Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was cloned. This issue is resolved by generating the product key based on the UUID of the system. **NOTE:** If a cloned Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance that runs any version lower than ArubaOS 8.2.2.0 was upgraded to ArubaOS 8.2.2.0 and higher, ArubaOS 8.3.0.2 and higher, or ArubaOS 8.4.0.0 and higher, in the respective releases, the serial number and passphrase were changed and all licenses associated with the older serial number were invalidated. Migrate or regenerate the existing licenses for the new serial number after the upgrade. Contact Aruba Technical Support before the upgrade. **Scenario:** This issue occurred when an OVA-based Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance was deployed, an OVF template was exported, and the exported OVF template was deployed. This issue was observed in Mobility Controller Virtual Appliance or Mobility Master Virtual Appliance running ArubaOS 8.2.0.0.	Controller-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181221	**Symptom:** Clients were unable to connect to the managed device. This issue is resolved by adding the entries to the route-cache table when the router IP table buffer overflows. **Scenario:** This issue occurred when enforce DHCP was enabled and route IP table buffer overflowed. This issue was observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
181355	**Symptom:** The **mDNS** process crashed on a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred because the hash table used to store MAC address was corrupt due to a race condition. This issue was observed in managed devices running ArubaOS 8.3.0.0.	AirGroup	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
181418 183863	**Symptom:** The ISAKMP process crashed unexpectedly in a managed device. The fix ensures that the managed device works as expected. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions.	IPsec	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.4.0.0
181440 182153	**Symptom:** A Mobility Master on Hyper V took longer than usual to boot. The fix ensures that the Mobility Master boots as expected. **Scenario:** This issue occurred when the **rngd** process was not running. This issue was observed in a Mobility Master running ArubaOS 8.3.0.0.	Controller-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
181564	**Symptom:** A Remote AP lost the gateway ARP after using split-tunnel mode virtual AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the Remote AP missed caching the ARP data for a specific gateway. This issue was observed in Remote APs running ArubaOS 8.0.0.0 or later versions.	Remote AP	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
181553	**Symptom:** A managed device crashed when the AP was downloading a build image. The fix ensures that the managed device does not crash in such occurrences. **Scenario:** This issue was observed in managed devices connected to AP-325 access points that downloaded the ArubaOS 8.4.0.0 build image.	Controller-Platform	All platforms	ArubaOS 8.4.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181606	**Symptom:** The output of the **show ap debug log** command displayed the **Bridge entry insertion failure** error message. The fix ensures that the error message is not displayed. **Scenario:** This issue was observed in AP-225 and AP-335 access points running ArubaOS 8.3.0.0 or later versions.	AP Datapath	AP-225 and AP-335 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
181615	**Symptom:** Mobility Masters lost licenses if the Mobility Master was unplugged within 3 hours of adding the license and there were no configuration changes made on the Mobility Master. The fix ensures that the database is backed up every time the write memory command is executed. **Scenario:** This issue occurred because the database backup was not triggered when the write memory command was not executed. This issue is not limited to any specific platform or ArubaOS version.	Configuration	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
181630	**Symptom:** User was not able to disable the **openflow-profile** on a managed device. The fix ensures that the **openflow-profile** is enabled by default. **Scenario:** This issue occurred when user disabled the **openflow-profile** at a configuration level lower than /md. This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	SDN	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
181678	**Symptom:** Same license key was displayed multiple times on a managed device when the **show license** command was executed. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Licensing	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
181721 178075	**Symptom:** Download speeds were less than normal. The fix ensures that higher download speeds are achieved even in noisy conditions. **Scenario:** This issue occurred in extremely noisy environments on 2.4 GHz channels. This issue was observed in 300 Series access points connected to a 7010 controller.	AP-Wireless	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
181729	**Symptom:** The **show running-config** command did not list an ACL although the **show configuration effective** command listed the same ACL. The fix ensures that the **show running-config** command lists the ACL. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.0.	Base OS Security	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
181773	**Symptom:** Managed devices rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed devices work as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
181801	**Symptom:** APs are unable to auto-negotiate Ethernet speed correctly with the switch. The fix ensures that the Ethernet speed and duplex setting are taken directly from the switch. **Scenario:** This issue occurred because of an inadequate cable. This issue was observed in AP-205 access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	AP-205 Access Points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
182049	**Symptom:** A client lost connectivity with an AP. The fix ensures that a client does not lose connectivity with an AP. **Scenario:** This issue occurred when the position of a validuser ACL deny rule was changed. This issue was observed in managed devices running ArubaOS 8.2.1.1.	Configuration	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
182248 182524	**Symptom:** Although the cluster node was up, the cluster upgrade failed with the **Cannot upgrade cluster as cluster node is down** error message. The fix ensures that the cluster upgrade completes successfully. **Scenario:** This issue occurred when a Mobility Master was upgraded and reloaded and a managed device reconnected back to the Mobility Master. The ArubaOS version on the Mobility Master and the managed device was different and the managed device ignored the active master IP address information that was sent by the Mobility Master. This issue was observed in a topology with active and standby Mobility Masters when both active and standby Mobility Masters were upgraded to ArubaOS 8.2.1.1 while the managed devices were running ArubaOS 8.2.1.0 as cluster members.	Configuration	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182352	**Symptom:** An AP did not take the EIRP settings from the radio profile and transmit with high EIRP. The fix ensures that the feasible opmode list does not contain a blank entry, the AP takes the EIRP settings from the radio profile, and transmits with the correct EIRP. **Scenario:** This issue occurred when a blank entry was stored in the feasible opmode list for radio. This issue was observed in access points running ArubaOS 8.2.1.1, managed devices running ArubaOS 8.2.0.0, and Mobility Master running ArubaOS 8.3.0.0.	AirMatch	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
182486	**Symptom:** A client was not able to access the internet. The fix ensures that the VLAN ID will be taken from the route-cache entry for the PPPoE gateway. **Scenario:** This issue occurred when the PPPoE interface included the **ip nat outside** configuration. This issue was observed in managed devices running ArubaOS 8.2.1.0.	VLAN	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
182590	**Symptom:** An error message, **Error reading transceiver ID Prom on 0/0/0** was displayed when the Small Form-factor Pluggable transceiver (SFP module) was connected to the controller. The fix ensures that the SFP modules are supported. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.3.0.0.	Controller-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
182604	**Symptom:** The **Illegal operation on the interface** error was observed when the user tried to add or remove a trusted VLAN on the managed device. The fix ensures that the error message is not displayed. **Scenario:** This issue occurred when the user tried to configure the GigabitEthernet interface with a valid port range. This issue was observed in managed devices running ArubaOS 8.2.0.0 or later versions.	VLAN	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
182612 182372	**Symptom:** Clients were unable to resolve ARP requests. The fix ensures that the clients are able to resolve ARP requests. **Scenario:** This issue occurred because the AP memory utilization rate was high, leading to drop in client traffic. This issue was observed in access points running ArubaOS 8.3.0.0.	AP Datapath	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182683	**Symptom:** A blank redirect page was displayed when **WISPr** client was trying to configure Captive Portal on a managed device. The fix ensures that the correct page is displayed when Captive Portal is configured on a managed device. **Scenario:** This issue occurred when a managed device was experiencing high CPU utilization. This issue was observed in managed devices running ArubaOS 8.1.0.0 or later versions.	WISPr Interoperability	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.4.0.0
182780	**Symptom:** The output of few **show datapath** commands displays the MAC address in upper case. This fix ensures that the output is displayed in lower case. **Scenario:** This issue occurred when the following show datapath commands were issued. This issue is not restricted to any controller or ArubaOS versions. ■ **show datapath route-cache** ■ **show datapath station** ■ **show datapath bridge** ■ **show datapath firewall-agg-sess** ■ **show datapath tunnel** ■ **show datapath tunnel station-list** ■ **show datapath user** ■ **show datapath user rad-counter**	Controller-Datapath	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
182909	**Symptom:** An AP displayed incorrect ACL index value on the user datapath. The fix ensures that the correct value is displayed. **Scenario:** This issue was observed in APs connected to a stand-alone controller running ArubaOS 8.0.0.0 or later versions.	AP Datapath	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
182941	**Symptom:** A managed device displayed the following alert message: **Expecting string of length 1 to 32**. This issue was resolved by increasing the string length to 255 characters. **Scenario:** This issue occurred when a user attempted to add a trunk VLAN of string length greater than 32 characters. This issue was observed in managed devices running ArubaOS 8.2.1.0 or later versions.	VLAN	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
182981	**Symptom:** XML data was displayed when the show license aggregate command was executed from API. The fix ensures that the JSON output is displayed instead of the XML data. **Scenario:** This issue occurred when the command was run over the API on the Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.3.0.1.	Configuration	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.4.0.0
183015	**Symptom:** An AP deauthenticated a client immediately after authenticating it. The fix ensures that the AP retains the authenticated clients. **Scenario:** This issue was observed in access points running ArubaOS 8.3.0.0.	AP Datapath	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
183034	**Symptom:** Clients got disconnected after roaming although auto connect was enabled. The fix ensures that the clients do not get disconnected. **Scenario:** This issue was observed in access points running ArubaOS 8.0.1.0 or later versions in an IPv6 deployment.	AP-Platform	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
183134	**Symptom:** The **profmgr** process crashed multiple times. The fix ensures that the Mobility Master Virtual Appliance works as expected **Scenario:** This issue occurred when SSID is defined on one node and Virtual APs or the AP groups were defined on lower nodes. This issue was observed in Mobility Master Virtual Appliance running ArubaOS 8.3.0.0.	AP-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
183464 190191	**Symptom:** Some APs failed to display interference though there was high RF interference. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 200 Series access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	200 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
183929	**Symptom:** The Edge browser did not redirect a user to the correct page after the user successfully completed Captive Portal authentication. This issue is resolved by redirecting the user to the correct page after a successful Captive Portal authentication. **Scenario:** This issue occurred when the redirect URI was not stored while storing the original URL. After successfully completing Captive Portal authentication, the user was redirected back the original URL instead of the URL with the redirect URI. This issue was observed in managed devices running ArubaOS 8.2.1.1.	Captive Portal	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
184082 184587	**Symptom:** Some APs failed to switch between Backup LMS IP and LMS IP. The fix ensures that the APs switch between Backup LMS IP and LMS IP successfully. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
184426	**Symptom:** An AP deauthenticated a client unexpectedly. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred because of an unexpected internal ageout and long connection delay. This issue was observed in 300 Series, 310 Series, 320 Series, 330 Series, 360 Series, and 370 Series access points running ArubaOS 8.2.1.0.	AP-Wireless	300 Series, 310 Series, 320 Series, 330 Series, 360 Series, and 370 Series access points	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
184786	**Symptom:** APs were not broadcasting on Virtual APs and on start up, displayed D flag, in the output of the command **show ap database**, indicating that the AP configuration either had errors or was missing, after managed devices were rebooted in a cluster. The fix ensures that the comparison of named VLAN is not case sensitive. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions in a cluster setup.	AP-Platform	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
184868	**Symptom:** The SNMP query for **OID: wlsxSysExtInternalTemparature** was displaying 0 for a Mobility Master. The fix ensures that the query displays the actual temperature. **Scenario:** This issue was observed in 7200 controllers running ArubaOS 8.2.1.1.	SNMP	7200 controllers	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
185082	**Symptom:** The Active AP Load Balancing information is not displayed in the output when the **show lc-cluster group-profile** command was executed. The fix ensures that the Active AP Load Balancing information is displayed. **Scenario:** This issue was observed in managed devices in a cluster setup are running ArubaOS 8.2.1.1 or later versions.	Cluster-Manager	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
185309	**Symptom:** Clients connected to AP-345 access points were unable to go online using TKIP encryption. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the clients were connected through bridge mode SSID using TKIP encryption. This issue was observed in AP-345 access points running ArubaOS 8.3.0.0.	AP-Wireless	AP-345 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
185508	**Symptom:** The WebUI was unresponsive after adding an additional license. The fix ensures that the WebUI works as expected. **Scenario:** This issue occurred when a user attempted to add an additional license and the Mobility Master already had 230 licenses. This issue was observed in Mobility Masters running ArubaOS 8.3.0.1.	Licensing	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.4.0.0
185597	**Symptom:** The output of the **show switches** command displayed the IPv6 address of a standby Mobility Master as **none**. The fix ensures that the output of the **show switches** command displays the IPv6 address of the standby Mobility Master. **Scenario:** This issue occurred when the **show switches** command was executed on a Mobility Master. This issue was observed in Mobility Masters running ArubaOS 8.2.1.1.	Configuration	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
185679 187734 188214 189144 189191 191414	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in APs running ArubaOS 8.2.2.0 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.2.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
186110	**Symptom:** The configuration synchronization failed and the status of the synchronization displayed **CONFIG Failure**. This issue is resolved by changing the user-role **default-iap-user-role** as a read only role. **Scenario:** This issue occurred when the **default-iap-user-role** was edited. This issue was observed in Mobility Masters running ArubaOS 8.3.0.1 or later versions.	Base OS Security	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.4.0.0
186224	**Symptom:** Clients could not connect to a bridge mode virtual AP after a VLAN assignment failure. The fix ensures that the clients connect to the virtual APs. **Scenario:** This issue occurred when the VLAN in a Mobility Master was removed causing subsequent deauthentication of all the clients associated with the virtual APs. This issue was observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions.	Station Management	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
186399	**Symptom:** ClientMatch steered clients to the same radio because of load balancing even though the BSSID of the radio and the AP were same. The fix ensures that ClientMatch does not steer the clients to the same radio. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.1.	ARM	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
186509	**Symptom:** A client failed dynamic WEP reauthentication with an AP. This issue is resolved by not dropping the unencrypted Rx EAPOL frames when dynamic WEP reauthentication is enabled. **Scenario:** This issue occurred when the wireless driver dropped unencrypted Rx EAPOL frames after the WEP key was set. This issue was observed in AP-305, AP-315, and AP-335 access points operating in bridge mode and running ArubaOS 8.2.1.1	AP-Wireless	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
186608	**Symptom:** The **datapath** process in a managed device crashed while initiating a Skype call from a wireless client. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.1 or later versions.	Controller-Datapath	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
186815	**Symptom:** The CPPM profile entries were not updated in the node hierarchies when the CPPM profile was configured in AirGroup server. The fix ensures that the CPPM profile entries are updated in different node hierarchies. **Scenario:** This issue occurred when the user added or deleted RFC 3576 servers by executing the **airgroupprofile cppm rfc-3576-server <rfc-3576-server>** command. This issue was observed in Mobility Master running ArubaOS 8.2.1.1 or later versions.	AirGroup	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
187027	**Symptom:** A user cannot import a CSV file that contained guest information on a managed device. This issue is resolved by removing the extra space from the sponsor email address field in the CSV file during file extraction. **Scenario:** This issue occurred when a sponsor email address was given as an input in the CSV file and an extra space was added to the sponsor email address field during the file extraction. This issue was observed in managed devices running ArubaOS 8.3.0.0 or later versions.	Guest Provisioning	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
187191	**Symptom:** Wireless clients were not added as OpenFlow hosts in the Mobility Master. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.	SDN	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
187364	**Symptom:** The configuration changes made to the system-defined **validuser** ACL rules were not applied upon reboot of a managed device. The fix ensures that the configuration changes in the ACL rule are applied instead of the default ACL rules. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
187390	**Symptom:** VoIP clients faced connectivity issues when IPv6 was enabled. The fix ensures that UCC functionalities work as expected in an IPv6 cluster. **Scenario:** This issue occurred when UCC flows were processed using the IPv6 address instead of the IPv4 address of the managed device in an IPv6 cluster. This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	UCC	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
187696	**Symptom:** A Mobility Master failed to install correct netdestination into datapath causing guest captive portal to fail. The fix ensures that the Mobility Master sends netdestination updates to datapath. **Scenario:** This issue occurred when: ■ netdestination was used in captive portal ACL. ■ there were multiple PAPI failures. This issue was observed in Mobility Masters running ArubaOS 8.3.0.1 or later versions.	Base OS Security	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.4.0.0
187735	**Symptom:** The configured MTU value of an AP was incorrect in the managed device. The fix ensures that the correct MTU value is reflected in the managed device. **Scenario:** This issue occurred when the AP was rebooted after configuring the SAP MTU in the AP system-profile. This issue was observed in access points running ArubaOS 8.1.0.0 or later versions.	Mesh	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.4.0.0
187744 189352 191419	**Symptom:** APs were rebooting randomly. The log files for the event listed the reason as Reboot caused by kernel panic: Fatal exception. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when EIRP table was not sent to the AP when either 2G or 5G channel list was empty. This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	AP Regulatory	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
187745	**Symptom:** AP requested for less Poe-at power in the LLDP negotiation, which lead to insufficient power. The fix ensures that the AP requests for 25.5W instead of 20.8W for Poe-at LLDP negotiation. **Scenario:** This issue occurred when the AP requested for 20.8W. This issue was observed in AP-377 running ArubaOS 8.3.0.2 or later versions.	AP-Wireless	AP-377 access points	ArubaOS 8.3.0.2	ArubaOS 8.4.0.0
187819 188349	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the reboot as **Reboot caused by kernel panic: Watchdog timeout received**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred due to a large number of debug messages printed in the log files. This issue was observed in AP-335 access points running ArubaOS 8.2.1.1 or later versions.	AP-Wireless	AP-335 access points	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
187865	**Symptom:** User was able to telnet the access point although the telnet option was disabled in the ap-system profile. The fix ensures that the user cannot telnet the access point if the option is disabled in the ap-system profile. **Scenario:** This issue was observed in stand-alone 7220 controllers running ArubaOS 8.3.0.0 or later versions.	AP-Platform	7220 controllers	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
187939	**Symptom:** The **authentication** process in a managed device leaked memory and generated a crash report. Improvements to memory management resolved this issue. **Scenario:** This issue occurred when the 802.1X authentication load was high. This issue was observed in AP-377 running ArubaOS 8.3.0.2 or later versions.	802.1X	All platforms	ArubaOS 8.4.0.0	ArubaOS 8.4.0.0
188025	**Symptom:** PEFNG license count was displayed incorrectly in the **Mobility Master > Configuration > License > License usage > PEF** column. The fix ensures that the correct license count is displayed. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.2.1.1 or later versions.	WebUI	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
188037	**Symptom:** Mesh APs were coming up unlicensed on a Data zone. The fix ensures that for a mesh AP in a MultiZone, no licenses are consumed in Data zone but in a Primary zone, the mesh APs consume licenses even if there are no Virtual APs for that mesh AP. **Scenario:** This issue occurred when MultiZone is enabled and a virtual AP is assigned to the Data zone. This issue was observed in APs connected to managed devices running ArubaOS 8.2.1.1 or later versions in Mesh mode.	AP-Platform	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
188135 188987	**Symptom:** The **STM** process in a managed device displayed the **Dynamic BSS tunnel could not be setup for bssid** error message. The fix ensures that the error message is not displayed on the managed device. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	AP-Platform	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
188497	**Symptom:** A managed device sent RSSI AMON data to **mgmt-server destinations** even though the location was disabled in **mgmt-server profile**. The fix ensures that the managed device does not send RSSI AMON data to **mgmt-server destination**. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.1.1 or later versions.	AMON	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
188517	**Symptom:** Multiple APs crashed unexpectedly. The fix ensures that the APs work as expected. **Scenario:** This issue was observed in APs running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
188601	**Symptom:** A managed device was unable to synchronize the configuration with the Mobility Master. This issue is resolved by not allowing the deletion of any system-generated ACL from the user role. **Scenario:** This issue occurred during the deletion of a system-generated ACL from a user role. This issue was observed in managed devices running ArubaOS 8.2.1.0.	Base OS Security	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
188659	**Symptom:** An SNMP walk reported incorrect values for Broadcast/ Multicast packets. The fix ensures that the correct values are reported during SNMP walk. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.3.0.3 or later versions.	SNMP	All platforms	ArubaOS 8.3.0.3	ArubaOS 8.4.0.0
188667 190096 190508	**Symptom:** APs were unable to boot on a stand-alone controller and APs rebooted with the reason, **Error:RC_ERROR_ISAKMP_N_CERT_ SELFSIGNED_VERIFY_FAILED**. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue occurred when CPsec was enabled. This issue was observed in AP-303 access points running ArubaOS 8.3.0.0 or later versions on a Mobility Controller Virtual Appliance.	AP-Platform	AP-303 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
188978	**Symptom:** During RADIUS session timeout, fixed 802.1X deauthentication occurred followed by 802.1X reauthentication. This issue is resolved by correctly populating the termination-action in the RADIUS AV pairs. **Scenario:** This issue occurred when the termination-action in the RADIUS AV pairs was not populated correctly. This issue was observed in managed devices running ArubaOS 8.4.0.0.	802.1X	All platforms	ArubaOS 8.4.0.0	ArubaOS 8.4.0.0
189024	**Symptom:** An AP did not receive an IP address when its ENET1 port was used as uplink and the ENET0 port was simultaneously connected to a client. The fix ensures that the ENET1 port is default uplink when both ENET0 and ENET1 ports are L2 connected. Also, the ENET0 port can be provisioned as default uplink too. **Scenario:** This issue was observed in AP-318, AP-374, AP-375, and AP-377 access points running ArubaOS 8.3.0.0.	AP-Platform	AP-318, AP-374, AP-375, and AP-377 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
189035 189956 189981	**Symptom:** Users were unable to connect to AirGroup servers intermittently. The fix ensures that the users are able to connect to AirGroup servers. **Scenario:** This issue occurred when the CPPM queries sent from the clients did not reach the AirGroup servers. This issue was observed in Mobility Master Hardware Appliances running ArubaOS 8.2.1.0 in a master-standby topology.	AirGroup	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0
189064	**Symptom:** Jabber desktop sharing caused unwanted traffic to reach a Mobility Master. Withdrawing the support for Jabber desktop sharing resolved this issue. **Scenario:** This issue occurred because of the wide range of ports being used by Jabber. This issue was observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions.	UCC	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
189159	**Symptom:** IP phones experienced voice gaps and about 500 msec packet losses periodically. The fix ensures that only the 20 MHz setting is considered. **Scenario:** This issue occurred as APs enabled **Extended Capabilities (ID 127) 20/40 BSS Coexistence Management Support** in the beacon although only 20 MHz is set by the user. This led to off-channel scanning and hence, the packet loss. 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 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
189270	**Symptom:** An attribute (**Filter-ID**) that assigns VLANs to the users was missing from a managed device even though the attribute was available in the device configuration settings. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices in a cluster setup running ArubaOS 8.2.1.1.	Configuration	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
189353	**Symptom:** The output of the **show ap arm client-match neighbors ap-name** command displayed very high entries. The fix ensures that the command output is displayed correctly. **Scenario:** This issue occurred when the command output was displayed in a loop. This issue was observed in Mobility Masters running ArubaOS 8.2.1.1 or later versions.	ARM	All platforms	ArubaOS 8.2.1.1	ArubaOS 8.4.0.0
189486 189904 190298	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred in a cluster setup when an IPv6 client initiated and stopped multiple FTP transfers. This issue was observed in 7200 Series controllers running ArubaOS 8.3.0.2 or later versions.	Controller-Datapath	7200 Series controllers	ArubaOS 8.3.0.2	ArubaOS 8.4.0.0
189521	**Symptom:** An AP displayed high rate of PHY errors when hybrid - spectrum mode was enabled. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 300 Series access points running ArubaOS 8.0.0.0 or later versions.	AP-Wireless	300 Series access points	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
189523 191049	**Symptom:** An AP that terminated on a managed device with CPsec enabled did not come up after a cluster failover. The fix ensures that the AP comes up after a cluster failover. **Scenario:** This issue occurred when a cluster failover message timed out in the AP after a cluster failover. 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 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
189539	**Symptom:** The **mDNS** process on the Mobility Master utilized memory space that is equal to or greater than the assigned value. The issue was resolved by clearing the memory and internal data structures of the **mDNS** packets. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.2.1 or later versions in a master-standby topology.	AirGroup	All platforms	ArubaOS 8.2.2.1	ArubaOS 8.4.0.0
189552	**Symptom:** IP access restrictions on VLAN interface did not work as expected and did not block expected traffic. The fix ensures that the VLAN interface IP access group traffic restrictions block the correct traffic. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.2.1 or later versions.	VLAN	All platforms	ArubaOS 8.3.0.3	ArubaOS 8.4.0.0
189722	**Symptom:** Configuration failure was observed on a Mobility Master in standby mode. The fix ensures that all configurations are applied to the standby Mobility Master. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.2.2.1 or later versions.	Logging	All platforms	ArubaOS 8.2.2.1	ArubaOS 8.4.0.0
189795	**Symptom:** A mesh point failed to come up after the mesh portal was rebooted. The fix ensures that mesh point comes up on a Mobility Master. **Scenario:** This issue occurred when the Mobility Master failed to set up a mesh link. This issue was observed in Mobility Masters running ArubaOS 8.3.0.2 or later versions.	Mesh	All platforms	ArubaOS 8.3.0.2	ArubaOS 8.4.0.0
190291	**Symptom:** An error message, **Max CP firewall limit (32) reached** was displayed even when less than the maximum number of ACE 32 entries were added to the device using the **firewall cp** command. The fix ensures that the error message is displayed only when the maximum limit is reached. **Scenario:** This issue occurred when firewall rules were configured and deleted from multiple managed devices. This issue was observed in Mobility Masters running ArubaOS 8.2.1.0 or later versions.	Base OS Security	All platforms	ArubaOS 8.2.1.0	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
190347	**Symptom:** The user was unable to add untrusted VLANs to interface from the **Mobility Master > Interfaces > Ports > Allowed VLANs> Add Allowed VLAN > Trust** page of the WebUI. The fix ensures that the user can add untrusted VLANs using the WebUI. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.3.0.3 or later versions.	WebUI	All platforms	ArubaOS 8.3.0.3	ArubaOS 8.4.0.0
190396	**Symptom:** The console logs of an AP showed the standby IP address as 0.0.0.0. During a failover, the AP lost connectivity with the standby managed device and it did not come up. The fix ensures that the AP failover occurs when the standby managed device is up and the AP obtains the correct IP address of the standby managed device. **Scenario:** This issue occurred during a cluster failover when an AP lost connectivity with the standby managed device. This issue was observed in APs running ArubaOS 8.3.0.1.	AP Datapath	All platforms	ArubaOS 8.3.0.1	ArubaOS 8.4.0.0
190448	**Symptom:** A few APs did not get HA standby IP address and failed to connect to a controller. The fix ensures that the AP connects to the controller. **Scenario:** This issue was observed in stand-alone controllers running ArubaOS 8.3.0.3 or later versions.	HA-Lite	All platforms	ArubaOS 8.3.0.3	ArubaOS 8.4.0.0
190542	**Symptom:** A radio experienced a high number of resets in APs. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the APs were in Air Monitor mode. This issue was observed in AP-335 access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-335 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
190571	**Symptom:** An AP failed to come up. The fix ensures that the AP works as expected **Scenario:** This issue occurred on an AP with EST key type **X9.62/SECG curve**. This issue was observed in AP-303H access points running ArubaOS 8.2.0.0 or later versions.	CPsec	AP-303H access points	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0
190677 191836 191870	**Symptom:** The **DDS** process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.2.2 in a Mobility Master-Managed Device topology.	DDS	All platforms	ArubaOS 8.2.2.2	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
190772	**Symptom:** The **show tech-support** command displayed incorrect output. This issue is resolved by executing the **show tech-support** command in **/mm** node. **Scenario:** This issue was observed in Mobility Masters running ArubaOS 8.4.0.0.	Configuration	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
190778	**Symptom:** All the managed devices were displayed as DOWN when the **show switches** command was executed. The fix ensures that the correct status is displayed when the **show switches** command is executed. **Scenario:** This issue occurred when the Mobility Master lost all routes to the active VPNC. This issue was observed in Mobility Masters running ArubaOS 8.4.0.0.	IPsec	All platforms	ArubaOS 8.4.0.0	ArubaOS 8.4.0.0
190795	**Symptom:** An AP failed to come up. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when a Remote AP was configured to use PPPoE. This issue was observed in AP-203R, AP-303H, and AP-305 access points running ArubaOS 8.3.0.3 or later versions.	Remote AP	AP-203R, AP-303H, and AP-305 access points	ArubaOS 8.3.0.3	ArubaOS 8.4.0.0
190797	**Symptom:** Incremental Frame Check Sequence received (FCS Rx) errors are observed in APs. Enhancements to the wireless driver resolved this issue. **Scenario:** The issue occurred when the APs were connected using a cable with length greater than 100 meters. This issue was observed in AP-365 access points running ArubaOS 8.3.0.0 or later versions.	AP-Wireless	AP-365 access points	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
190925	**Symptom:** Managed Device did not forward broadcast ARP packets to silent clients through GRE tunnels although the **no suppress-arp** parameter was set. The fix ensures that the **no suppress-arp** command overrides the **broadcast-filter arp** command to allow unknown broadcast ARP packets through GRE Tunnels. **Scenario:** This issue was observed in managed devices running ArubaOS 8.3.0.3 or later versions.	Controller - Datapath	All platforms	ArubaOS 8.3.0.3	ArubaOS 8.4.0.0

Table 6: *Resolved Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
190957	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for this event as **Hardware Watchdog Reset (Intent:cause:register 54:86:0:8020)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in 7280 controllers running ArubaOS 8.3.0.3 or later versions.	Controller-Datapath	7280 controllers	ArubaOS 8.3.0.3	ArubaOS 8.4.0.0
191092 191483	**Symptom:** Multiple processes in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected. **Scenario:** The issue occurred due to a memory leak and high CPU utilization on the managed device. This issue was observed in managed devices running ArubaOS 8.2.0.2 or later versions.	SDN	All platforms	ArubaOS 8.2.0.2	ArubaOS 8.4.0.0
191276	**Symptom:** Some clients get disconnected with error message **idle time out**. The fix ensures that the clients do not get disconnected. **Scenario:** This issue occurred when clients received user idle time out value of 300 seconds instead of 43200 seconds. This issue was observed in 7200 Series controllers running ArubaOS 8.0.0.0 or later versions.	Base OS Security	7200 Series controllers	ArubaOS 8.0.0.0	ArubaOS 8.4.0.0
192112	**Symptom:** A managed device showed Skype error messages in the HTTPD logs and dropped XML messages that were meant for UCM. The visibility of Skype for Business call records were missing from the WebUI. The fix ensures that the managed device works as expected and does not drop the XML messages that are meant for UCM. **Scenario:** This issue was observed in managed devices running ArubaOS 8.2.2.2.	Web Server	All platforms	ArubaOS 8.2.2.2	ArubaOS 8.4.0.0
192345	**Symptom:** Configuration failure occurred when IoT transport profile was used in a managed device. The fix ensures that the configuration failure does not occur on the managed device. **Scenario:** This issue was observed in Mobility Masters and managed devices running ArubaOS 8.4.0.0 and ArubaOS 8.3.0.0 respectively in a Mobility Master-Managed Device topology.	BLE	All platforms	ArubaOS 8.3.0.0	ArubaOS 8.4.0.0
192468	**Symptom:** An AP in IPv6 environment did not preempt to the active managed device although preemption was enabled. The fix ensures that the AP preempts to the active managed device when required. **Scenario:** This issue was observed in access points running ArubaOS 8.2.0.0 in an IPv6 high-availability topology.	AP-Platform	All platforms	ArubaOS 8.2.0.0	ArubaOS 8.4.0.0

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

Limitations

Following is the limitation observed in this release.

Fast BSS Transition

802.11r feature is not supported in WLAN SSIDs using WPA-3 security.

Zigbee Radio Mode

For Zigbee radio mode, there is no support provided through the WebUI.

Role Based VLAN

DUR Role Based VLAN is not supported for wireless authenticated users and is supported only for Dynamic Segmentation users.

Known Issues for 510 Series Access Points

Following are the known issues observed in this release.

Table 7: *Known Issues for 510 Series access Points in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
185579	**Symptom:** Invalid transmissions are observed when an AP boots up in the Air Monitor mode. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
186310 188308	**Symptom:** An AP sends multicast traffic to clients at a lower rate. **Scenario:** This issue occurs when **bcmc-optimization** is enabled and DMO is disabled. This issue is observed in AP-303P and AP-515 access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	AP-303P and AP-515 access points	ArubaOS 8.4.0.0
186918	**Symptom:** Air time fairness feature is not functional although the value of the **shaping-policy** parameter is set to **default-access**. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
186957	**Symptom:** The beacon and probe response packets do not display the country capabilities information element for 5 GHz non-DFS channel. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
188308	**Symptom:** Video multicast frames are transmitted at the lowest configured rate on an AP. **Scenario:** This issue occurs when **mcast-rate-opt** parameter is enabled on the AP. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
188356 190747	**Symptom:** Clients reconnect to the AP frequently as the effective rates and advertised rates are not the same. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** Ensure that the **g-basic-rates <mbps>** and **g-tx-rates <mbps>** parameters of the wlan SSID profile are set to the default value.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
188717	**Symptom:** CSR does not work for 2G and 5G networks. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0 or later versions. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0

Table 7: *Known Issues for 510 Series access Points in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
189298	**Symptom:** System LED is blinking with a green light after an AP connects to a managed device and boots up. **Scenario:** This issue occurs when 2.4 GHz radio is disabled. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** Modify any one of the 2.4 GHz radio profiles.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
189519	**Symptom:** Older Intel driver chipsets are unable to detect SSIDs with **high efficiency** enabled on the AP. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0 where the Intel driver is running a version prior to 20.70.x.x version. **Workaround:** Upgrade the Intel drivers to the latest version or disable the **high efficiency** parameter in the SSID profile by executing the following command : **(host) [node] # wlan he-ssid-profile default no high-efficiency-enable**	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
190654 193387	**Symptom:** APs reboot unexpectedly and experience packet loss. The log file lists the reason for the event as **Kernel Panic**. **Scenario:** This issue occurs when Jumbo frames are enabled between a managed device and the AP. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** Disable Jumbo frames or set the framed-mtu <mtu> to 1500 or 1578 in the AP System profile.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
191669	**Symptom:** The performance of **Iperf throughput** test drops when a **Multicast** process runs at the same time on an AP. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0

Table 7: *Known Issues for 510 Series access Points in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
191774	**Symptom:** Some APs running in 2G radio mode fail to transit from 1ss to 2ss power mode. **Scenario:** This issue occurs if there is a delay in the LLDP negotiation between an AP and a managed device. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
192771 189897	**Symptom:** The value returned from noise floor calculation is inaccurate when there is interference. **Scenario:** This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0
193223	**Symptom:** An AP took longer than usual to transfer packets to clients. **Scenario:** This issue occurs when a Surface Pro client does not aggregate traffic. This issue is observed in 510 Series access points running ArubaOS 8.4.0.0. **Workaround:** Disable aggregation for transmission using the **wlan ht-ssid-profile <> no mpdu-agg** command.	AP-Wireless	510 Series access points	ArubaOS 8.4.0.0

Known Issues

The following known issues are observed in ArubaOS 8.4.0.0.

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
124928	**Symptom:** The route-cache does not update the IPsec tunnel IDs correctly after a failover link comes up. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	Routing	All platforms	ArubaOS 8.3.0.0
151952	**Symptom:** When a managed device reboots, APs and clients boot without IP addresses and other fields. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None.	Monitoring	All platforms	ArubaOS 8.0.1.0
159222 179137	**Symptom:** The number of clients displayed in the active-standby IP field on the Mobility Master dashboard is incorrect. **Scenario:** This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.1.0.0
164332	**Symptom:** The IPM default list for an AP is not displayed even though the IPM feature is enabled in the WebUI. **Scenario:** This issue is observed in APs running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.2.0.0
164916	**Symptom:** A managed device does not display an error when executing the **show license-pool-profile-root** command. **Scenario:** This issue occurs when the managed device is a license client. This issue is observed in managed devices running ArubaOS 8.2.0.0. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.2.0.0
166937	**Symptom:** The AirGroup process in a managed device stops responding. **Scenario:** This issue occurs when an AirGroup profile is changed in a managed device with mDNS servers and users. This issue is observed in managed devices running ArubaOS 8.2.0.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.2.0.0
167795	**Symptom:** An AP fails to detect a microwave inverter. **Scenario:** This issue occurs in APs where either the **Hybrid** or **Spectrum** mode in 2.4 GHz is enabled. This issue is observed in AP-345 access points running ArubaOS 8.3.0.0. or later versions. **Workaround:** None.	Spectrum-Interferer Classification	AP-345 access points	ArubaOS 8.3.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
168457	**Symptom:** The license count in **Mobility Master > Licenses** page in the WebUI does not reflect the ACR license usage. **Scenario:** This issue occurs when the license count is not communicated to the applications running on Standby Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.2.0.0
170058	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7200 Series controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Datapath	7200 Series controllers	ArubaOS 8.0.0.0
170105 171721	**Symptom:** Some clients get deauthenticated and fail to connect to an AP. The log files list the reason for this event as **Reason Ptk Challenge Failed** and **deauth_reason 52**. **Scenario:** This issue is observed in APs running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.0.0.0
171246 187010 187759 187764 188678 188679 188681 189142	**Symptom:** A managed device crashes and reboots unexpectedly. **Scenario:** This issue is observed in 7240XM controllers running ArubaOS 8.2.0.0. in a Mobility Master - Managed Device topology. **Workaround:** None.	Controller-Datapath	7240XM controllers	ArubaOS 8.2.1.0
171397	**Symptom:** The WAN health-check is enabled in the default configuration. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.1. **Workaround:** None.	Branch Controller	All platforms	ArubaOS 8.2.0.1
172942	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2**. **Scenario:** This issue is observed in 7240XM controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Datapath	7240XM controllers	ArubaOS 8.0.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
173070	**Symptom:** The number of clients displayed in the AppRF dashboard in the WebUI is different from those that are displayed in the CLI. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Firewall Visibility	All platforms	ArubaOS 8.0.0.0
175233	**Symptom:** A client loses ping packets. **Scenario:** This issue occurs when the client aware scanning is enabled. This issue is observed in access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.4.0.0
175636	**Symptom:** An AP retransmits the ping packets twice even though the channel is not busy. **Scenario:** This issue occurs when dual 5 GHz radio channel is enabled. This issue is observed in 340 Series access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	340 Series access points	ArubaOS 8.3.0.0
176435	**Symptom:** The IP health-check in a managed device shows **Unreachable** although the outside network was reachable. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.2. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.2.0.2
176879	**Symptom:** Some clients are unable to pass traffic due to unresponsive ARP gateway. **Scenario:** This issue occurs because the device detects AES replay. This issue is observed in APs running ArubaOS 8.0.0.0 or later versions. **Workaround:** Moving to a different AP restores connectivity.	AP-Wireless	All platforms	ArubaOS 8.0.0.0
176991	**Symptom:** The **Configuration > Roles and Policies > Roles** table does not display **denyall and default-iap-user-role** roles. **Scenario:** This issue is observed in 7010 controllers running ArubaOS 8.2.0.2 or later versions. **Workaround:** Reload the controller to see **Denyall** in the WebUI.	Authentication	7010controllers	ArubaOS 8.2.0.2
177001	**Symptom:** An AP reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt" - code: bad PC value**. **Scenario:** This issue is observed in AP-315 access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	AP-315 access points	ArubaOS 8.3.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
177283	**Symptom:** Some APs experience packet loss and display the error message, **wl0: wlc_ampdu_watchdog: no memory**. **Scenario:** This issue is observed in 340 Series access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	340 Series access points	ArubaOS 8.3.0.0
177297	**Symptom:** Some APs display duplicate netdestination entries after an AP failover and switchover to standby mode. **Scenario:** This issue is observed in managed devices in a cluster setup running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	Cluster-Manager	All platforms	ArubaOS 8.1.0.0
177664	**Symptom:** An AP reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt (PC is at irq_work_run)**. **Scenario:** This issue is observed in AP-315 access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	AP-315 access points	ArubaOS 8.3.0.0
178008	**Symptom:** Some APs stop sending beacon frames and disconnect all clients. **Scenario:** This issue occurs when the static channel of the AP is changed from 36E to 36S. This issue is observed in 340 Series access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	340 Series access points	ArubaOS 8.3.0.0
178124	**Symptom:** Redirects fail for large cookies on Edge browser. **Scenario:** This issue occurs when: ■ the maximum HTTP header size is 8000. ■ requests that have large or higher number of cookies turn into bad requests. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Web Server	All platforms	ArubaOS 8.0.0.0
178711	**Symptom:** Wireless clients using PBR are unable to route traffic. **Scenario:** This issue occurs when IPsec tunnel is enabled on the Mobility Master. This issue is observed in Mobility Masters running ArubaOS 8.2.1.0. **Workaround:** None.	Policy Based Routing	All platforms	ArubaOS 8.2.1.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
179219	**Symptom:** AirMatch skips a number of APs and deploys a limited number of APs. **Scenario:** This issue occurs after the timezone is changed. This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	AirMatch	All platforms	ArubaOS 8.3.0.0
179307	**Symptom:** The **DHCP** process crashes in a managed device. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	DHCP	All platforms	ArubaOS 8.0.1.0
179356	**Symptom:** A managed device crashes and reboots unexpectedly. Once the managed device reboots, it fails to create the nexthop index and stops communicating with the Mobility Master. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
179723 188611 189642	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in 300 Series access points running ArubaOS 8.2.1.0 or later versions. **Workaround:** None.	AP-Wireless	300 Series access points	ArubaOS 8.2.1.0
180349	**Symptom:** The user is not able to disable the **prohibit ip-spoofing** using the **Configuration > Services > Firewall > Prohibit IP spoofing** check box in the WebUI. **Scenario:** This issue was observed in a managed devices running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.0
180383	**Symptom:** A client is deauthenticated unexpectedly. **Scenario:** This issue occurs when the User Anchor Controller (UAC) is down. This issue is observed in managed devices running ArubaOS 8.2.1.0 in a cluster topology. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.2.1.0
180571	**Symptom:** Some clients experience a sudden decrease in the network speed. **Scenario:** This issue occurs when BA-MSDU and jumbo frames are enabled on a managed device. The managed device creates TCP retransmits and multiple duplicate packets, causing the speed to drop. This issue is observed in managed devices running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
180973	**Symptom:** A managed device does not steer traffic as expected. **Scenario:** This issue occurs when a probe profile with UDP mode and corresponding threshold profile with **mos** value are configured. This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.0
181026	**Symptom:** Wireless clients are assigned default VLAN and MAC authentication roles after failing 802.1X authentication. **Scenario:** This issue occurs when a wireless client passes the MAC authentication but fails the 802.1X authentication. This issue is observed in 7005 controllers in a stand-alone mode running ArubaOS 8.2.1.0 or later versions. **Workaround:** None.	Base OS Security	7005 controllers	ArubaOS 8.2.1.0
182054	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Out of memory**. **Scenario:** This issue is observed in AP-335 access points running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	AP-Wireless	AP-335 access points	ArubaOS 8.2.1.1
182224	**Symptom:** The **License Successfully Claimed** message is not displayed for a successful license registration in the **Mobility Master > Configuration > Licenses > Aruba Support Portal (ASP)** page of the WebUI. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0. **Workaround:** None	WebUI	All platforms	ArubaOS 8.4.0.0
182409	**Symptom:** The **Eth0** port of an AP that operates in dual 5 GHz mode or dual band mode drops packets. **Scenario:** This issue occurs when an AP uses 1 Gbps uplink and the radios receive more than 1 Gbps traffic. This issue is observed in 340 Series access points running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	AP-Platform	340 Series access points	ArubaOS 8.2.1.1
182684	**Symptom:** Wireless clients are unable to connect to the VRRP IP of a Mobility Master. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
182885	**Symptom:** The aggregate number of VIA or PEFV licenses installed on a particular Mobility Master is not displayed in the **Mobility Master > Configuration > Licenses > Aruba Support Portal (ASP)** page of the WebUI. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0. **Workaround:** None	WebUI	All platforms	ArubaOS 8.4.0.0
183031	**Symptom:** The **IP address** column under **Dashboard > Overview > Wired clients** displays only one IP address. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
183128	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue is observed in AP-315 access points running ArubaOS 8.3.0.0. **Workaround:** None.	AP-Wireless	AP-315 access points	ArubaOS 8.3.0.0
183178	**Symptom:** A Remote AP fails to come up when connected to a 4G dongle. **Scenario:** This issue is observed on AP-303H access points running ArubaOS 8.3.0.0 or later versions. **Workaround:** None.	Remote AP	AP-303H access points	ArubaOS 8.3.0.0
183192	**Symptom:** Unable to check the ASP connection status of the standby Mobility Master from the **Mobility Master > Configuration > Licenses > Aruba Support Portal (ASP)** page in the WebUI. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0. **Workaround:** View the standby Mobility Master ASP connection status using CLI, **show asp status standby** command in the active Mobility Master.	WebUI	All platforms	ArubaOS 8.4.0.0
183193	**Symptom:** User is unable to use the **Enter** key to sign in from the **Signin to ASP** popup window after entering the correct credentials. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
183213	**Symptom:** ASP account information is not displayed in the **Mobility Master > Configuration > System > General > Aruba Support Portal** page in the WebUI. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0. **Workaround:** View the ASP account information by executing the command, **show asp account-info**.	WebUI	All platforms	ArubaOS 8.4.0.0
183325	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0
183430	**Symptom:** User is unable to move from external licensing server mode to ASP mode automatically without manually enabling the ASP profile. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.4.0.0
184030	**Symptom:** The cumulative count of licenses allocated and installed from both active and standby Mobility Masters is not displayed once the active Mobility Master comes up after a failover. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0. **Workaround:** To view the cumulative count of licenses allocated and installed from both active and standby Mobility Masters, navigate to **Mobility Master > Configuration > License > License Inventory** tab and click **update now** link, once the Mobility Master comes up after failover.	Licensing	All platforms	ArubaOS 8.4.0.0
183580	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue is observed in AP-303H access points running ArubaOS 8.2.1.1. **Workaround:** None.	AP-Wireless	AP-303H access points	ArubaOS 8.2.1.1

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
183973 186151	**Symptom:** Wireless clients failed to reconnect to the SSID after being dropped from the network. The managed device lists the following error messages: ■ **user repkey change failed** ■ **macuser repkey change failed** **Scenario:** This issue occurs when the GSM slot in a user channel is not deleted, which reduces the available GSM slots to zero. This issue is observed in managed devices running ArubaOS 8.2.1.1. **Workaround:** Reboot the managed device.	Base OS Security	All platforms	ArubaOS 8.2.1.1
184104	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW HANG (PCIE error(s) detected)** **Scenario:** This issue is observed in AP-335 access points running ArubaOS 8.2.1.1. **Workaround:** Reboot the managed device.	AP-Wireless	AP-335 access points	ArubaOS 8.2.1.1
184849	**Symptom:** Clients are unable to make or receive calls. A **Network busy** error message is displayed. **Scenario:** This issue occurs when WMM is disabled on the managed device. This issue is observed in AP-315 access points running ArubaOS 8.2.1.1. **Workaround:** None.	WMM	AP-315 access points	ArubaOS 8.2.1.1
185165	**Symptom:** A managed device crashes unexpectedly. The log files list the reason for this event as **Reboot Cause: Reboot by Upgrade Manager Intent:cause:register 60:86:50:60).** **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	Controller platform	All platforms	ArubaOS 8.2.1.1
185499	**Symptom:** Managed devices at the branch office are unable to receive IP address from the branch uplink pool. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.0 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.2.1.0
185561	**Symptom:** A client experiences pixelated video when streaming a multicast video stream. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	Multicast	All platforms	ArubaOS 8.3.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
185647	**Symptom:** A controller experiences low throughput while transmitting data through per user tunneled-node tunnels. **Scenario:** This issue occurs when the transmitted data packets are lesser than 256 bytes. This issue is observed in stand-alone controllers running ArubaOS 8.4.0.0. **Workaround:** None.	Tunnel-Node-Manager	All platforms	ArubaOS 8.4.0.0
185687	**Symptom:** APs crash and reboot unexpectedly. The log files lists the reason for the event as **Fatal exception: Data Cache Parity Error**. **Scenario:** This issue is observed in AP-335 access points running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	AP-Wireless	AP-335 access points	ArubaOS 8.2.1.1
187572	**Symptom:** All the upstream routers are receiving a lot of OSPF log errors. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.0 or later versions. **Workaround:** None.	OSPF	All platforms	ArubaOS 8.1.0.0
185834	**Symptom:** Some clients face a delay in receiving the IP address using a DHCP server. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	DHCP	7210 controllers	ArubaOS 8.0.0.0
185873	**Symptom:** The hotspot-shield application is not classified for some Android clients. **Scenario:** This issue occurs as the android client does not provide support for this application. This issue is observed in 7240 controllers running ArubaOS 8.3.0.2 or later versions. **Workaround:** None.	DPI	7240 controllers	ArubaOS 8.3.0.2
185938	**Symptom:** A managed device crashes and displays the **profmgr Module crashed** message. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.0.1 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.2.0.1
186324 192783	**Symptom:** The **Dashboard** > **Infrastructure** > **Cluster** page displays only the wireless clients count and not wired or remote count of PUTN clients. **Scenario:** This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
186739	**Symptom:** A managed device loses the IP address information during reboot of the Mobility Master due to power cycle failure. **Scenario:** This issue occurs in managed devices that are configured by zero-touch provisioning. This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. **Workaround:** ■ Set the secondary master IP on VLAN 4094 when the managed device is configured by zero-touch provisioning. ■ Do not change the master IP to any VLAN other than the one configured in the setup dialog.	Configuration	All platforms	ArubaOS 8.2.1.1
187033	**Symptom:** The **Usage** page under **Dashboard** > **Overview** does not display the transmitted and received throughput data (bps) for PUTN clients. **Scenario:** This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
187098	**Symptom:** Firewall DNS names do not age out leading to high CPU utilization in datapath. **Scenario:** This issue occurs when a large number of netdestinations with many name based entries are configured on a Mobility Master. These netdestination names get resolved to the DNS IP addresses which in turn retain the firewall DNS names causing CPU over utilization. This issue is observed in Mobility Masters running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0
187411	**Symptom:** The **mdns** and **authentication** processes consume high memory in a managed device although AirGroup is disabled. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.3.0.0
187621	**Symptom:** Some wireless clients face intermittent VRRP heartbeat drops. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	VRRP	All platforms	ArubaOS 8.0.0.0
187729	**Symptom:** Some wireless clients fail to get authenticated when the authentication process utilization exceeded 100%. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.0.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
187884	**Symptom:** A mesh point that is behind a remote mesh portal does not receive an IP address. **Scenario:** This issue occurs when the channel of a mesh point is changed. This issue is observed in access points running ArubaOS 8.3.0.0. **Workaround:** None.	Mesh	All platforms	ArubaOS 8.3.0.0
188018 188011 188954	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this event as **Reboot caused by kernel panic: Rebooting the AP because of FW HANG.** **Scenario:** This issue is observed in 300 Series access points running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	AP-Wireless	300 Series access points	ArubaOS 8.0.0.0
188021	**Symptom:** A managed device generates the following console error **|snmp| An internal system error has occurred at file ../unix/aruba_main.c function snmpRequestProcessing line 704 error Cannot send snmp response**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.0. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.3.0.0
188429	**Symptom:** A total of 10 capacity licenses are allowed per allocation attempt, with a maximum of 4 per type. A validation message for the same is not displayed when the count exceeds 10. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** Allocate licenses according to the limits.	Licensing	All platforms	ArubaOS 8.4.0.0
188639	**Symptom:** The **Access Points** page under **Managed Network** > **Dashboard** becomes unresponsive and does not display any information. **Scenario:** This issue occurs when the Mobility Controller WebUI is accessed using Firefox browser. This issue is observed in Mobility Controllers running ArubaOS 8.4.0.0. **Workaround:** Switch to Google Chrome browser.	WebUI	All platforms	ArubaOS 8.4.0.0
189012	**Symptom:** License synchronizing message, **Status: Error, License syncing is already in progress, please try later**, is displayed as an error instead of a warning or an information. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.4.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
189134	**Symptom:** APs are not tagging the correct VLAN ID. **Scenario:** This issue occurs when ports are set as trunk mode and the uplink and downlink packets are tagged as VLAN 2. This issue is observed in AP-303H access points running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	AP Datapath	AP-303H access points	ArubaOS 8.3.0.0
189698	**Symptom:** The Eth0 port of an AP does not work in **LACP bndl** state when the Eth1 port of the AP is down or the AP is rebooted. **Scenario:** This issue occurs when: ■ a LACP port channel is created on Eth0 and Eth1 ports of an AP. ■ the peer port of Eth1 (on switch) is shut down. This issue is observed in access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.4.0.0
189748	**Symptom:** Wired clients lose connectivity to the gateway resulting in a loss of network. **Scenario:** This issue occurs because the AP uplink port detects duplicate IP address sourced by multiple MAC addresses. This issue is observed in APs running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0.0.0
189885	**Symptom:** Managed devices fail to upgrade because of password failure during a scheduled upgrade. **Scenario:** This issue occurs when the managed devices are upgraded using the WebUI and the password is automatically picked from the configured upgrade-profile. However, the Mobility Master sends an incorrect password with the upgrade command. This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** Configure the upgrade profile for scheduling upgrade before upgrading any managed device.	WebUI	All platforms	ArubaOS 8.4.0.0
189921	**Symptom:** The **Age** column under **Dashboard** > **Overview** > **Wired Clients** table, and the **Tunneled Switches** table under **Dashboard** > **Infrastructure** display incorrect values. **Scenario:** This issue occurs when there is no NTP synchronization between the devices. This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** Perform an NTP synchronization across all connected Mobility Masters and managed devices.	WebUI	All platforms	ArubaOS 8.4.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
189952	**Symptom:** SNMP process crashes on a controller unexpectedly. **Scenario:** This issue is observed in 7200 Series controllers running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.2.1.1
190094	**Symptom:** A client connected to an AP displays low signal strength. **Scenario:** This issue occurs in 340 Series access points running ArubaOS 8.3.0.3 or later versions. **Workaround:** None.	AP-Wireless	340 Series access points	ArubaOS 8.3.0.3
190828	**Symptom:** The **Tunneled Switches** table under **Dashboard** > **Infrastructure** does not display PUTN clients running IPv6 tunnel. **Scenario:** This issue occurs in the Mobility Master UI, when the Mobility Master and managed device communicate over an IPv4 tunnel but the PUTN switch connects with the managed device over an IPv6 tunnel. This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
190869	**Symptom:** Active APs are not displayed in the **Dashboard > Access Points** page in the WebUI. **Scenario:** This issue is observed in managed devices running ArubaOS 8.3.0.3 or later versions. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.3.0.3
190873	**Symptom:** Clients get disconnected as the APs rebootstrap continuously. **Scenario:** This issue occurs when the **uplink-vlan** parameter is configured in the Remote AP mode using the **ap provisioning-profile** command. This issue is observed in AP-335 access points running ArubaOS 8.4.0.0. **Workaround:** None.	AP Datapath	AP-335 access points	ArubaOS 8.4.0.0
191050	**Symptom:** Controller crashes unexpectedly. **Scenario:** This issue occurs in 7240 controllers running ArubaOS 8.2.0.0 or later versions. **Workaround:** None.	Controller-Platform	7240 controllers	ArubaOS 8.2.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
191281	**Symptom:** Some VPN clients ignore configured certificate groups when IKEv2 is enabled. **Scenario:** This issue occurs when there is a mismatch between the certificate request and CA certificate. This issue is observed in Mobility Masters running ArubaOS 8.3.0.3 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.3.0.3
191516	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for this issue as **Kernel panic - Fatal exception running with code version 8.3.0.2**. **Scenario:** This issue is observed in APs running ArubaOS 8.3.0.2. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.3.0.2
191638	**Symptom:** Clients do not receive the multicast packets as the IPv6 streaming is not working as expected. **Scenario:** This issue occurs when there are clients on two different nodes acting as source and destination. This issue is observed in a cluster where MLD proxy is enabled and the managed devices are running ArubaOS 8.4.0.0. **Workaround:** None	Multicast	All platforms	ArubaOS 8.4.0.0
191667	**Symptom:** The **SNMP** process crashes in a managed device. **Scenario:** This issue occurs when the **SNMP** process receives a request to query the table, **wlsxSwitchAccessPointTable**. This issue is observed in 7240XM controllers running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	SNMP	7240XM controllers	ArubaOS 8.2.2.1
191811	**Symptom:** The AirGroup cache entry is dropping HP wired printers after cache expiry. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.3 or later versions. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.3.0.3
191816	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20).** **Scenario:** This issue is observed in 7205 stand-alone controllers running ArubaOS 8.2.2.0 or later versions. **Workaround:** None.	Controller-Platform	7205 standalone controllers	ArubaOS 8.2.2.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
192100	**Symptom:** The **DDS** process in managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1 or later versions. **Workaround:** None.	Base OS Security	All platforms	ArubaOS 8.2.1.1
192243	**Symptom:** A Mobility Master crashes and reboots unexpectedly. The log files list the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:40:2.** **Scenario:** This issue occurs when USB disconnects are seen from the internal flash device. This issue is observed in Mobility Controller running ArubaOS 8.2.2.2 or later versions. **Workaround:** None.	Controller- Platform	All platforms	ArubaOS 8.2.2.2
192344	**Symptom:** The **licensemgr** process crashes unexpectedly in a Mobility Master. The log file lists the reason for the event as **out of memory**. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.4.0.0
192346	**Symptom:** An AP drops Skype calls that originate from a client. **Scenario:** This issue is observed in 300 Series, 310 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points running ArubaOS 8.4.0.0 **Workaround:** None.	AP-Wireless	300 Series, 310 Series, 320 Series, 330 Series, 340 Series, 360 Series, and 370 Series access points	ArubaOS 8.4.0.0
192349	**Symptom:** The **mDNS** process running in a managed device consumes more memory than the typical threshold limit. **Scenario:** This issue is observed in managed devices running ArubaOS 8.4.0.0 **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.4.0.0
192378	**Symptom:** A client faces connectivity problem. **Scenario:** This issue occurs when the **enforce DHCP** feature is enabled. This issue is observed in managed devices running ArubaOS 8.3.0.4 **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.3.0.4

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
192430	**Symptom:** A cluster upgrade fails unexpectedly. The log file lists the reason for the event as **Image copy fail**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.1.1 in a cluster topology. **Workaround:** None.	Image Upgrade	All platforms	ArubaOS 8.2.1.1
192457	**Symptom:** The **datapath** process crashes unexpectedly in a stand-alone controller. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 8.4.0.0 **Workaround:** None.	Controller-Datapath	7210 controllers	ArubaOS 8.4.0.0
192484	**Symptom:** Some processes crash after deleting files from the storage space. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.3.0.2 or later versions. **Workaround:** None.	AirMatch	All platforms	ArubaOS 8.3.0.2
192486	**Symptom:** An Instant AP fails to receive an IP address and gets terminated. **Scenario:** This issue is observed in stand-alone controllers running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.0.0.0
192511	**Symptom:** The client usage graph of an AP displays low usage of client in the WebUI. **Scenario:** This issue is observed in 7240XM controllers running ArubaOS 8.2.2.0 in a Mobility Master-Managed Device topology. **Workaround:** None.	Station Management	7240XM controllers	ArubaOS 8.2.2.0
192618	**Symptom:** A managed device crashes and reboots unexpectedly. **Scenario:** This issue is observed in managed devices running ArubaOS 8.2.2.0 or later versions. **Workaround:** None.	Database	All platforms	ArubaOS 8.2.2.0
192642	**Symptom:** The **Dashboard > Access Points** page in a Mobility Master does not display the correct statistics of an AP. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
192645	**Symptom:** An API lists the station information twice even though the user-table has only one entry for the user. **Scenario:** This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	NBAPI-Helper	All platforms	ArubaOS 8.4.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
192649	**Symptom:** A license is not sent to a managed device. **Scenario:** This issue occurs when an external Mobility Master or a stand-alone controller is used as a licensing server. This issue is observed in managed devices running ArubaOS 8.3.0.3. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.3.0.3
186324 192783	**Symptom:** In the **Dashboard > Infrastructure > Cluster** page, clicking on **Active Clients Count** always displays the wireless clients table even if the table is empty. **Scenario:** This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
192901 194140	**Symptom:** Some APs are unable to connect to the managed device. **Scenario:** This issue occurred when the managed device is upgraded from 8.3.0.3 FIPS version to 8.4.0.0 FIPS version. This issue is observed in AP-318, AP-387, 310 Series, 320 Series, and 370 Series access points connected to managed devices running ArubaOS 8.4.0.0 FIPS version. **Workaround:** Downgrade the managed device to 8.3.0.3 FIPS version and factory reset the access points.	AP-Platform	AP-318, AP-387, 310 Series, 320 Series, and 370 Series access points	ArubaOS 8.4.0.0 FIPS
192812	**Symptom:** A per user tunneled-node client is unable to receive stream when the User Anchor Controller (UAC) fails over twice. **Scenario:** This issue occurs when two per user tunneled-node clients with different VLANs are requesting for the same stream and the **no-vlan** parameter is enabled on the per user tunneled-node clients. This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	Multicast	All platforms	ArubaOS 8.4.0.0
192915	**Symptom:** Per user tunneled-node clients received duplicate multicast packets. **Scenario:** This issue occurs in the following scenarios: ■ when multicast proxy feature is enabled on user VLANs. ■ when IGMP proxy is enabled for user VLANs. This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** None.	Tunnel-node-manager	All platforms	ArubaOS 8.4.0.0

Table 8: *Known Issues in ArubaOS 8.4.0.0*

Bug ID	Description	Component	Platform	Reported Version
193225	**Symptom:** The **Tunneled clients** column under **Dashboard > Infrastructure > Tunneled Switches** table displays zero. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.4.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
193297	**Symptom:** The **Tunneled Switches** table under **Dashboard > Infrastructure > Access Devices** displays zero **Tunneled Clients** for IPv6 tunnels between Mobility Master and the Managed Device. **Scenario:** This issue is observed in Mobility Masters running ArubaOS 8.4.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.4.0.0
193378	**Symptom:** The **all deviceClass** filter is applied by default to an IoT transport profile and when this filter is removed, it is not saved in configuration on the managed device. **Scenario:** This issue occurs when a **Telemetry-HTTPS** or **Telemetry-Websocket IoT transport** profile is created. This issue is observed in managed devices running ArubaOS 8.4.0.0 in Mobility Master-Managed Device topology **Workaround:** After creating an IoT transport profile, save the configuration, remove the **all deviceClass** filter, and save the configuration.	BLE	All platforms	ArubaOS 8.4.0.0
193441	**Symptom:** The **Station Management** process crashes continuously in the managed device because the database upgrade in a managed device fails. **Scenario:** This issue occurs when a managed device running ArubaOS 8.4.0.0 version is downgraded to ArubaOS 8.3.0.0 or lower versions, and then the **ap gap-db reinit-db** command is executed. Post this, the managed device is again upgraded to ArubaOS 8.4.0.0 by changing the boot partition. This issue is observed in managed devices running ArubaOS 8.4.0.0. **Workaround:** Copy ArubaOS 8.4.0.0 image in any of the partitions instead of switching boot partition using **boot system partition** command.	Database	All platforms	ArubaOS 8.4.0.0
193538	**Symptom:** The **Station Management** process crashes continuously in a controller. **Scenario:** This issue occurs when a stand-alone controller running any ArubaOS 8.x version is converted to managed node using the **write erase** command and then, upgraded to ArubaOS 8.4.0.0 version and rebooted in the managed node. Post this, the controller is again converted to stand-alone mode using **write erase** command. This issue is observed in controllers running ArubaOS 8.4.0.0 **Workaround:** Execute the **write erase all** command when converting a controller from stand-alone mode to managed node and vice-versa.	Database	All platforms	ArubaOS 8.4.0.0

This chapter details software upgrade procedures. Aruba best practices 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, and/or stand-alone controller.

Topics in this chapter include:

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?
  - Are all managed devices running the same version of ArubaOS?
  - What services are used on your managed device (employee wireless, guest access, Remote AP, wireless voice)?

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

Memory Requirements

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

- Do not proceed with an upgrade unless 100 MB of free memory is available. Execute the **show memory** command to identify the available free memory. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Do not proceed with an upgrade unless 150 MB of flash space is available. Execute the **show storage** command to identify the available flash space. If the output of the **show storage** command indicates that there is insufficient flash memory, free some used memory. Copy any log file, crash data, or flash backups from your managed device to a desired location. Delete the following files from the managed device to free some memory:
  - **Crash data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 93 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 93 to back up the flash directory to a file named **flash.tar.gz**. Execute the **tar clean flash** command to delete the file from the managed device.
  - **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 93 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 compact flash card. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

Deleting a File

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

In the WebUI

From the Mobility Master, navigate to **Diagnostic** > **Technical Support** > **Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

In the CLI

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

MIB Files

To access ArubaOS MIB files:

1. Log in to the Aruba Support site.
2. Navigate to **Download Software > ArubaOS**.
3. Navigate to the desired release folder.
4. Download the MIB file corresponding to the release.
5. Uncompress the MIB file to a local directory.

Syslog Files

To generate syslog file:

1. Log in to CLI of Mobility Master.
2. Switch to config mode.
3. Configure the logging command. Example: `logging <ipv4addr> facility local0`. For additional information, see ArubaOS 8.4.0.0 Command-Line Interface Reference Guide.
4. Execute the `show logging` command. For additional information, see ArubaOS 8.4.0.0 Command-Line Interface Reference Guide.

Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages

- x.509 certificates
- Log files
- Flash backup

Backing up and Restoring Flash Memory

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

In the WebUI

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

1. In the Mobility Master node hierarchy, navigate to the **Maintenance** > **Configuration Management** > **Backup** page.
2. Click **Create Backup** to backup the contents of the flash memory to the **flashbackup.tar.gz** file.
3. Click **Copy Backup** to copy the file to an external server.

   You can copy the backup file from the external server to the flash memory using the file utility in the **Diagnostics** > **Technical Support** > **Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance** > **Configuration Management** > **Restore** page and click **Restore**.

In the CLI

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

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

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

   ```
   (host) # backup flash
   Please wait while we take the flash backup.......
   File flashbackup.tar.gz created successfully on flash.
   Please copy it out of the controller and delete it when done.
   ```
3. Execute either of the following command to transfer the flash backup file to an external server or storage device.

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```

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

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Execute the following command to untar and extract the **flashbackup.tar.gz** file to the flash memory.

   ```
   (host) # restore flash
   Please wait while we restore the flash backup........
   ```

```
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

Upgrading ArubaOS

Upgrade ArubaOS using WebUI or CLI. Follow the below recommendations while upgrading:

- ArubaOS 8.4.0.0 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 8.4.0.0 to avoid upgrade failure. To remove a network adapter from ArubaOS 8.0.0.0 Mobility Master Virtual Appliance:

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 8.4.0.0 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 then 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 the 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 8.4.0.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

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

Ensure that there is enough free memory and flash space on your Mobility Master or managed device. For details, see Memory Requirements on page 92.

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

In the WebUI

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

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

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

4. Log in to the ArubaOS WebUI from the Mobility Master.
5. Navigate to the **Maintenance** > **Software Management** > **Upgrade** page.
   a. Select the **Local File** from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. If you do not want to reboot immediately, disable this option.

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

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

In the CLI

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

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

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

   or

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

   or

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

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

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

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

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

   or

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

   or

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

   or

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

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

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

7. Reboot the Mobility Master.

   ```
   (host)# reload
   ```

Verifying the ArubaOS Upgrade

Verify the upgrade using the WebUI or CLI.

In the WebUI

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

1. Log in to the WebUI to verify all the managed devices are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.

3. Verify that the number of access points and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory, to an external server or mass storage facility. See Backing up Critical Data on page 93 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 and verify that all your managed devices are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of APs and clients are as expected.
4. Test a different type of client in different locations, for each access method used.
5. Complete a backup of all critical configuration data and files on the flash memory to an external server or mass storage facility. See Backing up Critical Data on page 93 for information on creating a backup.

Downgrading ArubaOS

If necessary, you can return to your previous version of ArubaOS.

Pre-requisites

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

1. Back up your Mobility Master or managed device. For details, see Backing up Critical Data on page 93.
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 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 ArubaOS version and configuration files.
5. After switching the boot partition, perform the following steps:
   - Pre-upgrade flash backup from the file stored on the Mobility Master or managed device. Do not restore the ArubaOS flash backup file.
   - Do not import the WMS database.

- If the RF plan was changed before switching the boot partition, the changed RF plan does not appear in the downgraded ArubaOS version.
- If any new certificates were added in the upgraded ArubaOS version, reinstall these certificates in the downgraded ArubaOS version.

Downgrade ArubaOS version using the WebUI or CLI.

In the WebUI

The following steps describe how to downgrade the ArubaOS version:

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the Mobility Master or managed device by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. From **Select source file** drop-down list, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. From **Select destination file** drop-down list, enter a file name (other than default.cfg).
   c. Click **Copy.**
2. Determine the partition on which your previous ArubaOS version 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/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Enable **Reboot controller after upgrade**.
   d. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The Mobility Master or managed device reboots after the countdown period.
4. When the boot process is complete, verify that the Mobility Master or managed device is using the correct ArubaOS version by navigating to the **Maintenance > Software Management > About** page.

In the CLI

The following steps describe how to downgrade the ArubaOS version:

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

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

   or

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

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

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

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

```
#show image version
```

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

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

5. Reboot the Mobility Master or managed device.

```
(host) # reload
```

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

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

Before Calling Technical Support

Provide the following information when you call Technical Support:

- The status of installation (new or existing) and recent changes to network, device, or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
- A detailed network topology including all the devices in the network with IP addresses Interface numbers.
- The make and model number of the wireless device and NIC, driver date, version, and configuration of the NIC, and the OS version including any service packs or patches.
- The logs and output of the **show tech-support** command.
- The syslog file at the time of the problem.
- The date and time when the problem occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
- Any wired or wireless sniffer traces taken during the time of the problem.
- The device site access information, if possible.